

**PROCEEDINGS OF**

**PSAM — II**

*An International Conference Devoted to the Advancement of  
System-based Methods for the Design and Operation of  
Technological Systems and Processes*

**San Diego, California, U.S.A.**

**March 20-25, 1994**

*Editors*

**G.E. Apostolakis and J.S. Wu  
University of California, Los Angeles**

*Contributing Editors*

**D. Bley, PLG, Inc.  
S. Guarro, Aerospace Corp.  
V. Ho, PLG, Inc.  
R. Mulvihill, PRC, Inc.  
D. Orvis, APG, Inc.  
N. Sankaran, Unocal Corporation  
N. Siu, Idaho National Engineering Laboratory  
M. Stamatelatos, Scientech, Inc.**

## FOREWORD

These volumes contain papers that were presented at the PSAM II Conference. PSAM I was held in February, 1991 and its success led to the present Conference and hopefully many more.

The purpose of the PSAM Conferences is to provide a forum for the presentation of scientific papers covering both methodology and applications of system-based approaches to the design and the effective, safe operation of technological systems and processes. These include nuclear plants, chemical and petroleum facilities, defense systems, aerospace systems, and the treatment and disposal of hazardous wastes. The objective is to share experiences to the benefit of all industries.

We would like to comment on the production of these proceedings, specifically the printing and binding. Unfortunately, the publishers we had contracted to publish the proceedings did not fulfill their obligation to have them available in time for the Conference. Due to our strong belief that the proceedings should be handed out at the Conference, we have done our best to produce these volumes in the very short time available.

The Editors



**SPONSORED BY THE**

***Society for Risk Analysis***

***European Safety and Reliability Association***

**COSPONSORED BY THE**

***American Nuclear Society***

***American Society of Mechanical Engineers***

***IEEE Reliability Society***

**SPONSORING ORGANIZATIONS**

***Aerospace Corporation***

***APG, Inc.***

***ASCA, Inc.***

***Electric Power Research Institute***

***Idaho National Engineering Laboratory***

***Kazarians & Associates***

***Los Alamos National Laboratory***

***PLG, Inc.***

***PRC, Inc.***

***SAIC***

***Sandia National Laboratories***

***Scientech, Inc.***

***Tenera***

***Unocal Corporation***

***University of California, Los Angeles***

***University of Maryland***

***US Department of Energy***

## **GENERAL PROGRAM CHAIRMAN**

**Michael G. Stamatelatos, Scientech, Inc.**

## **ASSOCIATE GENERAL CHAIRMAN**

**Doug Orvis, Accident Prevention Group**

## **SENIOR ADVISORY BOARD**

**B.J. Garrick, PLG, Inc., Chairman**

**A. Amendola, Commission of European Communities  
A.H-S. Ang, University of California, Irvine  
A.T.D. Butland, SRD, United Kingdom  
J.E. Fitzgerald, Jr., US Dept. of Energy  
V.L. Grose, Omega Systems Group  
D-Y. Hsia, Institute of Nuclear Energy Research, Taiwan  
V. Joksimovich, Accident Prevention Group  
S. Kondo, University of Tokyo  
J. Meltzer, The Aerospace Corporation  
N.C. Rasmussen, Massachusetts Institute of Technology  
L. Ybarrondo, Scientech, Inc.**

## **CONFERENCE LOCAL ORGANIZING COMMITTEE**

**A.A. Dykes, PLG, Inc., Chairman**

**D. Bley, PLG, Inc.  
S.Guarro, The Aerospace Corporation  
D. Henneke, TENERA  
V. Ho, PLG, Inc.  
M. Kazarians, Kazarians & Associates  
A. Mosleh, University of Maryland  
R. Mulvihill, PRC, Inc.  
D. Orvis, APG  
N. Sankaran, UNOCAL Corporation  
N.O. Siu, INEL  
M. Stamatelatos, Scientech, Inc.**

## **ORGANIZING STAFF**

**D. Bell, UCLA  
M. Hanna, UCLA  
J. George, UCLA  
C. Garrett, UCLA  
T. Paulos, UCLA**

## TECHNICAL PROGRAM COMMITTEE

### CHAIRMAN

G. Apostolakis, University of California, Los Angeles, USA

### ASSOCIATE CHAIR

J.S. Wu, ASCA, Inc.

### MEMBERS

D. Aldridge, USA  
H.P. Alesso, USA  
A. Amendola, Italy  
D.R. Anderson, USA  
B. Ayyub, USA  
R.A. Bari, USA  
J.H. Bickel, USA  
V.M. Bier, USA  
D. Bley, USA  
E.J. Bonano, USA  
S. Book, USA  
B. Bream, USA  
D. Brooks, USA  
M.L. Brown, UK  
B. Buchbinder, USA  
R.J. Budnitz, USA  
P.C. Cacciabue, Italy  
A. Camp, USA  
R.M. Cooke, Netherland  
R.A. Cox, UK  
D. Croucher, USA  
G.E. Cummings, USA  
D. Cunha, USA  
K. Dahlgren, Sweden  
J. Devooght, Belgium  
A.A. Dykes, USA  
T. Eng, USA  
D. Frangopol, USA  
M.V. Frank, USA  
R. Friedman, USA  
R.R. Fullwood, USA

W.J. Galyean, USA  
D.I. Gertman,  
USAL.H.J. Goossens,  
Netherlands  
S. Guarro, USA  
M. Haim, Israel  
G.W. Hannaman, USA  
J.C. Helton, USA  
D. Henneke, USA  
S. Hirschberg,  
Switzerland  
V. Ho, USA  
E. Holnagel, UK  
K. Inoue, Japan  
K. Jamali, USA  
D.H. Johnson, USA  
P. Kafka, Germany  
G.D. Kaiser, USA  
D.M. Karydas, USA  
W.E. Kastenber, USA  
M. Kazarians, USA  
D.L. Kelly, USA  
K. Klein, USA  
R.F. Lavelle, USA  
C. Lavine, USA  
L. Lee, USA  
S. Lydersen, Norway  
M. Maharik, Israel  
D. Majumdar, USA  
G. Mancin, Italy  
M. Marseguerra, Italy  
T. Matsuoaka, Japan

M. Modarres, USA  
D.A. Moore, USA  
A. Mosleh, USA  
R. Mulvihill, USA  
K. Murphy, USA  
D. Okrent, USA  
L.F. Oliveira, Brazil  
N. Ortiz, USA  
D. Orvis, USA  
I.A. Papazoglou, Greece  
C.K. Park, Korea  
G.W. Parry, USA  
M.E. Pate-Cornell, USA  
P. Prassinis, USA  
C. Preyssl, Neth.  
D. Rice, USA  
L.K. Rudolph, USA  
B. Sagar, USA  
N. Sankaran, USA  
J.C.H. Schuler,  
Netherland  
N.O. Siu, USA  
D. Stack, USA  
M. Stamatelatos, USA  
J-P. Surssock, USA  
O. Svenson, Sweden  
B. Thompson, U.K.  
W. Tosney, USA  
L.P. Vestrucci, Italy  
J. Wreathall, USA  
J. Ziagos, USA

## CONTENTS

### **073 Human Reliability Applications and Models**

*Chair: S. Kondo, Tokyo Univ.*

**Human Reliability Analysis for Surry Midloop Operations**

*J.C. Lin, D.C. Bley, D.H. Johnson (PLG); T-L. Chu (BNL)*

**Enhancing Conditions for Correct Human Actions at the Ignalina Nuclear Power Plant in Lithuania**

*P. Holmgren (RELCON)*

**Human Error Model Development for Savannah River Site Nonreactor Facilities**

*R.E. Vail, H.C. Benhardt, J.E. Held, L.M. Olsen (Westinghouse Savannah Rvr.); S.A. Eide (LATA)*

**Benchmarking an Automated Human Error Analysis Technique**

*J. Wilson, P. Cloutier, S. Fogarty (Westinghouse Idaho Nucl.)*

**Assessment of Dependence of Human Errors in Test and Maintenance Activities**

*L. Reiman (STUK, Finland)*

### **074 Comparative Risk Assessment of Complex Technological Systems (II)**

*Chair: S. Hirschberg, P. Scherrer Inst.*

**Comparative Assessment of the Health and Environmental Impacts of Various Energy Systems from Severe Accidents: Issues in Review**

*A.V. Gheorghe (ETH, Switzerland)*

**Consideration of Probabilistic Safety Objectives in OECD/NEA Member Countries**

*M.F. Versteeg (Nucl. Safety Insp., Netherlands)*

**Risk Assessment of Large Industrial Complexes in Eastern Europe: A Comparative Prospective**

*A.V. Gheorghe (ETH, Switzerland)*

## **075 Fire Risk Analysis for Engineered Systems**

*Chair: R. Friedman, NASA Lewis*

**Risk Analysis of Environmental Hazards at the High Flux Beam Reactor**

*J.L. Boccio (BNL), V.S. Ho, D.H. Johnson (PLG)*

**A Model for Fuel Fire Duration and Application to the B-1B Bomber**

*D.E. Magnoli (LLNL)*

**Implementation of the FIVE Methodology: Results and Lessons Learned**

*R.C. Lindquist, M.S. Powell (Arizona Pub. Serv.)*

**Fire Risk Assessments at Rocky Flats Plant**

*T.L. Foppe, E. Stahlnecker (EG&G Rocky Flats)*

## **076 Risk-Based Regulation (I)**

*Chair: V. Joksimovich, Accident Prevention Group*

**Application and Extension of Formal Decision-Making Methods to Generic Safety Issue Decisions**

*M.P. Bohn (SNL)*

**Risk-Based Regulation Using REVEAL**

*H. Dezfuli, J. Meyer (SCIENTECH); M. Modarres (U. Maryland), H. Specter (RBR Conslts.)*

## **078 Process Safety Management**

*Chair: R.L. Cummings, Interstate Assessment Technologies*

**Integrating Compliance Efforts for Process Safety Management Regulations**

*D.A. Moore (Primatech)*

**OSHA PSM: Impact on Accident/Incident Investigation**

*D.A. Wetzel, S. Hall (Wetzel, Herron & Drucker); R.E. Rimkus, J.C. Clark (Rimkus Consulting)*

**079 Impact of Different PRA Methodologies on the Results of Nuclear Power Plant PSAs (I)**

*Chair: F.R. Hubbard, FRH*

**Risk Assessment Impacts on Risk Management**

*K.I. Kiper (N. Atlantic Energy Service)*

**Comparison of PRA Event Tree Approaches - Some Thoughts and Reflections**

*D.M. Rasmuson (USNRC)*

**On Encountering Small Numbers: How Good Models Go Bad**

*D.C. Bley, D.H. Johnson (PLG)*

**Completeness and Complexity of PSA: Do They Need it?**

*A.D. Chambardel, L. Magne (EDF, France)*

**080 Understanding Organization Factors Through Risk Models**

*Chair: J.H. Gittus, British Nuclear Industry Forum*

**An Approach for Incorporation of Organizational Factors into Human Reliability Analysis in PRAs**

*P. Moieni, D.D. Orvis (Accident Prevention Grp.)*

**The Work Process Analysis Model (WPAM): An Integrated Approach to the Incorporation of Organizational Performance into Probabilistic Safety Methodology**

*K. Davoudian, J-S. Wu, G. Apostolakis (UCLA)*

**Risk Assessment - Including the "CHAOS" Factor**

*C.T. Kleiner (C.T.K. Enterprises); R.L. Cummings (Interstate Assessment Tech.)*

**081 DOE Safety Studies**

*Chair: R.E. Hall, BNL*

**An SAR Issue for the Savannah River Reactors Resolved with PRA Methods**

*S.V. Topp (Westinghouse Savannah Rvr.)*

**Evaluation of Replacement Tritium Facility (RTF) Compliance with DOE Safety Goals Using Probabilistic Consequence Assessment Methodology (U)**

*K.R. O'Kula, J.M. East, M.L. Moore (Westinghouse Savannah Rvr.)*

Fault Tree Analysis on the F&H Canyon Exhaust Systems at the Savannah River Site  
*J.M. Low, K. Marshall (Westinghouse Savannah Rvr.)*

## **082 Fires, Floods, and Spatial Interactions**

*Chair: R. Oehlberg, EPRI*

Fermi Internal Flood Analysis Using a Component-Based Frequency Calculation Approach  
*J.C. Lin, Y.M. Hou (PLG); J.V. Ramirez, E.M. Page (Detroit Edison)*

Advances in the Methodology for the Analysis of Location-Dependent Hazards for Probabilistic Risk Assessment (PRA)  
*J.K. Liming, L.A. Bennett (ERIN Eng. & Res.)*

Location Transformation for Identification and Screening of Internal Fire and Flood Scenarios  
*T.A. Thatcher, J.L. Jones (INEL); S.A. Eide (LATA)*

EPRI Fire Events Database  
*K. Bateman, M. Marteeny, B. Najafi, B. Parkinson (SAIC); R. Oehlberg (EPRI)*

## **083 Environmental Restoration Decision Support System**

*Chair: D. Rice, LLNL*

Application of Decision Support Systems to Environmental Restoration Processes  
*D.W. Rice, J. Ziagos (LLNL); D. Bell (UCLA)*

The SEDSS - A Risk Assessment Based Decision Support Tool  
*R. Knowlton Jr., E. Webb (SNL)*

Environmental Decision Support Systems  
*J. Coleman (USEPA); J. Franco, W. Wee (U. Cincinnati)*

## **084 Reliability Based Design in Structural Engineering**

*Chair: D. Frangopol, U. Colorado*

Time-Dependent Reliability of Rock-Anchored Structures  
*M. Chakravorty, J.E. Pytte, D.M. Frangopol (U. Colorado); R.L. Mosher (USAE Waterways Exp. Station)*

Reliability Analysis of Redundant Structures by Response Surface Method  
*Y. Murotsu, S. Shao (U. Osaka, Japan); N. Chiku (Kawasaki Heavy Ind., Japan)*

**Risk Analysis of Pipeline Systems Based on Structural Reliability Models**  
*M.Sinisi, G.M. Uguccione, M. Tominez (SIAP, Italy)*

**085 Transportation Risk (II)**  
*Chair: M. Kazarians, Kazarians & Assoc.*

**A Zone Model for Determining Atmospheric Contaminant Transport Aboard Human-Crewed Spacecraft**

*S. Jones, M. Paul, F. Issacci, I. Catton, G. Apostolakis (UCLA)*

**Commercial Space Transportation Regulation: An Evolution in Risk Management**  
*R.K. Gress, D.E. Lang (USDOT)*

**System Safety Management in the UK Air Traffic Services**  
*R. Profit (Natl. Air Traffic Services)*

**086 Impact of Different PRA Methodologies on the Results of Nuclear Power Plant PSAs (II)**  
*Chair: J.H. Bickel, INEL*

**The Search for Dependencies or How Could Two Current Design Nuclear Power Plants Produce IPE Results Three Orders of Magnitude Different?**  
*F.R. Hubbard (FRH); A. Mosleh (U. Maryland)*

**Impact of Methodology and Design Changes on Turkey Point IPE Results**  
*C.N. Guey, W.A.Skelley (Florida Pwr. & Lt.)*

**087 Causal Factors in Human Reliability: Experiments and Databases**  
*Chair: A.A. Dykes, PLG*

**On the Use of Data Collected During Crew Reliability Experiments at PAKS Nuclear Power Plant - Status Report**

*A.Bareith, Z. Karsa (Inst. for Electric Pwr. Res.); A.J. Spurgin; I. Kiss (Nucl. Pwr. Plt. of Paks); L. Izso (Tech. U. Budapest)*

**Causal Identification of Human Errors Towards Intelligent CAI System for Plant Operation**  
*Y. Furuhashi, K. Furuta, S. Kondo (U. Tokyo)*

**Development of a Human Error Data Bank**  
*S.E. Taylor-Adams, B. Kirwan (U. Birmingham, England)*



Causal Factors of Operator Unreliability: An Application of Simulator Data  
*D. Orvis, P. Moieni (Accident Prevention Grp.); A.J. Spurgin*

**088 Risk Based Methods for Reliability/Availability/Maintainability**  
*Chair: S. Lydersen, Norwegian Inst. Technol.*

Some New Measures of Reliability Importance with Applications to Reliability Centred Maintenance  
*S. Lydersen (Norwegian Inst. Technol.)*

"INTEGRIT" - A Parametric Reliability and Maintainability Methodology and Safety Risk Management Tool  
*R. Vote, T. Barritt, R. Blanchford (ELINTECH)*

On-Line VS. Off-Line Maintenance in Nuclear Power Plants - Insights from a Cycle-Wide O&M Cost Model  
*J.R. Hewitt, L.A. Bennett, R.L. Durling (ERIN Eng. & Res.)*

A User-Friendly Program for System and Component Availability Monitoring and Its Potential Application in Maintenance Rule Implementation  
*D.M. Kapinus (Commonwealth Edison); T.A. Petersen (NUS)*

**089 Seismic Risk Analysis**  
*Chair: D.A. Moore, Primatech*

The Experimental Breeder Reactor II Seismic Probabilistic Risk Assessment  
*J. Roglans, D.J. Hill (ANL)*

Seismic Risk Management Using Earthquake Injury Epidemiology  
*P.J. Amico, T.A. Haley, S.J. Krill (SAIC)*

**090 Risk Based Regulation (II)**  
*Chair: G. Apostolakis, UCLA*

Regulatory Decision Making by Decision Analysis  
*J. Holmberg, U. Pulkkinen (Tech. Res. Ctr. Finland); L. Reiman, R. Virolainen (Finnish Ctr. for Radiat. & Nucl. Saf.)*

Application of Risk-Based Prioritization to QA Requirements  
*F.J. Rahn, W. Parkinson (EPRI); G.D. Bouchey (SAIC); M. Meisner (Entergy)*

*Operations)*

### **091 Management Issues**

*Chair: D. Cunha, Northrop Corp.*

**"Risk Index" - A Proposed Concept**

*S. Chakraborty (Swiss Fed. Nucl. Saf. Insp.); C. Preyssl (European Space Agency)*

**The Quality Issues of Technologic Risk Assessment**

*B.O.Y. Lydell (RSA Technologies)*

### **092 Industrial and Transportation Risks**

*Chair: D. Henneke, TENERA*

**The ARIPAR Project: Analysis of the Industrial and Transportation Risk Connected with the Ravenna Area**

*D. Egidi (Civil Protection, Emilia Romagna Region); F. Foraboschi, G. Spadoni (U. Bologna); A. Amendola (CEC-JRC)*

**Identification and Evaluation of Maritime Exposures**

*J.L. Borrello, M.J. Spansel (Adams & Reese)*

**A Decision Model of a Multi-Point Mooring of a Tanker with a Tug Assist**

*M.L. Eskijian (Calif. St. Lands Commis.)*

### **093 Time Dependence of Equipment Failure Rates-- Models, Data, and Impacts on System Modeling**

*Chair: D. Bley, PLG*

**On a Class of Dependent Failures**

*I. A. Papazoglou (National Center for Scientific Research, Greece)*

**Statistical Treatment of Time and Demand-Related Failures in the Nordic Reliability Data Book (T-Book)**

*K. Porn (Studs vik Eco & Safe)*

**Derivation of Time Dependent Component Unavailability Models and Application to Nordic PSAs**

*M. Knochenhauer (Logistoca Consult.); G. Johanson (Ind. Process Safety)*

## **094 Applications of Human Reliability Analysis**

*Chair: D.I. Gertman, INEL*

**HRA for Explosive Ordinance Disposal**

*L.N. Haney, R.G. Peatross, D.I. Gertman (INEL)*

**Nuclear Case Study for A SGTR Sequence**

*D.I. Gertman, W.J. Reece, M.B. Calley, C.L. Smith (INEL)*

**Insights into Pilot Situation Awareness Using Verbal Protocol Analysis**

*H. Blackman, C. Sullivan, K. Seidler (INEL)*

## **095 Risk Methods for Defense Applications**

*Chair: M.V. Frank, Safety Factor Assoc.*

**Probabilistic Risk Assessment of Weapon-Systems Field-Testing: Accounting for System's Complexity and Unfamiliarity**

*S. Feller, M. Maharik (RAFAEL, Israel)*

**Nuclear Weapon System Risk Assessment**

*D.D. Carlson (SNL)*

**Probabilistic Risk Assessment of Disassembly Procedures**

*D.A. O'Brien, T.R. Bement, B.C. Letellier (LANL)*

## **096 Risk Communication to the Public**

*Chair: M.E. Pate-Cornell, Stanford U*

**Effectively Communicating Risk to the Public and to Regulators: Can It Be Accomplished?**

*G.M. Pilie, G.T. Croxton (Adams & Reese)*

**Effectively Communicating Risk Assessments to the Public**

*C. Lambert, M. McDaniel (UNOCAL); S. Santos (FOCUS Grp.)*

## **097 Broad Risk Perspectives Within the DOE Weapon Complex**

*Chair: H.P. Alesso, LLNL*

**A Global Overview of Risk Management of the DOE Complex**

*H.P. Alesso, K.C. Majumdar (LLNL)*

The Integration of Human Factors into the Risk Assessment of a Nuclear Device Arming and Firing System

*T. Altenbach, W. Ferrell (LLNL)*

A Method for Determining Risk to Ground Facilities from Aircraft Accidents

*C.Y. Kimura, C.T. Bennett (LLNL)*

## **098 Risk Management - International Space Applications**

*Chair: C. Preyssl, European Space Agency*

Risk Assessment - The European Space Agency Approach

*C. Preyssl (European Space Agency)*

Risk Management of the Japanese Experiment Module on Space Station Freedom

*J.C. Lin, D.H. Johnson, W.R. Fuller (PLG); K. Sakata, H. Suzuki, S. Kojima (Mitsubishi Atomic Pwr. Ind., Japan); H. Himeno (Mitsubishi Heavy Ind., Japan)*

Rocky the Rover: PRA Meets ET

*M.V. Frank, S.A. Epstein, A.J. Spurgin (Safety Factor Assoc.)*

## **099 Root Cause and Precursor Analysis**

*Chair: M.G.K. Evans, NUS*

The Barseback Incident - A Precursor Challenging Fundamental Safety Principles of LWRs

*L. Carlsson, S. Erixon, C. Karlsson, B. Liwang, J. Olsen (SKI); G. Johanson (Ind. Proc. Saf.)*

Inferring Safety Trend From The Accident Sequence Precursor Analysis Program

*M. Modarres (U. Maryland)*

Estimating the Frequency of Electrical Overload Events in the Proposed Space Station

*T. Paulos, F. Issacci, I. Catton, G. Apostolakis (UCLA)*

## **100 Reducing Errors through Quality and Design**

*Chair: T.G. Ryan, INEL*

The Pros and Cons of Using Human Reliability Analysis Techniques to Analyze Misadministration Events

*L.T. Ostrom (INEL)*

Construction Error and Human Reliability for Structural Systems  
*M.G. Stewart (U. Newcastle)*

The Feasibility of Designing Human-Error Backup Systems for Fail-Safe Structures  
*Y. Sato (Tokyo U.); K. Inoue (Kyoto U)*

A Methodology to Support Space System Designer in Minimizing Human Error  
*M. Ferrante, C. Vivalda (Alenia Spazio); C. Fogli (ESA/ESTEC)*

### **101 Risk Assessment of Nuclear Waste Storage and Processing** *Chair: D. Stack, LANL*

PSA Results for Hanford High-Level Waste Tank 101-SY  
*D.R. MacFarlane, T.F. Bott, L.F. Brown, D.W. Stack (LANL); J. Kindinger, R.K. Deremer, S.R. Medhekar, T.J. Mikschl (PLG)*

### **102 Fire Risk** *Chair: V. Ho, PLG*

Development of the Fire Risk Analysis Methodology for Nuclear Power Plants  
*T. Matsuoka, K. Miyazaki (Ship Res. Inst., Japan); M. Kondo (JAERI, Japan)*

A Methodology for Quantifying Fire Risk On-Board Spacecraft  
*K.R. Paxton, F. Issacci, G. Apostolakis, I. Catton (UCLA)*

### **103 Risk-Based Regulation (III)** *Chair: F. Rahn, EPRI*

Where Do We Go from Here in U.S. Nuclear Safety Regulation?  
*V. Joksimovich (Accident Prevention Grp.)*

The Use of Probabilistic Risk Assessment in Satisfaction of the Nuclear Regulatory Commission's Maintenance Rule  
*R.M. DuBord, M.W. Golay (GE Nuclear Energy); N.C. Rasmussen (MIT)*

The Beneficial Use of Risk Analysis in the Regulatory Process  
*M.V. Bonaca, D.A. Dube, S.D. Weerakkody (Northeast Utilities Serv.)*

## **104 Industrial Risk Management - An EEC Perspective**

*Chair: D.M. Karydas, Factory Mutual Res. Corp.*

**Industrial Risk Management: An EEC Perspective**

*A. Amendola (CEC-JRC, Ispra)*

**Plant Level Hazard Identification Based on Functional Models**

*J. Suokas (VTT, Finland)*

**Decision Making in Process Design - Assessment of Total Safety by Aggregating the Safeties of the Subparts of the Process**

*R. Koivisto (VTT, Finland), V.J. Pohjola, M.K. Alha (U. Oulu, Finland)*

**Short Cut Risk Assessment**

*G. Wells (U. Sheffield, UK); S. Allum (Bowring Marsh & McLennan, UK)*

## **105 Environmental Risk Management--Restoration**

*Chair: T.E. McKone, LLNL*

**Scope Definition for the Hanford Tank Farms PRA**

*J.P. Kindinger (PLG), D.W. Stack (LANL)*

**Risk Management Applications at the INEL for Advanced Test Reactor Operations and Safety and Environmental Restoration and Waste Management**

*S.A. Atkinson, R.L. Nitschke (INEL)*

**Decision Analysis in Environmental Risk Management: Evaluating Multiple Stakeholder/Multiple Objective Decisions**

*D.C. Bell, G. Apostolakis, W.E. Kastenberg (UCLA)*

## **106 Data Collection and Evaluation**

*Chair: D. Croucher, EG&G Rocky Flats*

**Risk Assessment Data Banks at the Savannah River Site (U)**

*C.S. Townsend, W.S. Durant, D.F. Baughman (Westinghouse Savannah Rvr.)*

**Data Worth Analysis for Performance Assessment Using Influence Diagrams**

*J.E. White (INTERA), A.S. Heger (U. New Mexico)*

**Integrated Risk Management Database Systems**

*H. Wilhite, J.R. Pearson (CYCLA)*

## **107 Organizational Factors and Nuclear Power Plant Safety**

*Chair: K. Dahlgren, Swedish Nucl. Pwr. Insp.*

**Organizational Factors and Nuclear Power Plant Safety: A Process Oriented Approach**  
*K. Dahlgren (SNPI, Sweden); J. Olson (Battelle)*

**Organizational Assessment of a Maintenance Department at a Nuclear Power Plant**  
*L. Reiman (STUK, Finland), L. Norros (VTT, Finland)*

**Evaluation of Quality Systems**  
*I. Blom (SNPI, Sweden), B. Melber, N. Durbin (Battelle)*

**Two Solutions to the Same Problem - Assessing Processes and Their Outcomes**  
*G. Svensson (SNPI, Sweden)*

## **108 Interactive Fault Detection and Diagnosis--Approaches**

*Chair: A. Poucet, ITER EDA*

**Development of Diagnosis Systems of Autonomous Operation System for Nuclear Power Plants**  
*A. Saiki, K. Okusa, A. Endou (PR& NFD Corp., Japan)*

**A Unified Paradigm for Verifying Reliability Requirements in Dynamic Systems**  
*J. Ruiz, M. Roush (U. Maryland)*

**Towards a Taxonomy of System Failures**  
*J. Ruiz, M. Modarres (U. Maryland)*

### **073 Human Reliability Applications and Models**

*Chair: S. Kondo, Tokyo Univ.*

**Human Reliability Analysis for Surry Midloop Operations**

*J.C. Lin, D.C. Bley, D.H. Johnson (PLG); T-L. Chu (BNL)*

**Enhancing Conditions for Correct Human Actions at the Ignalina Nuclear Power Plant in Lithuania**

*P. Holmgren (RELCON)*

**Human Error Model Development for Savannah River Site Nonreactor Facilities**

*R.E. Vail, H.C. Benhardt, J.E. Held, L.M. Olsen (Westinghouse Savannah Rvr.);  
S.A. Eide (LATA)*

**Benchmarking an Automated Human Error Analysis Technique**

*J. Wilson, P. Cloutier, S. Fogarty (Westinghouse Idaho Nucl.)*

**Assessment of Dependence of Human Errors in Test and Maintenance Activities**

*L. Reiman (STUK, Finland)*



## HUMAN RELIABILITY ANALYSIS FOR SURRY MIDLOOP OPERATIONS

James C. Lin,<sup>1</sup> Dennis C. Bley<sup>1</sup>, David H. Johnson<sup>1</sup> and T-L Chu<sup>2</sup>

<sup>1</sup>PLG, Inc.

4590 MacArthur Boulevard, Suite 400  
Newport Beach, CA 92660-2027

<sup>2</sup>Brookhaven National Laboratory  
Department of Advanced Technology  
32 Lewis Avenue, Building 130  
Upton, Long Island, NY 11973

### INTRODUCTION

The analysis is performed in support of the Level 1 probabilistic risk assessment (PRA) for Surry during low power and shutdown conditions.<sup>1</sup> The objectives of this study are to evaluate the important accident sequences initiated during midloop operations and to compare the qualitative and quantitative results with those for accidents initiated during power operations. The primary type of human actions analyzed in this study involves the dynamic operator actions and recovery actions that take place during the accident sequence following an initiating event. Two parts of the human actions were analyzed: failure to diagnose and failure to perform the action.

The scope of the Level 1 PRA for Surry during midloop operations includes internal, fire, and flood initiating events. To evaluate human actions in the shutdown conditions, the following important differences from the power operation case must be recognized. Due to the different decay heat levels, the time windows available for operator diagnosis and action performance are different if the timings of accident initiation relative to the reactor shutdown time are different. This implies that the operator performance may be different for the same action responding to the same event initiated at different times after shutdown. For the same reason, greater times are available for recovery actions. Because of the relative lack of instrumentation and emergency procedures and the need to consider possibilities for loss of containment integrity that are unique to plant shutdown conditions, there is a greater uncertainty in the behavior of the operators. Due to the many operator actions involved during the accident response to events initiated in shutdown conditions, more dependencies may exist among the preceding and subsequent actions.

## QUALITATIVE EVALUATION

The approach to evaluating human actions and recovery actions that follow an initiator is to, first, qualitatively define the event scenario, required action, important factors affecting operator performance, and the consequences of the action not being successful. Relatively detailed qualitative descriptions of all relevant information that could affect operator performance were prepared. This is because such actions are beyond direct experience and relevant statistical data. Therefore, most practical estimates of human error rates are strongly influenced by the experience and judgment of the experts performing the analysis. It is essential that these experts base their evaluations on the most complete and accurate descriptive information available. Table 1 gives an example page of these qualitative descriptions.

Then, a set of seven performance-shaping factors (PSF) were selected to characterize the important elements that affect the successful completion of the operator actions. These factors include preceding and concurrent actions, plant interfaces, time adequacy, availability of procedures, task complexity, training and experience, and stress level. Because of the decreasing decay heat levels, timing of the accident scenario initiation is very important to the time available for operator response or recovery actions during the transient prior to core damage and significant radioactive material release. These time windows are based, in large part, on the thermal-hydraulic analyses that have been performed for Surry in the pressurized water reactor (PWR) Low Power and Shutdown Accident Sequences Program. They were considered for both diagnosis and action performance.

## QUANTITATIVE ANALYSIS

The qualitative evaluations of the actions and the important factors that affect operator performance were used to derive the human error probabilities (HEP) using an adaptation of the success likelihood index methodology. This methodology is based on the assumption that the likelihood of operator error in a particular situation depends on the combined effects of a relatively small set of performance-shaping factors that influence the operator's ability to accomplish the action.

To quantify the HEPs, the PSFs were rated against a weight that relates the relative influence of each PSF on the likelihood of the success of the action and a score that relates whether the PSF helps or hinders the operator to perform the action. With the ratings for PSFs, the numerical model was calibrated using well-defined actions obtained from analysis for other PRAs. The calibration procedure ensures that the error probabilities are realistic and consistent with available data, observed human behavior, and the results from comparable expert evaluations of similar activities. A ranking of contributors to the human error rate is accomplished by multiplying the weight of the PSF by the numerical score of the PSF. Because the score increases as the failure potential increases, the product of the weight and the rating becomes a direct measure of the relative contribution of that PSF to the human error rate of that action. The uncertainties of the HEPs are estimated from the uncertainties in the ratings of the PSFs and the uncertainties associated with the calibration tasks.

## ACTIONS AT MIDLOOP

Several hundred specific actions are considered in this analysis, and over 150 are quantified directly. Others are assigned HEP equal to one of those actually quantified directly because of similarities in required response, cues, timing, and all other factors.

**Table 1. Example page of qualitative descriptions of dynamic human actions evaluated for the Surry shutdown PRA.**

<p><b>SRA(B,3,4,5)R6:</b></p> <p>Operator establish steam generator bleed and feed (reflux cooling) following a loss of RHR at mid-loop in POS 6 of refueling.</p> <hr/> <p><b><u>PRECEDING EVENTS</u></b></p> <ul style="list-style-type: none"> <li>• 4 days since reactor shutdown.</li> <li>• Loss of RHR due to             <ul style="list-style-type: none"> <li>- over-draining (RA),</li> <li>- failure to maintain RCS level (RB),</li> <li>- unrecoverable RHR failure (R3),</li> <li>- operating RHR train failure (R4), or</li> <li>- recoverable RHR failure (R5).</li> </ul> </li> <li>• For the action event of establishing SG reflux cooling, Operators have successfully diagnosed that a loss of RHR has occurred and referred to 1-AP-27.00 Loss of Decay Heat Removal Capability.</li> <li>• Restoration of RCS level has failed (for RA(B)R6-XHE-S-16) or Restoration of RHR cooling has failed after successfully restoring level (for RA(B,4,5)R6-XHE-S-8).</li> </ul> <hr/> <p><b><u>INDICATIONS OF PLANT CONDITIONS</u></b></p> <ul style="list-style-type: none"> <li>• Low RCS level (for RA(B)R6-XHE-S-8(16)), restored RCS level (in the event of failure to restore RHR cooling; for RA(B)R6-XHE-S-8(16)), and slowing decreasing RCS level.</li> <li>• Control room RCS standpipe level 1-RC-U-100A (may not be accurate if RCS boiling starts).</li> <li>• Control room cold shutdown RCS level narrow range 1-RC-LR-106.</li> <li>• Intra-loop indication of RCS level within the loop, i.e., from middle to top of the loop; may be partially unavailable if vital bus is unavailable).</li> <li>• RCS standpipe level local indication.</li> <li>• Shutdown cooling low level annunciator 8-C-8.</li> <li>• RHR pump motor amperage oscillation (for RA(B)R6-XHE-S-8(16)).</li> <li>• Excessive RHR pump noise (for RA(B)R6-XHE-S-8(16)).</li> <li>• No RHR flow</li> <li>• Control room RHR flow indication 1-RH-FI-1605.</li> <li>• RHR heat exchanger low flow annunciator 8-C-6.</li> <li>• Incore thermal couples for RCS temperature monitoring (may be partially unavailable if vital bus is unavailable).</li> </ul> <hr/> <p><b><u>PROCEDURAL GUIDANCE</u></b></p> <ul style="list-style-type: none"> <li>• 1-AP-27.00 Loss of Decay Heat Removal Capability</li> <li>• Steps 26, 27, and 28 and Attachment 6, Part 4: Maintain SGs near 33% NR level and dump steam using SG PORVs or main condenser to control RCS temperature.</li> </ul> <hr/> <p><b><u>TRAINING AND EXPERIENCE</u></b></p> <ul style="list-style-type: none"> <li>• Operators train on this scenario during simulator drills.</li> </ul> <hr/> <p><b><u>CONCURRENT ACTIONS/COMPETING FACTORS</u></b></p> <ul style="list-style-type: none"> <li>• Restoration of RCS level (for RA(B)R6-XHE-S-8(16)).</li> <li>• Restoration of RHR cooling (for RA(B,4,5)R6-XHE-S-8).</li> </ul> <hr/> <p><b><u>INDICATION OF SUCCESSFUL COMPLETION/IMPACT OF SUCCESS</u></b></p> <ul style="list-style-type: none"> <li>• SG pressure is stable or slowly decreasing.</li> <li>• SG level is slowly decreasing if water is not feeding into the SGs.</li> <li>• WR hot leg temperatures are stable or slowly decreasing.</li> <li>• WR cold leg temperatures are at saturation for SG pressure.</li> <li>• RCS level is stable.</li> <li>• Successful decay heat removal is established.</li> </ul> <hr/> <p><b><u>IMPACT OF FAILURE/ADDITIONAL CUES</u></b></p> <ul style="list-style-type: none"> <li>• SG pressure is increasing if steam dump is unsuccessful.</li> <li>• SG level is decreasing if no water is provided to the SGs.</li> <li>• As RCS heats up RCS temperature increases; loss of subcooling and alarms.</li> <li>• Belieff would lead to decreasing RCS levels.</li> </ul> <hr/> <p><b><u>TIME CONSTRAINTS</u></b></p> <ul style="list-style-type: none"> <li>• At 4 days into the outage, boiling would occur within about 21 minutes and core uncover could occur as early as 144 minutes.</li> <li>• Establishing SG reflux cooling should only take a few minutes if instrument air and semi-vital bus are available and if providing water to the SGs is not necessary.</li> </ul>
--

A large number of specific action scenarios are actually special cases of a small number of functional responses defined by plant procedures and colored by special conditions of the sequence of events that leads to the need for action.

## Human Responses

All of the actions discussed and quantified fall into four broad categories, as shown in Table 2. It should be noted that this analysis is not a cognitive model of human behavior.

Table 2. Human response categories.

Category	Specific Case	Discussion
Global Actions		These global events strongly affect other actions within the same event tree. If they fail, the subsequent actions that depend on them cannot succeed.
	Diagnosis	The initiator creates a loss of RHR cooling condition that must be recognized. Furthermore, it must be understood to the extent that appropriate procedures are begun that can restore core cooling within the time available.
	Isolation of Canal	The loss of power events trip the major water supplies to the canal. If action is not taken quickly, the canal will drain through the main condensers, and service water cooling will be lost. No actions that involve equipment that requires cooling (pumps and heat exchangers) can succeed.
Primary Cognitive Responses		These actions are associated with the individual top events in the event trees. They represent the likelihood that, given a successful diagnosis (and, if necessary, successful isolation of the canal), the operators carry out the actions required by procedure to provide core cooling.
	Makeup	If the reactor vessel level falls either because of active overdraining or failure to properly maintain level, the operators can restore level to permit recovery of RHR flow.
	Restore RHR Cooling	If the loss of RHR cooling is recoverable, the operators can shift to standby equipment or recover failed equipment.
	Steam Generator Bleed and Feed Cooling	The reactor can be cooled by boiling water on the secondary side of the steam generator. For conditions analyzed in this study, only reflux cooling is possible. While procedures call for feeding the steam generators, the cases of interest have sufficient inventory to support steaming alone.
	Primary Feed and Bleed	The mode of preference for this cooling method is fill and spill. The procedures and training follow this approach--forced feeding of the primary until water spills out the PORVs. Operators indicate that they would throttle flow gradually to conserve water as long as the RCS is cooling down.  For scenarios in which no injection source is available, procedures guide operators to the use of the charging pump of the adjacent unit.
	Gravity Feed	For many cases, gravity draining water to the RCS can provide acceptable cooling. Often this cooling mode cannot provide long-term stability but can greatly extend the time available for recovery for other cooling paths.
	Recovery of Room Cooling	For loss of emergency switchgear ventilation scenarios, early recovery by opening doors and rigging portable fans can avoid the loss of RHR initiating event entirely. When the operators respond effectively to high room temperature alarms, no impact on the plant occurs.
Specific Activities		In several cases, detailed operator actions associated with establishing specific equipment in support of the preceding activities are modeled separately in the fault trees. Diagnosis and the cognitive aspects of the detailed action are quantified by high level events in the fault tree. If they are successful, then the lower level actions are possible.
Recovery		Recovery actions beyond those indicated above are considered on a limited case-by-case (i.e., cutset-by-cutset) basis.

## Factors Affecting Performance

The continuum of factors affecting performance can be thought of in terms of a discrete set of conditions as described in Table 3. Thus, the current analysis is thorough in terms of modeling actions for which the operators are well trained. However, for some unlikely but possible situations, the analysis is optimistic. It is believed that the overall impact of not quantifying such situations will be small.

**Table 3. Factors affecting performance.**

Factor	PRA Model
<u>Initiating Event</u>	Each human action is conditioned on the initiating event that begins the event sequence. They are all identified and explicitly considered. In some cases, the effects of different initiators are identical, and the same quantification is used for those cases.
<u>Previous/Concurrent Hardware Failures and Human Actions</u> No Other Complicating Factors	All actions are first analyzed under this condition. This value of the human action quantification is used for some cases in which complicating factors should degrade human performance. Therefore, some cutsets with additional failures are optimistically quantified. That such cutsets would have negligible impact on risk should be verified in the future comprehensive HRA.
Event Tree Sequence	To some extent, the impact of the action occurring on different branches of an event tree is quantified. Treatment of this dependency is not complete in the analysis.
Isolated Hardware Failures and Maintenance Activities that Create an Impediment to Successful Action due to the Hardware Failure Alone but Create no Confusion and Require No Special Response	These effects are not modeled except that possible failure of the backup equipment is modeled. Because they have little impact on human cognitive response, and because few situations have extremely short time windows for action, these cases are expected to have minimal impact on the results.
Significant Support System Failures	These effects are not modeled except for some recovery action cases. They can lead to very severe degradation in human performance for scenarios with substantial functional failures, but such cases are expected to be of very low frequency.
Previous Failure of Human Action	These effects are not thoroughly modeled except for some recovery action cases. However, if diagnosis fails, all subsequent actions are failed. Otherwise, because diagnosis was successful, the operators are on the right track. Therefore, the failures are probably due to minor slips or physical difficulties that can be bypassed by continuing with the procedure. While we do not expect this approach to lead to major errors in quantification, the validity of this judgment requires verification through detailed modeling.
<u>Other Performance-Shaping Factors</u>	The other performance-shaping factors described earlier are thoroughly considered.
<u>Time after Shutdown</u>	No special maintenance unavailability conditions that apply during each POS are considered other than positions of the LIVs, inventory in the steam generators, and likelihood of the pressurizer safety valves being removed.  Drain-down initiators must happen on entering the respective POS. However, the earliest times for entering this condition are used for all events except for a few recovery action cases. Because that time is fairly long after shutdown for POS R10, little variation in HRA results is expected if more thorough treatment of time is performed. As for POS D6, that time is very short, and the effects are much more severe.

## RESULTS

Table 4 illustrates a sample calculation of the HEPs. The results of this study indicate that the dominant cause of core damage is operator failure to mitigate the accidents. This is primarily because, during shutdown operations, most of the automatic actuation features for accident mitigation are disabled, very few procedures are currently available for accident mitigation, and a significant fraction of the mitigation equipment is removed from service. However, due to the long period of time during which a potential shutdown accident sequence may be initiated, significant uncertainty and conservatism are involved in the analyses of plant thermal-hydraulic and operator responses. As a result, there is a very large uncertainty in the human error probabilities used in this study.

Table 4. Example page for PSF ratings and HEPs for flood initiating events.

Dynamic Human Action Evaluation for: Surry Midloop Operations														
Evaluation Team: DCE/JCL														
Action Grouping Logic: Floods														
Action Code	Preceding & Other Actions Weight Score	Plant Interfaces Weight Score	Time Adequacy Weight Score	Procedures Weight Score	Complexity Weight Score	Training & Experience Weight Score	Stress Weight Score	FLI	P(fail)	LOG(P(fail))				
<b>Rated Actions</b>											7.87	1.0E+00	0.00	
<b>MAX</b>														
D-F1A26-KHE	0.00	1	0.24	5	0.18	10	0.12	2	0.12	5	0.24	5	0.12	9
D-F1A10-KHE	0.00	1	0.24	5	0.18	5	0.12	2	0.12	5	0.24	5	0.12	8
D-F1A06-KHE	0.00	1	0.24	5	0.18	10	0.12	2	0.12	5	0.24	5	0.12	10
D-F2A26-KHE	0.00	1	0.24	4	0.18	8	0.12	2	0.12	4	0.24	3	0.12	7
D-F2A10-KHE	0.00	1	0.24	4	0.18	5	0.12	3	0.12	4	0.24	3	0.12	6
D-F2A06-KHE	0.00	1	0.24	4	0.18	9	0.12	3	0.12	4	0.24	3	0.12	9
D-F3A26-KHE	0.00	1	0.24	5	0.18	9	0.12	3	0.12	5	0.24	4	0.12	9
D-F3A10-KHE	0.00	1	0.24	5	0.18	5	0.12	3	0.12	5	0.24	4	0.12	8
D-F3A06-KHE	0.00	1	0.24	5	0.18	10	0.12	3	0.12	5	0.24	4	0.12	10
D-F4A26-KHE	0.00	1	0.24	2	0.18	5	0.12	2	0.12	2	0.24	2	0.12	5
D-F4A10-KHE	0.00	1	0.24	2	0.18	2	0.12	2	0.12	2	0.24	2	0.12	4
D-F4A06-KHE	0.00	1	0.24	2	0.18	7	0.12	2	0.12	2	0.24	2	0.12	6
A-F1A26-KHE-S-8	0.17	9	0.09	8	0.17	7	0.09	4	0.17	5	0.17	7	0.13	10
A-F2A26-KHE-F-4	0.20	7	0.10	6	0.15	4	0.10	4	0.10	8	0.20	5	0.15	9
A-F2A10-KHE-F-4	0.21	7	0.11	6	0.11	4	0.11	8	0.21	5	0.16	8	0.11	8
A-F2A06-KHE-F-3	0.19	7	0.10	6	0.19	8	0.10	4	0.10	8	0.19	5	0.14	9
A-F2A26-KHE-G-5	0.19	9	0.10	6	0.14	7	0.14	4	0.10	6	0.19	5	0.14	10
A-F2A10-KHE-G-4	0.19	9	0.10	6	0.14	5	0.14	4	0.10	6	0.19	5	0.14	9
A-F2A06-KHE-G-4	0.16	9	0.08	7	0.16	8	0.12	5	0.16	8	0.16	6	0.16	10
A-F2E26-KHE-S-8	0.18	8	0.09	8	0.18	6	0.09	3	0.14	3	0.18	7	0.14	10
A-F3A26-KHE-S-8	0.18	9	0.09	8	0.18	6	0.09	3	0.14	3	0.18	7	0.14	10
A-F4A26-KHE-S-5	0.10	2	0.14	5	0.19	5	0.10	2	0.14	7	0.19	4	0.14	6
A-F4A10-KHE-S-5	0.11	2	0.17	5	0.11	3	0.11	2	0.17	7	0.22	4	0.11	4
A-F4A06-KHE-S-4	0.09	2	0.14	6	0.18	7	0.09	2	0.14	8	0.18	4	0.18	7
A-F4A26-KHE-S-9	0.00	6	0.12	7	0.24	5	0.12	3	0.18	3	0.24	6	0.12	9
A-F4A10-KHE-S-5	0.19	6	0.10	6	0.19	5	0.10	3	0.18	8	0.19	3	0.14	6
A-F4A06-KHE-S-5	0.11	6	0.11	6	0.22	3	0.11	5	0.06	8	0.22	3	0.17	4
A-F4A26-KHE-F-4	0.17	6	0.08	6	0.17	9	0.08	5	0.17	8	0.17	3	0.17	9
A-F4A10-KHE-G-6	0.20	7	0.10	5	0.15	5	0.15	4	0.10	6	0.20	2	0.10	7
A-F4A06-KHE-G-5	0.21	7	0.11	5	0.11	3	0.16	4	0.11	6	0.21	2	0.11	5
A-F4A26-KHE-G-5	0.17	8	0.08	7	0.17	8	0.08	5	0.17	8	0.17	6	0.17	10
<b>MIN</b>											0.00	1.1E+08	-7.98	
<b>Calibration Actions</b>														
WSAC2A: OEI-IC	0.09	2	0.18	4	0.18	3	0.18	4	0.09	2	0.18	2	0.09	2
WSAC2A: MCA-LOCA	0.09	6	0.18	3	0.18	8	0.18	8	0.09	6	0.18	9	0.09	8
WSAC2A: RTI-LOCA	0.11	3	0.11	4	0.22	5	0.11	5	0.11	0	0.22	4	0.11	2
											<b>Regression Output:</b>			
											Constant	-7.98		
											Std Err of Y Est	0.506		
											R Squared	0.971		
											No. of Observations	3		

## FOLLOW-UP ANALYSIS

In a follow-up phase of this study, a refined approach that defines several time intervals after shutdown to better account for the decay heat level at which the initiating event occurs is used. It is shown that the dynamic operator actions taken in response to shutdown initiating events depend much more on the time interval during which the initiating event occurs than on the types of outage (i.e., refueling outage and drained maintenance outage) and the POSS; i.e., 6 and 10 for midloop operations.

## REFERENCE

1. T-L. Chu, et al., "PWR Low Power and Shutdown Accident Frequencies Program, Phase 2 — Internal Events," Draft Report, Brookhaven National Laboratory, Upton, New York (1992).

**ENHANCING CONDITIONS FOR CORRECT HUMAN ACTIONS  
AT THE IGNALINA NUCLEAR POWER PLANT IN LITHUANIA  
(RBMK-REACTOR TYPE)**

Per Holmgren

RELCON AB  
Box 1288  
S - 172 25 SUNDBYBERG, SWEDEN

**1. INTRODUCTION**

This paper presents parts of the work performed in the field of man-machine interactions within the Barselina Project which is a multilateral project between Lithuania, Russia and Sweden. The intention of the Barselina Project is to share and develop knowledge in the area of analysis and assessment of severe accident risks. The purpose is also to transfer knowledge to the Ignalina RBMK plant in Lithuania, regarding these matters.

The paper describes a method used to investigate the human factors at the Ignalina Nuclear Power Plant (INPP). Preliminary results from the first case is presented and discussed.

**2. MODEL DESCRIPTION**

In the Barselina project there was a lot of work done during 1991 - 1993 to create a preliminary model of a probabilistic safety analysis (level-1 study). In the study several critical human interactions of importance for reactor safety were identified. To be able to quantify this first version of the study screening values for the operator action probabilities were used. No effort were in this phase made to specify these interactions and their probabilities. During the current phase of the Barselina project one of the main areas of the project is to investigate these identified critical human interactions.

The intention of the investigation of the human interactions is to increase the overall reactor safety at the Ignalina Nuclear Power Plant (INPP). Both the method and results are an outcome of this clearly stated intention. The used method needed to be rather simple but effective and also give an accurate description of the actual situation. From earlier work within this field a combination of the models from Swain's handbook of Human Reliability Analysis (ref. 2), SHARP (ref. 3) and Rasmussen's mental scheme (ref. 3) was chosen.

The five steps in the method can shortly be described as:

- 1. Identification** of important human actions in the perspective of reactor safety. This includes both human actions in accident sequences and human actions as initiating event of an accident sequence. The method also investigates and takes into account how the human actions related to test and maintenance can affect safety.
- 2. Modelling** and subdividing of each human action. This is done by using operator actions trees (event trees). The operator action trees includes errors in diagnoses, errors of omission and recovery actions, (at this point no modelling of human actions that aggravates the situation has been made).
- 3. Probabilities** for the human actions are set in two steps. First the Rasmussen's model for human behaviour is used to set a range for the probability for a specific human action. After that, different issues that affects the conditions for performing the operation is discussed and validated. This is done in checklists that finally results in a probability for a non-successful human action. The issues in the checklists can be related to as Performance Shaping Factors (PSF). The probability is then input to the operator action tree. This procedure is done for each action (event) in the operator action tree.
- 4. Quantification** of the operator action tree. This gives the failure probability of the identified human action. If the operation in question is identified as a part of the PSA it is implemented in the PSA.
- 5. Safety enhancement.** By going through this procedure and using the checklists it is easy to make recommendations for enhancing the conditions for correct human actions. These recommendations can point at relatively small and specific matters as well as a general policy for the plant. You can also easily perform sensitivity analysis for the recommendations to show the most effective way to enhance safety. Just by going through this procedure you will in fact get an improvement of human actions related to safety, while people at the plant that's involved in the analysis starts to discuss and investigate different human actions.

The model is described in detail by presenting the pilotcase made at the Ignalina plant in cooperation between Sweden and Lithuania. The case describes the analysis of the human interactions involved in decreasing the breakflow by closing manually operated valves in case of a rupture in a GDH (fig. 1).

## 2.1 DESCRIPTION OF THE EVENT

This accident sequence is initiated by a rupture in a Group Distribution Header (GDH), see fig. 1. After closing the valves at the Main Circulation Pumps (MCP) the water level will start to increase in the Drum Separator and after approximately 15 minutes there will be a backflow in the 40-44 channels that are connected to the ruptured GDH. To decrease the loss of water the operator reduces the flow by closing manually operated valves.

The available time for closing the valves is at least 7 hours from the rupture occurs. This is the time before the water supply is depleted and it is based on a very conservative water balance calculation. During this time a correct diagnosis must be made and correct actions need to be taken.

In the control room there are three main activities. The reactor operator (RO) has the surveillance of the reactor. The turbine operator (TO) do the same for the turbine and the third operator is the operator of the safety systems of the reactor, safety systems operator (SSO). The SSO has one assistant, assistant safety systems operator (ASSO). The deputy shift



supervisor (DSS) is in charge of the reactor control room. These five persons are together the control room team. In charge of the whole shift at the plant is the shift supervisor, situated in another room. For one exception we assume in this analysis that the people in the control room team are the only ones available for making diagnosis and for taking the actions according to the diagnosis. The exception is if the deputy shift supervisor DSS becomes unavailable (e.g. sick) then the shift supervisor can replace him.

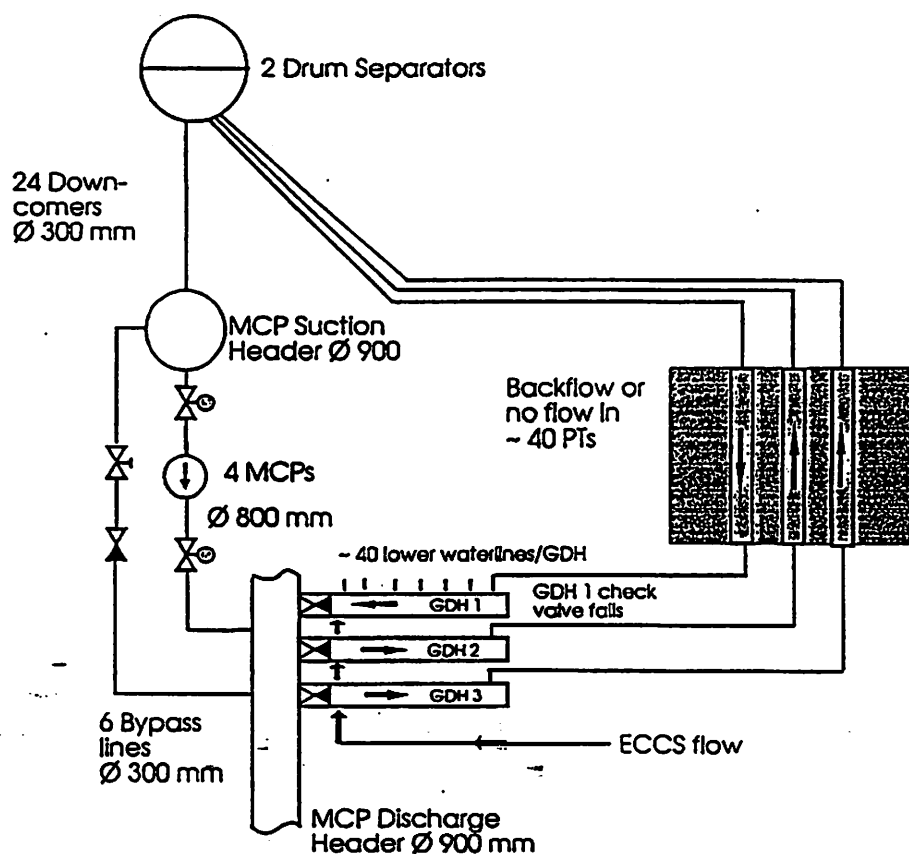


Figure 1

In front of the RO there is a large scheme showing the flow rate for each channel in the reactor. In case of changes of the flow rate, if passing the setpoints low/ high, there is a red dot lighting and a sound signal. In case of the initiating event the control rods are automatically inserted. The lights and signals indicate low flowrate in the 40-44 channels, that are connected to one GDH. Indication also comes from high pressure in one of the rooms. The fast scram system will automatically start immediately after the accident. It is followed by automatic start-up of the ECCS and AFWS (approximately 35 seconds after the accident occurred). This is surveyed by the SSO and his assistant. Both RO and DSS will notice that the flow is decreased in a group of channels (red lighting). He will also receive the alarm of high pressure in the room for the GDH. Thus, there are two clear indications of damage of a GDH. When the control room team identify the event as a GDH rupture the DSS will make the decision to close the valves. He will notify the RO and call the manager of the reactor shop (MR), who is sitting in another room, to close the specific valves. The MR calls for the valve operators, three persons sitting in another room, to come to the reactor shop. When they get there they will be verbally informed which valves that shall be closed. At least two of them will go to a room above the damaged GDH, where the valves are situated. The door to the valve room is locked, so they need to get the key from the MR. In that room they will have direct contact to the RO in the control room. In the valve room there are 40-44 valves to be closed. That will take about 30 minutes. To keep the water balance calculations show that it is necessary to close

at least 20 of them.

There are written instructions for these types of accident sequences, but they are in a bad shape and not used by the personnel. They regard the instructions as a book which they study for their monthly examine.

### 2.3 ANALYSIS

The description above is made into a logical structure by using event tree modelling (figure 2). The event tree covers both the interactions between man and machine and the dependencies between different manual operations. Done with the logical structure we look for what kind of behaviour (cognitive modelling) that is needed for the specific operation. That gives us a field for the probabilities. The probabilities, which are taken from ref. 2 and ref. 3, are:

- |                     |                                   |
|---------------------|-----------------------------------|
| 1. Skilled-based:   | Probability $10^{-4}$ - $10^{-2}$ |
| 2. Rule-based:      | Probability $10^{-3}$ - $10^{-1}$ |
| 3. Knowledge-based: | Probability $10^{-2}$ - $10^0$    |

To get a more precise value, every operation has to be examined in detail. For this part checklists like the one shown in figure 3 were used. The checklist rates the conditions for the operator to carry out the operation correctly. By going through everything that has any impact on the conditions of the operation, the result will be a list of things that could improve the conditions for the operation. After filling out the checklist it will be possible to get a more accurate probability for failure. The quantification and the remarks in the checklist will then point at the most efficient steps to take for improving safety. After using the checklist, a linear approximation is used to get a probability, where the highest rate corresponds to the lowest probability in that specific field of probability. The probabilities are shown below.

Table 1

EVENT	OPERATION	TYPE	PROB.
V33M3	DSS identifies and decides to close the valves.	3	0.06
V33M4	Communicate the right valves.	1	0.0003
V33M5	RO correct the mistake made by DSS.	3	0.05*
V33M6	Valve operator closes the right valves.	2	0.003
V33M7	Control room correct mistake from valve operator.	1 (0.1 - 1.0)	0.4

\* For the event V33M5 we assume that there is a dependent relation to what has happened before that event. Therefore the event V33M5 is judged to have the probability 0.1.

Given these probabilities the result of the quantification was that the total probability for failing to close 20 valves is 0.013 per demand. In the part of results and conclusions the remarks in the checklist will be further discussed.

## 3 RESULTS AND CONCLUSIONS FOR THE PILOT CASE

The results from the analysis are both a probability (0.013 per demand) for the failing to close at least 20 valves and a number of suggestions for decreasing that probability, that is to enhance safety.

### 3.1 SUGGESTIONS FOR ENHANCING SAFETY

The first issue is that the instructions are in a bad shape. The attitude among the personnel in the control room is that the instructions are only used for studying for the examinations, and they do not use them in an emergency. So there is no practice in using written instructions during an accident sequence. A recommendation is that the instructions should be rewritten and put in order. Then it should be investigated if there should be a policy about following the written instructions during an accident sequence. In the Swedish plants it is "forbidden" to follow one's memory instead of using written instructions in an accident situation. A few other issues were noticed:

- The deputy shift supervisor goes for simulator training every 3 - 4 years in a simulator that is not an exact model of the INPP. A long term goal for the plant should be to give the operators a more frequent and accurate training for emergency situations.

- There should be an extended discussion if it is really possible to reach or to be in the valve room during LOCA-circumstances.

### 3.2 QUESTIONS TO INVESTIGATE FURTHER

- Has this operation, closing valves in accident situation, ever been practised ? Practising it should point out any bad parts in the operation.

- Knowing that there are examinations every month for the deputy shift supervisor - is there a training program for the rest of the control room operators and is there some sort of training for the whole team together ?

- It seems to be a bit troublesome to first have the DSS to talk to MR about closing the valves and then MR have to call for the valve operators. They have to run down to the reactor shop and from there to the valve room, where they are in contact with the RO.

## 4. GENERAL CONCLUSIONS

The main conclusion from the pilotcase analysis is that the method is easy and effective to use, and also acceptable and understandable for the staff at the plant.

## REFERENCES

1. Peter Jacobsson and Per Holmgren. "Human Interactions Analysis V3.3", BPR(93)6. (1993)
2. A.D. Swain and H.E. Guttman. "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", NUREG/CR-1278, US NRC. (August 1983).
3. Systematic Human Action Reliability Procedure (SHARP), EPRI NP-3583, Project 2170-3, Interim report. (June 1984)
4. Instructions from the Ignalina Nuclear Power Plant.
5. Guidelines for Conducting Human Reliability Analysis in Probabilistic Safety Assessment, IAEA Document.

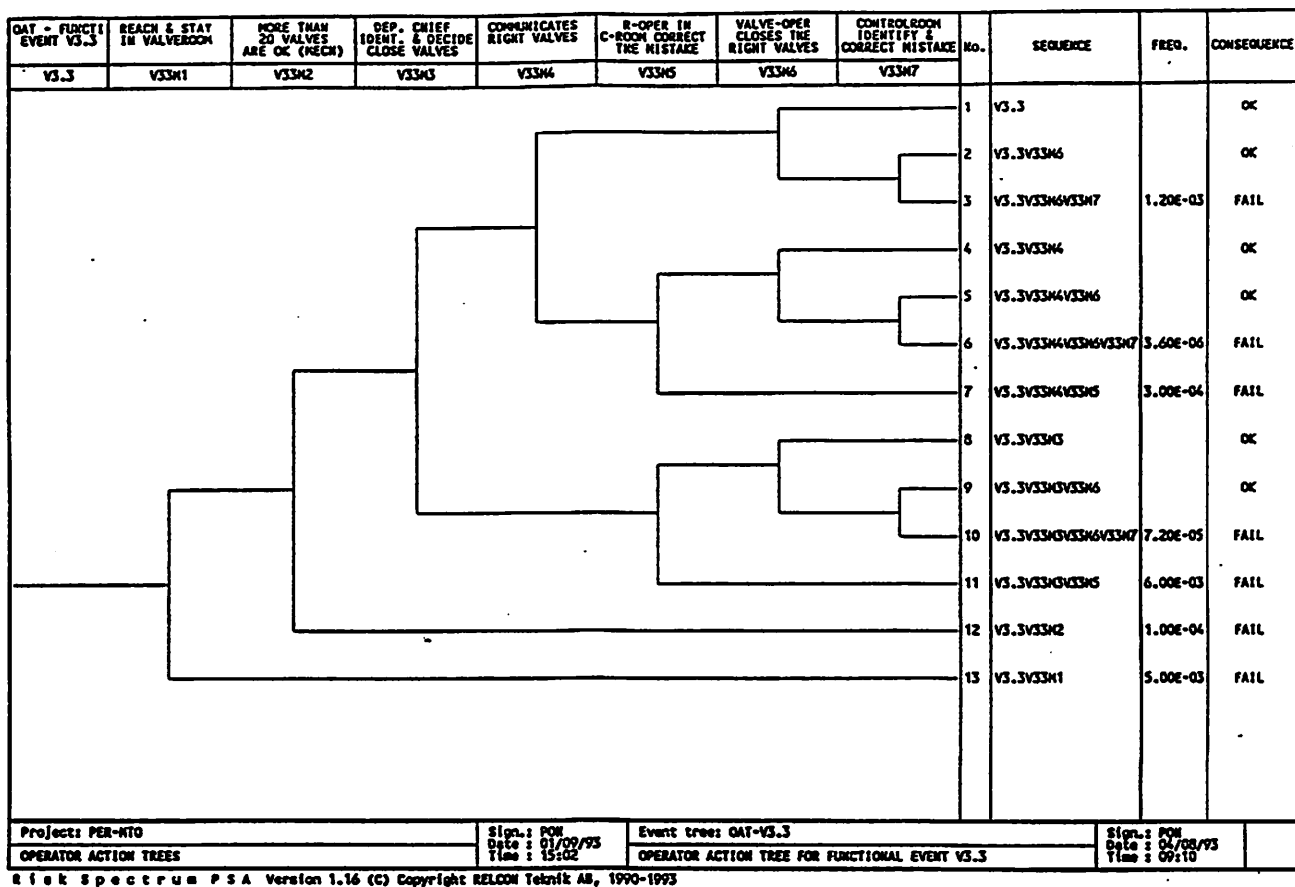


Figure 2

ISSUE	RATE	REMARKS
SYSTEM ADAPTION	4	Alarm (light and sound) for low flowrate and also for high pressure in the GDH-room.
LEVEL OF SKILL OF THE OPERATOR (Education)	4	Examined from Institute, 6-7 years of experience, 3 years as a RO, SSO or MR. Every 3-4 year simulator training (too seldom!), Questions every month.
INSTRUCTIONS	1	Instructions exist, but are not used. The instructions were in bad shape - they should be rewritten and put in order.
TIME FACTOR	4	They have approx. 7 hours to close the valves before they lost too much water, but it could be that they don't act before it's short of time.
MAINTENANCE (What's the condition of the system?)	5	Test of all indicators every shift.
SUBSTITUTER	4	If it's an emergency they substitute the deputy with the supervisor, if it's not an emergency they replace him with a deputy from another shift.
STRESS	2	Noisy, rather dark. In this case it is a serious accident situation, which probably affects the actions.
TOTAL RATE	24	

Figure 3 Event V33M3 (Dep. supervisor identifies and decides to close the valves, type 3)

## **HUMAN ERROR MODEL DEVELOPMENT FOR SAVANNAH RIVER SITE NONREACTOR FACILITIES**

R. E. Vail,<sup>1</sup> S. A. Eide,<sup>2</sup> H. C. Benhardt,<sup>1</sup> J. E. Held,<sup>1</sup>  
and L. M. Olsen<sup>1</sup>

<sup>1</sup>Westinghouse Savannah River  
Company  
1991 S. Centennial Avenue  
Building 1  
Aiken, SC 29803

<sup>2</sup>Los Alamos Technical  
Associates, Inc.  
P.O. Box 51688  
Idaho Falls, ID 83405

### **INTRODUCTION**

As part of an overall effort to improve safety analysis methods for the Savannah River Site (SRS) nonreactor nuclear facilities, a comprehensive human reliability analysis (HRA) methodology has been developed. The HRA methodology covers a wide variety of human errors that may exist in risk analyses of the nonreactor nuclear facilities. Such risk analyses are an integral part of safety analysis reports (SARs) at the SRS, forming the basis for severe accident analysis and assisting in the identification of safety classes for equipment. Nonreactor nuclear facilities at the SRS include nuclear fuel fabrication and reprocessing, nuclear waste processing, and nuclear waste storage and disposal.

The SRS HRA methodology improvement included both adaptation of existing human error models and updating of selected models with SRS-specific data on actual human errors. The data were obtained mainly from four existing SRS data bases: 1) Fuel Processing, 2) Fuel Fabrication, 3) Waste Management, and 4) Reactors. These four are part of the Risk Analysis Methodology (RAM) Fault Tree data banks and the Reactor data bank. Events in these data banks are obtained from a wide variety of sources, including operator log books, occurrence reports, safety newsletters, and others.

Development of the SRS HRA methodology involved a six-step process:

1. Generation of a comprehensive list of human errors applicable to the SRS nonreactor nuclear facilities
2. Adaptation of existing HRA models
3. Collection of SRS-specific human error data

4. Updating of SRS HRA models, using SRS-specific data
5. Independent peer review of the final SRS HRA models
6. Documentation of the methodology.

The first four steps are discussed in the remainder of this paper. Conclusions concerning the overall project are also presented.

## **LIST OF REPRESENTATIVE SRS HUMAN ERRORS**

Risk models of SRS nonreactor nuclear facilities may include initiating event fault trees, event trees, and/or fault trees for event tree top events. These models contain a wide variety of human errors from many different types of facilities. A comprehensive SRS HRA methodology must cover most, if not all, of these types of human errors. Also, this methodology should apply to future nuclear facilities or facility changes at the SRS. The comprehensive list of SRS human errors was developed with both goals in mind.

An initial list of representative human errors was generated using three basic inputs:

1. Review of existing SRS nonreactor SARs to identify human error events in risk models
2. Review of typical human errors being modeled in ongoing SAR upgrade efforts
3. Limited review of actual human errors listed in the RAM Fault Tree data banks (1991 - 1993).

Implicit in the first two inputs is a review of applicable SRS procedures. Given these inputs, a list of approximately 25 representative human errors was generated. This list was expanded to the final 34 events when concerns associated with completeness and applicability to future facilities were addressed. The final list of 34 human errors is presented in Table 1. The list includes typical events such as miscalibration, failure to respond to an alarm, misdiagnosis, and selection of incorrect controls. Also, for waste management facilities there are events associated with manual fire suppression, forklift and crane operations, and transportation.

## **ADAPTATION OF HRA MODELS**

Given the 34 representative human error events in Table 1, an applicable human error model and quantification methodology was desired for each. To accomplish this, a limited survey of HRA practices at other Department of Energy (DOE) sites was conducted. Results of the survey indicated that the Technique for Human Error Rate Prediction (THERP)<sup>1</sup> and Accident Sequence Evaluation Program (ASEP)<sup>2</sup> methodologies were most widely used. Also some limited use has been made of INTENT<sup>3</sup> and Human Cognitive Reliability (HCR).<sup>4</sup>

Model adaptation for the 34 SRS human errors involved choosing one of these four models (or others as appropriate) for each error, identifying the influencing factors that result in different human error probabilities, developing a representative set of

Table 1. Representative human error events.

**Basic**

Failure to notice/respond to an alarm/annunciator/other  
 compelling signal  
 Failure to verify status of instrument in control  
 room  
 Failure to verify status of instrument outside  
 control room  
 Error in selecting or operating a control in control room  
 Error in selecting or operating a control outside  
 control room  
 Communication error  
 Failure of supervisor/checker authorization/verification  
 Incorrect reading/recording of data

**Complex**

Miscalibration  
 Failure to restore following test  
 Failure to restore following maintenance  
 Failure of administrative control  
 Diagnosis error  
 Failure to lock out  
 Chemical addition/elution error  
 Transfer error (transfer liquid to incorrect tank)  
 Overfilling of tank  
 Failure of visual inspection  
 Laboratory analysis error  
 Failure to verify parameter with calculation  
 Incorrect labeling/tagging  
 Failure of manual fire detection  
 Failure of fire suppression by occupant  
 Failure of fire suppression by non-occupant  
 Random actuation/shutdown of system  
 Failure of accident recovery over hours or days  
 Vehicle collision with stationary object  
 Single vehicle accident during transportation  
 Vehicle collision with another moving vehicle  
 Dropping of load when using forklift  
 Puncturing of load with forklift forks  
 Dropping of load when using hoist/crane  
 Impact of hoist/crane with stationary object  
 Excavation errors

three probabilities (low, medium, and high) to cover these influencing factors, and providing guidance for deciding which value is appropriate for the application in question. Results of this process for five of the 34 SRS human errors are presented in Table 2. The generic human error probabilities presented in the table reflect SRS practices, where appropriate, but do not reflect actual SRS experience.

Calculation of the three probabilities for each human error depended on the model used. In some cases the three human error probabilities came directly from tables associated with a model. In others, some representative influencing factors or recovery factors had to be specified to obtain the probabilities. Each of the three probabilities is meant to be a mean value for a specific application. The three values are not meant to be different percentiles of a common distribution.

Table 2. Selected SRS human error models and data.

SRS Human Error	HRA Model Used to Determine Generic Human Error Probabilities	Generic Human Error Mean Probability (low, medium, and high)	SRS Data	SRS-Specific Human Error Mean Probability (low, medium, and high) <sup>a</sup>
Failure to restore following maintenance	THERP	1.0E-3, 5.0E-3, 5.0E-2	14 events in 2822 restorations	1.0E-3, 5.0E-3, 5.0E-2
Failure to lock out	Basic Human Error	5.0E-4, 5.0E-3, 3.0E-2	53 events in 92,718 lockout plans	5.0E-5, 5.0E-4, 3.0E-3
Random actuation/shutdown of system	Simple Model	1.0E-6/h, 1.0E-5/h, 1.0E-4/h	2 events in 340,389 hours	5.0E-7/h, 5.0E-6/h, 5.0E-5/h
Laboratory analysis error	THERP	5.0E-5, 5.0E-4, 3.0E-2	20 events in 772,000 analyses <sup>b</sup>	5.0E-6, 5.0E-5, 3.0E-3
Dropping of load when using hoist/crane	Generic data	1.0E-5, 1.0E-4, 1.0E-3	1 event in 25,615 operations 2 events in 9,450 operations 1 event in 850 operations	3.0E-5, 1.0E-4, 1.0E-3 <sup>c</sup>

a. Obtained by using a Bayesian update, with the generic model medium value as the prior and the SRS-specific data as the evidence.<sup>6</sup> The results were rounded to 1, 3, or 5 times the appropriate power of ten. The low and high values were adjusted based on the change seen in the medium value from the Bayesian update, unless otherwise indicated.

b. These data involve incorrect laboratory analysis results that were used by operations personnel.<sup>6</sup> It was assumed that the operations personnel detect one-half of the incorrect laboratory results before use. Therefore, the actual number of incorrect analyses was assumed to be 40.

c. The first set of data was used for the update of the low generic value, the second set of data for the medium value, and the third set of data for the high value.



## COLLECTION OF SRS-SPECIFIC HUMAN ERROR DATA

Human error data at the SRS were collected by performing searches on the RAM Fault Tree data banks or the Reactor data bank to determine the numbers of events and by interviewing operations personnel to estimate the numbers of opportunities for such errors. Results are summarized in Table 2 for selected human errors. Based on the interviews with operations personnel, the actual numbers of events may be as high as twice that reported in the data banks. This underreporting is mainly the result of differing requirements for the data banks compared with this project. Also, the estimates for numbers of opportunities were estimated to have an uncertainty range of plus or minus fifty percent.

The SRS-specific data were not used directly to obtain human error probabilities. Rather, the data were used in a Bayesian update process as explained in the following section.

## UPDATING OF SRS GENERIC HRA MODELS

The SRS-specific human error data were used to update the HRA models and error probabilities shown in Table 2. As an example, for the failure to lock out (second entry in Table 2), the SRS data indicate 53 such events in 92,718 lockout plans. Not enough events with detailed descriptions were identified to try to determine the impact of influence factors on the human failure probabilities. However, the SRS data were used in a Bayesian update process, using the medium generic estimate as a prior, assuming a beta distribution for the prior and an error factor of ten.<sup>5</sup> The magnitude of the change in the generic estimate caused by the Bayesian update (a factor of ten increase) was also applied to the low and high generic failure probabilities. The results were then rounded to 1, 3, or 5 times the appropriate power of ten.

For some of the human errors, the SRS-specific data were detailed enough to apply the Bayesian update to all three of the probabilities (low, medium, and high). An example is the dropping of a load when using a crane or hoist (fifth entry in Table 2). In these cases, the data provided information to adjust the effects of influencing factors. However, for most of the human error probabilities, the SRS-specific data were not detailed enough to determine whether the spread between the three probabilities was appropriate; i.e., whether the impact of the influencing factors was appropriate. In such cases, however, the data were still used to determine the impact (change caused by the Bayesian update) on the medium value.

## CONCLUSIONS

The SRS HRA model development has resulted in a set of three human error probabilities for each of the 34 representative human errors. In addition, approximately one-half of the probabilities were modified based on SRS-specific data. This site-specific data collection was important, because the data resulted in up to a factor of twenty change in the generic model results. However, most of the SRS-specific data agreed well with the generic model results. The data collection was not, in general, detailed enough to discern impacts of influence factors on the probabilities.

## ACKNOWLEDGEMENT

This work was supported by the U.S. Department of Energy under Contract Number DE-AC09-89SR18035.

## REFERENCES

1. A.D. Swain and H.E. Guttman, *Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Operations: Technique for Human Error Rate Prediction*, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, D. C. (1983).
2. A.D. Swain, *Accident Sequence Evaluation Procedure (ASEP)*, NUREG/CR-4772, U.S. Nuclear Regulatory Commission, Washington, D. C. (1987).
3. D.I. Gertman et al., INTENT: a method for estimating human error probabilities for decisionbased errors, *Reliability Engineering and System Safety* 35:127-136(1992).
4. G.W. Hannaman et al., *Human Cognitive Reliability Model for PRA Analysis*, NUS-4531 (draft), NUS Corporation, San Diego, CA (1984).
5. *PRA Procedures Guide*, NUREG/CR-2300, U.S. Nuclear Regulatory Commission, Washington, D.C. (1983).
6. W.C. Perkins, The Probability of Process Laboratory Errors Affecting Reprocessing Operations, *Advances in Human Factors in Nuclear Power Systems*, American Nuclear Society, La Grange Park, Illinois (1986).

## **BENCHMARKING AN AUTOMATED HUMAN ERROR ANALYSIS TECHNIQUE**

James R. Wilson, Priya Cloutier, Steve Fogarty

Westinghouse Idaho Nuclear, Inc.  
Box 4000, MS-3212  
Idaho Falls, Idaho  
83403

### **BACKGROUND**

Problems have been experienced using THERP<sup>1</sup> (Technique for Human Error Rate Prediction), one of the more popular procedures used to quantify human reliability. Results can be in error if THERP is utilized by an analyst who has not had formal training in both human factors and THERP.

This problem was demonstrated in 'benchmarking exercises' performed by the Commission of the European Communities,<sup>2</sup> using THERP. The exercises consisted of several teams of analysts independently modeling reactor failures due to human error. The results using THERP varied by almost four magnitudes from team to team. (This variance may be due to a lack of certified THERP training).

The need for a simpler technique for human reliability analysis was recognized by the Nuclear Regulatory Commission (NRC) years ago. Their request was for a simpler technique to provide estimates of human error probabilities (HEPs) for the analyst with no human factors training. Hence, a new technique was developed as part of the NRC's Accident Sequence Evaluation Program (ASEP).<sup>3</sup>

The ASEP procedure consists of a set of questions the analyst must answer to model an event. In 1989, Westinghouse Idaho Nuclear Company Inc. (WINCO) computerized ASEP.

### **WINCO-ASEP**

The Idaho Chemical Processing Plant (ICPP) at the Idaho National Engineering Lab (INEL) near Idaho Falls, Idaho, handles and conditions spent nuclear fuel in a human factors environment similar to an industrial processing plant. Only small amounts of stored energy are present in the process, limiting post-accident mitigation needs to primarily passive filtration. Almost no time stress exists: the main post-accident operation is evacuation. For this reason, the WINCO-ASEP emphasized pre-accident tasks, defined

as "routine and corrective maintenance, calibration, surveillance tests and restoration (e.g., returning to operational status)". This pre-accident methodology has also been applied to the routine operational tasks (e.g., no high stress) encountered at the ICPP facility. Pre-accident tasks involve primarily rule-based behavior, and response time is generally not a factor.

During a PRA (Probabilistic Risk Assessment) in which the computerized version of ASEP was being used, the issue came up of proving that WINCO-ASEP always presented results which were defensible, that is, more conservative, than THERP. That was the motivation for this study.

In theory, ASEP always produces numbers that are conservative compared to THERP. This is because ASEP always assumes errors of commission and errors of omission. Further, ASEP does not take credit for all recovery factors that may affect how a plant is stabilized from an accident state. However, nonconservative results were discovered.

Upon closer examination, it was discovered that these nonconservative results were not software or methodology problems, but the analyst misunderstanding the application of ASEP. This prompted a search for those concepts needing further attention in the training manual in order to avoid this misapplication.

## **INDEPENDENT BENCHMARKING**

Five Department of Energy (DOE) contractors (WINCO, EG&G Idaho, Hanford, Sandia National Lab and Idaho State University) participated in this benchmarking exercise. This study was double-pronged: To assure that theoretically ASEP was always more conservative than THERP, and when in practice, THERP was more conservative, determine the cause. These findings were used to update the user manual to minimize misapplication in the future.

## **TYPES OF ERRORS**

In exercising the WINCO-ASEP, the following notes were made:

- 1) Since the WINCO-ASEP involves pre-accident tasks, post-accident tasks should be avoided. For example, if an alarm is present, ASEP assumes a negligible HEP. Also, when using THERP as a check, avoid the post-accident tables.
- 2) Some of the analysts used incomplete HRA (Human Reliability Analysis) event trees to analyze the pre-accident tasks. Where the fully developed tree would have had failure paths branching off from a success branch (i.e., the operator could get into trouble after the initial success), this inadequate development resulted in a nonconservative analysis.
- 3) Some discrepancies resulted from incomplete system understanding. This was not so much the fault of the analyst, but an incomplete specification of the scenario (some of the scenarios were "manufactured", and too much system background was assumed).
- 4) ASEP assumes operator involvement in the initial error. For example, an operator may be doing an operation that sounds an alarm upon his error. Conversely, the system may have a component fault that pushes it outside some alarm point. The analyst must decide if the alarm is a recovery factor for an operator error, or an alert

to the operator of a system error. For the first event, the WINCO-ASEP correctly evaluates both the operator error and the alarm. ASEP should not be applied to the second task.

5) ASEP assumes all operators and supervisors in a task are assessed at once. For example, if an operator and checker are involved in a task, only one ASEP HEP is generated. Nonconservatism results if ASEP is used to generate a separate "checker HEP" to multiply with the "operator HEP".

6) Because the WINCO-ASEP is simplified, credit could not always be taken for all the recovery factors in a scenario. This caused many different scenarios to have the same basic description and HEP, frustrating the analysts using the code. The user needs to realize this is one of the prices paid for the simplicity.

7) Series and parallel were sometimes confused. For example, redundant pumps are in parallel for system operability, but in series for leakage scenarios.

8) The supervisor was sometimes given too much credit. In order to credit the supervisor, he must function much like a checker, being able to monitor all critical actions taken by the operator. For example, no credit can be taken for a supervisor signature if the supervisor was not present to observe the critical action.

These observations should be fairly obvious to a person trained in HRA. However, since ASEP is designed for the nonHRA user,<sup>1</sup> these basic issues must be spelled out prior to use of the code.

## RECOMMENDATIONS AND CONCLUSIONS

Based on this exercise, the following changes were made to the users manual for the WINCO-ASEP at the ICPP:

- 1) Use only on pre-accident tasks. Also, ensure that the task developed by ASEP involves the initial operator error and all personnel immediately involved with that task.
- 2) Additional examples of the use of HRA event trees are included to help the analyst be thorough.
- 3) Additional hints on system walkdowns and interviewing (talkthroughs) are given to the analyst to ensure complete system understanding.
- 4) The user is warned about the tendency of ASEP to coalesce many scenarios into a limited subset (i.e., limiting the analyst's desire to express the complexity of the scenario).

---

<sup>1</sup> ASEP is not endorsed for a nonHRA user working alone. HRA expertise is assumed to be available to the nonHRA user. Hopefully, being sensitized to the pitfalls derived by this study, the nonHRA user may better know when to call upon the expert.

In addition to helping us discover and formulate these changes, this benchmarking exercise demonstrated that WINCO-ASEP does indeed yield defensible results, when used properly.

## REFERENCES

1. A. D. Swain, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", NUREG/CR-1278 (1983).
2. A. Poucet, Insights from the Benchmark Exercises and Impact on Methodological Development, *Reliability Engineering and System Safety*, Vol. 31 (1991), pg. 65-90.
3. A. D. Swain, "Accident Sequence Evaluation Program, Human Reliability Analysis Procedure", NUREG/CR-4772 (1987).

## ASSESSMENT OF DEPENDENCE OF HUMAN ERRORS IN TEST AND MAINTENANCE ACTIVITIES

Lasse Reiman  
Finnish Centre for Radiation and Nuclear Safety (STUK)

### INTRODUCTION

When analyzing the behaviour and error possibilities of NPP personnel main attention has often been focused on the operating crew in the main control room. This is justified, taking into account their central role in managing accidents. Their chances of succeeding might be worse, however, if there are latent equipment faults at the plant as a consequence of test and maintenance activities. In several studies it has been shown that test and maintenance errors made by personnel working outside the control room have comprised a noticeable percentage of all human errors.

The aim of this study has been to evaluate human errors which take place in connection with regular test and maintenance activities. Errors that are specifically studied are of a type that have a possibility to go unnoticed (latent) at least until the next regular test or the next refuelling shutdown.

The dependence of errors between tasks performed in redundant subsystems of a safety system is the most important issue when the safety significance of human errors related to test and maintenance activities at NPPs is considered. Dependence between errors has been studied in psychological tests that are not related to nuclear applications. A clear indication of a learning process is presented by Kay (1951) who stated that persons learned to repeat the errors that they had performed. The results of this study were attempted to be verified in another study reported by Holding (1970). The hypothesis of error learning received limited support.

Spettell (1986) presents results of a laboratory experiment using small-scale simulators the purpose of which was to validate the MSF model and to examine the relationship between psychological and behavioral characteristics of individuals and their performance. In the experiment students especially trained for the tasks were used. In general, the results of the test showed that there was convergent evidence that dependent sequential errors do occur. The results also indicated that there were relatively stable individual differences in the performance of the tasks.

Lucas (1987) describes an analysis of dependent failures in order to identify their major psychological root causes. A classification scheme of human failures was first devised for the study. The first stage of classification is based on the three levels of human performance proposed by Rasmussen. Whenever feasible, more specific categories

of error were devised for each of these first stage classes. The database of the study consisted of 53 dependent and 36 independent errors from LERs and periodic maintenance reports prepared for the NRC. Each of these human errors was classified using the devised classification scheme. There were no differences between events classed as dependent and those identified as independent in terms of the distribution of different types of human error. The highest proportion of failures occurred at the skill-based level (49,4 % of all events). The next most frequent category were errors at the knowledge-based level (16,9 %). Errors at the rule-based level occurred in 10.1 % of the events. In the second stage classification of skill-based behaviour the dominating class was omissions (63,6 %).

The method most often used to assess dependence presented in Handbook (Swain & Guttman, 1983) is oriented towards operator actions in control room and is, as such, not suitable for assessing dependence during test and maintenance activities. The Multiple Sequential Failure method (Samanta et. al., 1985) is mathematically more advanced but it does not give any guidance for the evaluation of the dependence factor in practice.

In this study the dependence of test and maintenance errors was assessed in two ways: (1) by reviewing the operating experiences at Finnish NPPs, and (2) by an expert judgment exercise. When using expert judgment methods, special attention has to be paid to the point that the experts have the prerequisites for making the judgments required. Therefore it is often better to use methods that do not presuppose a direct quantification of human error probabilities. The starting-point in the study was that experts are only asked to make comparisons between error probabilities. Also practical limitations have to be taken into account. This includes the number of experts available and the nature of their expertise. Based on a critical review of methods, Paired Comparisons and Ranking methods were chosen for this study.

## ASSESSMENT OF DEPENDENCE BASED ON OPERATING EXPERIENCES

As the operating experiences gained at the Finnish NPPs were analyzed, all the quarterly reports published by the regulatory body were reviewed from the beginning of 1982. Attention was focused on those cases that included a human error in testing, repair or preventive maintenance or an equipment left in a wrong state after these activities. Also corresponding incident reports by the utility were reviewed in these cases. Only a small number of dependent errors were found. Although the number of cases is small, the incident reports are detailed enough to permit a detailed study of these cases. To review the different dependence models, the dependent errors were classified on the basis of the time between successive tasks in redundant subsystems. The time between tasks was divided in six classes. In Table 1 these classes and the number of cases in each class are presented.

As it is evident that only a fraction of all human errors in test and maintenance activities have been reported to STUK, the database cannot be used for quantification purposes. However, the results can be used to qualitatively review the basis of the dependence models of Swain. These models are more useful when evaluating dependence in control room activities. The models cannot be used to assess test and maintenance activities because the time limit proposed in the models is too restricting. In seven cases the dependent error occurred in spite of both time and spatial separation of the tasks in redundant subsystems. An important finding is that a large part of dependent errors is related to modifications of the plant. These failures cannot be identified in PSAs and, thus, comprise an additional risk for the plant.

In the next phase of the study the data provided in the failure reports of one Finnish utility were reviewed. The data collection systems at Finnish NPPs are well developed and provide good possibilities for this kind of work. The utility provided a list of all failure



Table 1.

Class	Time difference	The number of cases
1	< 5 min	3
2	5-30 min	3
3	30-60 min	2
4	1-8 h	0
5	> 8 h	4

reports in which the cause of the failure was related to either operating or maintenance personnel performance or to procedures. The list covered the whole operating history of the plant. The information received from the utility was used to identify human errors that may have affected different subsystems of a system.

A starting-point in the identification was to look for dependencies only inside systems (between subsystems) to simplify the identification procedure. In a preliminary selection phase candidates for dependent failures were chosen based on equipment codes, times and dates of the starting of the work and codes for the cause(s) of the failures. The final selection of dependent failures was in most cases based on qualitative description of the failure and on remedial action. It turned out that the qualitative descriptions of failures were rather complete in the database and, thus, the identification could be done reliably. In addition to dependent failures, all omission errors and errors of a type "mistakes among alternatives" were identified. This information was used also as a basis for the selection of cases for the Paired Comparisons case study.

From the database 33 dependent human errors were identified in the first phase. In the second phase of the identification, a list of dependent errors was delivered to the utility, where experts from different maintenance areas made an assessment of the causes of errors and their nature. Then all the identified cases were discussed by the author and representatives from the maintenance department. Based on this review seven of the candidate cases could be excluded from the final list. The identified dependent error cases were classified using a simplified form of the scheme presented by Lucas (1987). The results of the classification are presented in Table 2. The number of dependent failures is only a small fraction of all the failures analyzed.

The design errors were errors made by other than test and maintenance personnel of the plant and were therefore separated from other cases. They were made partly in the original design phase and partly in designing modifications of the plant. Also in the class "omissions" two cases were related to the returning of equipment into correct state after a modification. If only errors made by the plant personnel are examined, 80 % of dependent errors have taken place at the skill-based level. Dependent errors at the knowledge-based level occurred in 15 % of the cases. The results have been used also to estimate the dependence factor for the abovementioned types of errors using the moment method.

An attempt was also made to identify errors in those independent tests or inspections that should have prevented dependent errors from occurring. This identification usually had to be based usually only on assumptions about inspections that should have taken place. In 10 cases it was assumed that such a connected error must have taken place. However, there are large uncertainties in this identification. In five cases they were related to deficient quality control and in three cases to plant start-up inspections after refuelling maintenance. General quality assurance deficiencies were found in two cases.

**Table 2. Classification of identified dependent failures**

Class	Number of cases
<b>Skill-based errors</b>	
• mistakes among alternatives	3
• omission	7
• carelessness	6
<b>Rule-based errors</b>	1
<b>Knowledge-based errors</b>	3
<b>Design errors</b>	6

The results of the study indicate that dependent human failures occur at NPPs but their contribution to the total amount of failures is minor. On the other hand, their safety significance may be notable once they occur. The results indicate that there is not a clear timely trend in the amount of dependent human errors per year. The information in the database is not detailed enough to evaluate, which factors have, in each case, contributed to the dependence. Therefore, the results cannot be used to evaluate the causes of dependent errors.

The great percentage of skill-based errors and the relatively large amount of connected failures point out that increased attention should be paid to the motivation of maintenance and inspection staff so that the likelihood of dependent errors would be minimized. Increased attention should be paid to work procedures and work permits to avoid omissions in routine tasks.

## PAIRED COMPARISONS EXERCISE

In the other part of the study the dependence of selected test and maintenance activities at Finnish NPPs was studied using expert judgment methods. A detailed qualitative analysis was done concerning 12 cases and detailed descriptions of the cases were prepared. The factors that contribute to the dependence of errors were identified and described. Photographs were taken at the plant to be able to further demonstrate the cases to experts. Six experts were selected for the exercise from the Finnish Technical Research Centre (VTT) and the regulatory body (STUK).

Three tasks were given to the experts. Task A was an assessment of the human error probabilities of the 12 test and maintenance actions using the Paired Comparisons method. Task B was an assessment of the dependence of human errors in the same cases, also using the Paired Comparisons method. Task C was an assessment of the dependence of human errors using the Ranking method. The Paired Comparisons method was modified in task B so that the experts were asked to explain the arguments of every judgment. The purpose of this modification was to guarantee a careful consideration of every comparison and to make it possible to study afterwards the experts' reasonings.

The cases were so arranged that in every comparison neither of the cases were the same as in the previous comparison. The purpose of this arrangement was to make the comparisons as independent as possible. All experts performed the tasks and the comparisons in the same sequence.

In paired comparison judgments, the experts may exhibit internal inconsistencies that

are shown as circular triads. The consistency of an expert is determined using "the coefficient of consistency" by David (1963). Statistical tests of the calculated coefficients showed that they were all significant at 1 % confidence level. The internal consistencies of the judgments were analyzed also by examining the correlation of the results of tasks B and C for each expert using the Spearman rank correlation coefficient. Also these correlation coefficients showed that the judgments were internally consistent. The coefficient of concordance was used to measure to what extent there was agreement between the experts' judgments. The between-expert agreement of the results of the whole group (all experts) was statistically significant at 5 % confidence level in tasks A and B. In task C the agreement was worse. The coefficient of concordance was calculated, in addition to the group of all experts, for some smaller sub-groups. Smaller groups were established using two principles: on one hand based on the organization that the experts came from and, on the other, on their field of expertise.

By examining the quantitative results one can notice that the between-expert agreement in tasks A and C was better in the expert group representing the regulatory organization than the research organization. In task B the results were comparable. Considering the other two subgroups one can further notice that in all tasks the between expert agreement was better in the quite heterogenous group "others" than in the group of reliability engineers. The arguments that different experts had presented were studied to find explanations for these findings.

On the basis of the results it is possible to assess the sources of correlation between experts and compare the results with the findings of Meyer and Booker (1987). In accordance with Meyer and Booker, the basic education of experts obviously was not an important source of correlation. The latest working experiences seemed to have some effect on the judgments. Another factor, that is not mentioned by Meyer and Booker, is the values and attitudes prevailing in the organization, i.e. cultural factors. These factors have a tendency to unify the judgments of experts from an organization where a strong culture exists. It can be hypothesized that the general attitude in the regulatory organization concerning the importance of procedures and their high quality had an effect on the judgments made by STUK's experts. The results thus point out that the background characteristics of the experts, especially the cultural factors of their organization, may be a source of correlation between the experts.

As concerns the quantitative results of the study, the scale values were calculated using a procedure described by Seaver and Stillwell (1983), which is based on condition C of Torgerson (1958). Calibration was done based on the fact that for small base error rates the dependence factor is close to the conditional human error probability of the second sequential task. The quantitative results of tasks A and B were found to be sensible to the calibration points used. The dependence factors for typical test and maintenance activities were found to lie between 0,15 and 0,25. The estimation of the dependence factor using the moment method based on an analysis of the failure reports of one Finnish utility supported the assumptions used in the calibration of the results.

As a conclusion of the exercise it can be noted that the within-expert consistency was rather good and the between expert agreement was also statistically significant in two out of three tasks. The cases could be reasonably well separated from each other. The modification of the method in task B made it possible to obtain information which is also qualitatively useful and which can be used to develop administrative and technical procedures at the power plants. All the results of the study indicate that the experts were well motivated and made careful judgments.

## REFERENCES

- David, H.A., 1963, The method of Paired Comparisons. Hafner, New York.
- Holding, D.H., 1970, Repeated errors in motor learning. *Ergonomics*, Vol. 13, No. 6.
- Kay, H., 1951, Learning of a serial task by different age groups. *Quarterly Journal of Experimental Psychology*, 3.
- Lucas, D.A., 1987, Human errors causing dependent failures in nuclear power plants: a database, taxonomy and analysis. *Reliability '87*.
- Meyer, M.A., Booker, J.M., 1987, Sources of correlation between experts: Empirical results from two extremes. NUREG/CR-4814. Los Alamos National Laboratory. U.S. NRC.
- Samanta, P.K., O'Brien, J.M., Morrison, H.W., 1985, Multiple-Sequential Failure Model: Evaluation of and procedures for human error dependency. NUREG/CR-3637. Brookhaven National Laboratory, U.S.NRC.
- Seaver, P.A., Stillwell, W.G., 1983, Procedures for using expert judgment to estimate human error probabilities in nuclear power plant operations. NUREG/CR-2743. US. NRC.
- Spettell, C.M., 1986. The application of laboratory data from small-scale simulators to human performance issues in the nuclear industry. *Proceedings of the International Topical Meeting on Advances in Human Factors in Nuclear Power Systems*. Knoxville, Tennessee.
- Swain, A.D., Guttman, H.E., 1983, Handbook of human reliability analysis with emphasis on nuclear power plant applications (Final report). NUREG/CR-1278. Sandia National Laboratories, New Mexico.
- Torgerson, W.S., 1958, Theory and Methods of Scaling. John Wiley & Sons, New York.

**074 Comparative Risk Assessment of Complex Technological Systems  
(II)**

*Chair: S. Hirschberg, P. Scherrer Inst.*

**Comparative Assessment of the Health and Environmental Impacts of Various Energy Systems from Severe Accidents: Issues in Review**

*A.V. Gheorghe (ETH, Switzerland)*

**Consideration of Probabilistic Safety Objectives in OECD/NEA Member Countries**

*M.F. Versteeg (Nucl. Safety Insp., Netherlands)*

**Risk Assessment of Large Industrial Complexes in Eastern Europe: A Comparative Prospective**

*A.V. Gheorghe (ETH, Switzerland)*

## **COMPARATIVE ASSESSMENT OF THE HEALTH AND ENVIRONMENTAL IMPACTS OF VARIOUS ENERGY SYSTEMS FROM SEVERE ACCIDENTS: ISSUES IN REVIEW**

**Adrian V. Gheorghe**

Swiss Federal Institute of Technology - ETH  
Polyproject "Risk and Safety Technological Systems"  
ETH Zentrum, 8092-Zurich  
Switzerland

### **BASIC DEFINITIONS, METHODOLOGICAL ISSUES, AND INDICATORS**

#### **Basic Definitions**

It is already agreed that the potential for severe accidents exists for most energy systems - fossil, nuclear and renewables-at various stages of their fuel cycle. The main issues associated with the comparative risk assessment of health and environment from severe accidents of different energy systems and fuel cycles can be summarized as follows:

- i) The consequences of severe accidents in isolation are not a good base for risk comparison. The likelihood (or probability) of occurrence should also be considered into the overall comparative assessment process. It is difficult to assess and compare the frequency of such accidents, because such data are not systematically collected.
- ii) The lack of methods, information and data concerning the indirect and delayed health effects or long term environmental impacts from severe accidents associated with different energy generation systems is recognized. Assessment results are often limited to immediate/acute health effects, which make a complete comparison difficult.
- iii) There is a need to re-think the current methods of presenting the results of comparative risk assessment for severe accidents from different energy sources, so as to ensure that all elements of risks are included. It may not be appropriate in all cases to present the comparison results on a normalized per unit of energy basis. Alternative and complementary indicators of comparison may need to be developed.
- iv) Variations in technologies and possible future technological developments of different energy systems generates special problems to be solved in the comparative risk assessment process for severe accidents.

Consideration of energy sources is restricted in this paper to those systems which lead to electricity production. After they were agreed and defined the boundaries of the systems delineated in order to allow an equitable risk type comparison. The distinction between 'severe' and other accidents is somewhat arbitrary. Other studies in the literature are directed to comparative risk assessments in normal operation. An important point is that when comparisons are being made between different energy systems the risks from both normal operation and 'severe' accidents have to be considered together. In the recent international practice three groups of energy sources for the generation of electricity are considered: fossil fuel, nuclear and renewable. Methodologies and data base structures should be made flexible.

to accommodate additional energy sources if such sources became significant contributors to electricity generation. According with some already agreed definitions, one can summarize:

**Definition 1:** An undesired event is considered as severe accident if has the potential to cause any of the following: i) ten or more deaths or serious injuries; ii) evacuation of more than 200 people; iii) a ban on consumption of locally produced food or drinking water; iv) the enforced clean-up of more than 25 km<sup>2</sup> of land or water; v) the enforced clean-up of more than 10 km of shoreline or river; vi) a direct economic loss of more than 10 million dollars.

As an aide to decision making it is helpful to evolve a set of performance indicators in order to make comparative assessments. It is important to recognize that not all aspects of severe accident analysis are amenable to quantification. There will always be a need to retain some qualitative inputs to comparative assessment and the decision making process, mainly in the field of environmental impacts.

**Definition 2:** Energy systems comparative risk assessment is an interdisciplinary field of knowledge of engineering, environmental, health, economics and social sciences, focusing on identifying indicators, data, information, knowledge and a consistent methodological framework in order to (objectively) compare various type of risks (e.g. health, environmental, economic) in view to assist and implement (in the decision making process and its political congruence), a rational and "risk acceptable" energy - environmental policy.

Care must be taken in using data from a 'severe' accidents database or any other source as an input into a comparative risk assessment study. The data available usually have orvarying degrees of depth, quality and usefulness. Some data will be of immediate application, e.g. the number of miners killed in a mine disaster. Other data will be purely indicative (e.g. the number of fish were killed). This will require further investigation before being capable of being used in a comparative risk assessment.

**Remark 1:** Acquisition of data on severe accidents: a high quality database will only be constituted if those responsible for maintaining the database play an active part in seeking out data and following up in detail all reports of severe accidents.

### Methodological Issues

**Remark 2:** The main methodological issue in conducting a comparative risk assessment for severe accidents is consistency in the definition of the boundaries of the energy systems and the indicators used as a measure of risk. In theory, there is a potential for a severe accident to occur at each stage of an energy chain. In reality, the operation of only a few technologies can result in a severe accident.

Practical considerations say that only the primary technologies should be included within the boundaries set up (e.g. the process of manufacturing solar cells for photo-voltaic system would be included, not the process involved in the manufacture of the metal components used in the construction).

**Remark 3:** Limits in time, space, and risk should be placed in a equitable way between energy systems. In some cases assumptions in comparative risk assessment can be made to allow for estimates of impacts to be made for 10 000 years into the future; in other cases the assessment is not done due to lack of information. A detectable impact is not necessarily significant. The determination of a *de minimis* or trivial risk level is necessary; below this level the impacts would not be considered.

For health indicators the *de minimis* level suggested was the individual risk of death of 10<sup>-7</sup> to 10<sup>-6</sup> in a small group. For a large population potentially exposed to different sources of risk the level covered be set a factor of ten lower. For environmental indicators the *de minimis* level could be set as background levels before the accident or if the data is known, the level below which no harm occurs. These levels would be set on a site specific and/or risk acceptable basis.

## Indicators

The indicators that are used in the assessment of severe accidents should be the same as those used to quantify the impacts of normal operation of the technologies. They can be classified as: health impacts, environmental impacts, economic impacts, social factors.

Health indicators are mainly mortality and morbidity. Methodologies exist for economically value such impacts. Mortality can be reported in terms of immediate death or delayed effects resulting in death, (such as fatal cancers occurring after a latent period); one measure of this is Years Of Life Lost, (YOLL). Morbidity is measured in number of injuries; for the general public / workers these effects can be reported as numbers of injuries, Quality Adjusted Life Year (QALY) or for the working population only as Working Days Lost (WDL).

Environmental indicators for effects of severe accidents proves difficult; area of land, number of species and concentration in the receptor medium, (e.g air, water and soil) are clearly defined, but the information is not always available. When they are available, these indicators can be economically valued. Non-quantifiable impacts such as loss of quality, disturbance of the ecosystem and genetic deterioration should also be considered for environmental impacts. These are difficult to measure and may not be obvious at the time of the accident. One suggestion is to quantify an incremental change from the base line level before the accident has occurred.

Economic impacts includes the group of consequences in severe accidents that can only be measured in monetary terms. (e.g. the clean-up and decommissioning costs, the costs of the evacuation of the population surrounding the area of the accident ).

The social impact of severe accidents has been documented as important. This category falls into the group of indicators that are important to consider in the overall comparative analysis but may not be possible to quantify in the same manner as the other consequences (e.g. the risk aversion factor, psychological impact on the population).

**Remark 4:** For the case of electricity generation, the reporting of the indicators should be normalized to the amount of electricity generated. If this is not applicable a common ground must be found. The common denomination of cost can be used when normalized per unit energy produced, (e.g GW(e)a).

**Time and Space Dimensions:** For comparison purposes it is important for the time and space (local, regional, global) of occurrence to be taken into account. There are difficulties in setting very rigid definitions for these dimensions. The two dimensions of time and space that require further discussion in terms of severe accidents are short term and regional. There are many cases where the short term impacts can be on the order of a few hours. It is considered important to indicate a distinction between a few thousand people evacuated for a few hours and a few people evacuated for a few months. Within the short term category a sub-category of impacts on a hourly basis should be established. For regional effects an important factor will be the impacts resulting as a consequence of crossing national borders. An indication of this in reporting the results will prove useful in the analysis of the information.

## THE SOURCE OF DATA AND USE OF DATABASES

A database for comparative risk assesment (normal operation and severe accidents) to assess and compare the frequency of the health and environmental effects of such events/accidents is currently under development of a number of UN and other international organizations. Health effects in cases of severe accidents are generally only reported in terms of immediate fatalities, immediate injuries and details of evacuation when large numbers of people are involved. The ultimate long term environmental effects are difficult to assess. Because of the single occasion or very infrequent exposure of ecosystems to releases from severe accidents, it may be difficult to establish if the effect is irreversible or whether recovery may be taking place. This is not to say that data does not necessarily exist, some data are



known to exist, other data will have been collected by authorities not directly concerned or connected with the accident i.e., medical records, environmental health monitoring authorities, agricultural and fishery departments, water authorities etc. The main problem is that data has not been collected and analyzed in a systematic manner with a view to using it in the context of dealing with the comparative aspects of severe accidents. It should be recognized that there are two broad categories of data, those which are based on historical (actual) occurrences and those based on predictions of likely future events. It is important that data based on historical events is not compared directly with those based on predictions. The quality and quantity of the data available on the health and environmental effects of severe accidents from different energy sources varies significantly. Generally it can be said that the greater the impact of a severe accident then, at least in recent times the data improves in both quality and quantity. However, there is still the major problem that all the data relevant to any particular accident is never collected together and systematically analyzed with reference to the accident.

### **The Application of Data**

The areas of application of a specialized database on the health and environmental effects of severe accidents are: as an input to comparative risk assessment studies of different energy systems; as a source of information on health, environmental impact assessment and the true cost of severe accidents; as a data source for developing countries, i.e. to provide a yardstick by which to compare with their own activities at any stage of a particular energy source fuel cycle; as a data source for the mitigation effects due to the response of the various authorities who have responsibility of dealing with the post-accident stages of a severe accident; as a means of comparison with predictive studies carried out on the same or similar types of installation; as a factual means of convincing governments, agencies, utilities that predicted, very unlikely severe accidents can and do occur.

### **Requirements of a Comparative Risk Assessment (severe accidents) Database**

A prime consideration in defining the broad requirements of a comparative risk assessment (severe accident) database is that the number of input fields should be restricted to those field which have a high probability of being provided with useful information. The essential requirements of a database in the context of severe accident are as follows:

**Observation 1:** the database should relate specifically to severe accidents from the prime sources of energy

Whilst it is noted that a proposed database for the health and environmental impacts from normal (routine) operating conditions and continuous discharges is to be limited to energy sources which are used in the generation of electricity it is suggested that severe accident data is collected on all major energy sources. It should be noted however that when using information from sources such as coal, oil or gas that it will be necessary to adjust the data to take account of the proportion of that energy source used for electrical generation.

**Observation 2:** the database should include information on severe accidents which occur throughout the entire fuel cycle of the different energy sources.

The various stages of the fuel cycle include extraction, transport, processing, storage, conversion and waste disposal. It should be recognized that some fuel cycles will not include all of the above stages and also that some fuel cycle stages will not have the potential for the type of severe accidents defined earlier.

**Observation 3:** the database should clearly distinguish between information which is factual from that which is based on predictive assumption.

**Observation 4:** the database should include details of health and environmental impacts.

In order to have access to all the relevant categories of risk it will be necessary to present and treat the various types of health and environmental impacts separately.

**Observation 5:** the database should give reference to the source of information.

Only enough information should be shown on the database to enable the original source(s) of data to be identified. Past experience has demonstrated that databases become unwieldy if attempts are made to hold more than just an adequate reference as information.

**Observation 6:** the uncertainties in data and estimation should be reported.

It is recognized that in many cases the uncertainties may be difficult to identify or quantify but where they are reported they must be included.

### **Components and Contents of the Database**

There are several approaches for the establishment of a structure to accommodate the general requirements of the database. The following parameters and or data element are presented as a preliminary structure framework in order to be consistent with the proposed database for data from routine (normal) operating conditions and routine emissions: country, region, energy source, energy system, application, fuel cycle step, technology, essential technical characteristics, fuel / input material characteristics, operational phase. These components are the same as those proposed in general for the routine (normal) operation conditions database. A description of the accident can be given in a series of sub-fields. These sub-fields could be organized to cover the material involved and its properties, the quantity of material, was it toxic, flammable, explosive, cryogenic etc? if fire was involved what was the type of fire-pool, jet etc? if an explosion occurred was it confined, semi-confined, unconfined. Other sub-fields would indicate physical aspects of the effects of the accident such as extent of building damage, window breakage, crater size etc. The fields for this section could be chosen after consideration of the effects of a range of accidents from the different energy organizations.

**Health impact data:** most accident reporting will include details of the number of instantaneous deaths, severe injuries and number of persons evacuated. The fields here would contain data on the agreed indicators.

**Environmental impact data:** for a number of reasons the information on the environmental impact of severe accidents will be sketchy to say the least. Much of it will only be available some time after the accident. Fields in the database should include the following: nature of the major pollutants (i.e. gaseous, liquid, particulate); environmental media affected; possible nature of impact (i.e., short-medium-long term); nature of principal receptors; details of any assessment of environmental impact; details of any observed environmental impact (i.e., dead fish, discoloured vegetation, water concentration measurements etc.)

### **Sources of Data**

A number of databases which contain information relative to the consequences of severe accidents already exist. These include OFDA - the computerized database run by the Office of Foreign Disaster Assistance, U.S. Agency for International Development, MHIDAS, (Major Accident Incident Data Service), UK Health and Safety Executive (this contains details of over 5000 severe accident involving hazardous materials). Veritec (1990) WOAD - World Offshore Accident Databank Statistical Report - Veritas Offshore Technology and Services, Hovik, Norway. Other sources of data include incident reports collected by insurance organizations (e.g. Swiss Re-Insurance Co., Marsh and McKellan Ltd, Browning Risk Assessment). Newspaper accounts, should not be discounted as a major source of information. Most photographs of the early stages of severe accidents originate from newspaper sources and reporters files often contain material not subsequently reported. It should be stressed that serious acquisition of good reliable data on severe accidents will not be obtained by waiting passively for organizations to report them. A high quality severe accident database will only result if those responsible for maintaining the database play a very active part in seeking out data and following up in detail all reports of severe accidents. It is essential that once a severe accident has been identified, analyzed and recorded on the

database, that data collection for that accident does not cease. Accident investigations, public enquiries and long term environmental studies can take many months/years to complete, (i.e. investigations into the consequences of the Chernobyl incident which will carry on for years to come). For the purpose of carrying out a comparative risk assessment of different energy sources it is essential that the risks from severe accidents are not considered in isolation from those incurred during routine operations. There will always be a need to retain some qualitative inputs to comparative assessment and the decision making process, especially in the field of environmental impacts. It is essential that those carrying out a comparative risk assessment recognize this factor. It is recommended that further work should be carried out in order to quantify some of the more important factors which can only currently be treated in a qualitative manner. Most of the current health and environmental impact data is related to the effects of radioactive materials and that there exists a disproportionate amount of data relative to that relative to non-nuclear energy sources. A comparative risk assessment should take account of the dimensions of space and time. Whilst it is acknowledged that there will be difficulties in setting rigid definitions for these dimensions it is recommended that definitions should be attempted and clearly indicated. One of the main uses of severe accident information would be to provide an input when carrying out comparative risk assessments of different energy sources result both from severe accidents and routine operations. The databases on the health and environmental impacts from severe accidents and from routine operations cannot be regarded as separate entities. In many cases they will overlap and strong interlinking of the two should be considered. It will be necessary to ensure that data from different sources, (especially for different countries), are information based on the same criteria. Before the final details of a database are established, a number of case studies of suitable severe accidents should be studied in order to assist determining the final form of the methodology and database.

## **HEIES DATABASE**

The joint Inter-agency (CEC/IBRD/IAEA/OECD-NEA/OPEC/IIASA/WMO/ESCAP/UNIDO) project on databases and methodologies for comparative assessment of different energy sources for electricity generation (DECADES) administered by IAEA (International Atomic Energy Agency) aims towards providing information and tools to decision makers and energy analysts for enhancing their capabilities for comprehensive comparative assessment of different energy chains for electricity generation, normal and accidental situations, incorporating health and environmental issues in the planning and decision making process. A computer package (DECPAC) gives access to the DECADES databases which include numerical values, textual information (with hyper-text), and pictorial information (e.g. graphics, schematics and photographs). Three main reference databases are currently in work:

- RTDB (The Reference Technology Data Base) which contains generic data on technical, economic and emission parameters of energy chains (fossil, nuclear, renewables);
- TOXDB (Toxicology Data Base) provides dose effect relationships and coefficients for selected toxic emissions and releases from fuel chains described in the RTDB;
- HEIES (Health, Environmental Impacts, Energy Systems) provides indicators for **normal and severe accidents** of health and environmental impacts of different power plants and fuel chain facilities referring to literature surveys, results from case studies or measurements.

HEIES is designed to give essentially site specific information, related to a given area where the facility is located. HEIES includes numerical data, textual and visual information and extensive references to the sources of information and is dedicated to comparative risk assessment studies for electricity generation systems.

## **REFERENCES**

- 1.\*\*\* "Comparative Assessment of the Health and Environmental Impacts of Various Energy Systems from Severe Accidents", Working Material, IAEA, Vienna, Austria, 1993

## CONSIDERATION OF PROBABILISTIC SAFETY OBJECTIVES IN OECD/NEA MEMBER COUNTRIES.

Magiel F. Versteeg<sup>1</sup>

Nuclear Safety Inspectorate  
Ministry of Social Affairs & Employment  
P.O. Box 90804  
2509 LV The Hague  
The Netherlands

### INTRODUCTION

Since it has been recognized that PSA's produce numbers which can be used as a yardstick in safety decisions, a lot of effort has been put in the development of probabilistic safety criteria (PSC). Almost every member country of the Nuclear Energy Agency (NEA) of the Organization for Economic Cooperation and Development (OECD) uses PSC, in one way or another, for the safety assessment of nuclear power plants. For instance, these might be dose limits for anticipated occupational occurrences and design basis accidents with implicit or explicit frequency considerations of these incidents, or PSC related to the probability of loss of core integrity. A large variety of different PSC can be recognized in these OECD member countries. The choice of the PSC, their applicability, and whether or not these PSC are used in a formal and/or legal way, is dependent on the political and regulatory situation. In some countries PSC are used in a formal way, while in other countries these are only informally used. The spectrum of utilisation includes the use as design requirements and the use as a regulatory and licensing tool by the authorities.

These PSC can be grouped according to the addressed level of consequence. The following PSC groups can be recognized:

- PSC relating to the reliability of a particular safety system/ function (level-0 PSC),
- PSC relating to the probability of loss of integrity of the reactor-core (level-1 PSC),
- PSC relating to the probability or magnitude of a large radioactive release (level-2 PSC),
- PSC relating to public health effects (level-3 PSC).

The PSC related to public health risks can be divided into two parts:

- PSC referring to early or late mortality risk,
- PSC relating to received dose.















In tables [1 - 4] an overview is given of the various PSC as applied to nuclear power plants in the OECD member countries. However, one should be careful when comparing similar PSC with each other, because boundary conditions and definition of terms might be different. In Reference 1 complementary general information can be found on the use of PSC in OECD member countries.

---

<sup>1</sup>) The author is chairman of a task force on 'the use of quantitative safety guidelines' within Principal Working Group 5 (on risk assessment) of the Committee on the Safety of Nuclear Installations (CSNI) of the Nuclear Energy Agency (OECD).

The PSC related to mortality risk is not restricted to the nuclear industries alone. In some countries these PSC are applied as well in other hazardous industries.

Table 1. Probabilistic Safety Objectives/ Criteria on the Safety System/ Function Level (Level - 0 PSC) and on the Core Integrity Level (Level - 1 PSC).

PSC	Country	Can.	Finl. <sup>2</sup>	Italy	Spain <sup>3</sup>	Neth. <sup>4</sup>	UK <sup>5</sup>	USA <sup>6</sup>
Safety Function/ System failure probability PSC = Level - 0 PSC (/demand)								
Safety Systems (general)							$< 10^{-3}$	
Reactivity control			$< 10^{-5}$					
Shut down 1 (control rod)		$< 10^{-3}$						
Shut down 2 (liquid poison)		$< 10^{-3}$						
Core Cooling Capacity at power			$< 10^{-4}$					
Emergency Core Cooling Systems		$< 10^{-3}$						
Containment Isolation System		$< 10^{-3}$	$< 5 \cdot 10^{-3}$					
Containment Heat Removal System		$< 10^{-3}$						
Containment Spray System		$< 10^{-3}$						
Auxiliary Feedwater Supply			$< 10^{-4}$					$< 10^{-4}$
Rapid depressurization (e.g. ADS)			$< 10^{-4}$					
Core damage/ melt frequency = Level - 1 PSC (/year)								
New <sup>7</sup> Nuclear Power Plants formal informal						$< 10^{-5}$	$< 10^{-5}$	
Existing Nuclear Power Plants formal informal				$< 10^{-5}$	$< 10^{-4}$	$< 10^{-4}$	$< 10^{-4}$	$< 10^{-4}$

<sup>2</sup>) Compliance with 90-th percentile has to be shown.

<sup>3</sup>) Informally, core melt frequencies larger than  $10^{-4}$ / year require a more detailed analysis and/ or some design and operational modifications.

<sup>4</sup>) Regulatory statement.

<sup>5</sup>) The maximum credit given for a safety function performed by redundant safety systems is  $10^{-5}$ / demand due to common cause failures.

<sup>6</sup>) Semi-official policy statement US-NRC.

<sup>7</sup>) For The Netherlands and the UK, the headings new and existing nuclear power plants refer also to the objective and limit value of the PSC.

Table 2. Probabilistic Safety Objectives/ Criteria on the Large Release/ Source Term Level (Level - 2 PSC).

Country	Finland	France	Italy	Neth.	Sweden	UK	USA
Large Release (Frequency)/ Source Term (Frequency) PSC. (Level - 2 PSC)							
Unacceptable consequences and Source Terms.	<0.1% of core invent. excl. iodines and N.G.				<0.1% of core invent. excl. iodine and N.G.		
Frequencies of Large Releases or unacceptable consequences.		<10 <sup>-6</sup> /y for unaccept. conseq.	<5% of core melt freq. if Source Term contains >0.1% iodine and Cs.	<10 <sup>-6</sup> /y for large release = dose equival. of .5 Sv to the most exposed person		<10 <sup>-6</sup> /y limit for Source Term of 10 <sup>4</sup> TBq I <sub>131</sub> and/ or 200 TBq Cs <sub>137</sub> or equival. <10 <sup>-7</sup> /y objective	<10 <sup>-6</sup> /y

## TYPES OF PSC

The PSC considered in the OECD/NEA member countries are:

- a) System level PSC - Reliability of important safety systems or functions, usually defined in terms of tolerable unreliability (unavailability) per demand. Established PSC of this type refer to essential functions like reactor shut-down, emergency core cooling system, and the containment systems (the systems safeguarding the containment function under accident conditions). See table 1.
- b) Level-1 - Loss of core integrity, usually defined in terms of a probability limit per unit time (year) for reaching a downgraded core condition. This is mostly understood as severe damage of the fuel and its cladding or as a total melt down of the fuel and consequent breach of the primary circuit boundary. See table 1.
- c) Level-2 - Radioactivity release limits as PSC appear in two distinct forms. One is the Farmer type criterion which defines a release magnitude vs. frequency limit over the whole possible range of releases, the other sets a maximum tolerable frequency for a so called "large release" - a term which needs to be defined if it is to be used (Source Term). See table 2.
- d) Level-3 Dose/frequency PSC specify the tolerable probability per unit time for which given dose levels might be exceeded (or vice versa). A common variant of this criterion is the limitation of doses for specified plant conditions implicitly probabilistic in nature (anticipated operational occurrences, incidents and design basis accidents). Especially these type of PSC are broadly used in the OECD member countries in the area of operational occurrences and design basis accidents. In this case the probabilistic aspect is implicitly given by the class of incidents/ accidents the PSC applies to. See table 4.

e) Level-3 - Individual risk of early and/or late fatalities specifies the probability of death of a member of the public (either average or most exposed) per year due to all releases. Early fatalities can result only from the consequences of very severe accidents and can occur only in the vicinity of the site. See table 3.

f) Level-3 - Societal or group risk is mostly used in conjunction with severe accident. It might be specified by the probability per year of death of any specified number or percentage of the public. See table 3. Another approach is a limit value for the collective dose for operational occurrences and design basis accidents (See table 4; remarks regarding Canada).

Table 3. Probabilistic Safety Objectives/ Criteria on the Public Health Level (Level - 3 PSC).

Country	Netherlands	United Kingdom	USA
Public Health Level PSC (Level - 3 PSC)			
Individual Risk			
Prompt fatalities	$10^{-6}/y$ limit value & $10^{-6}/y$ de minimis value; both early and late fatalities. Applicable to all hazardous industries.	$10^{-4}/y$ limit for old NPP and any other hazardous industrial plant $10^{-6}/y$ limit for new NPP. $10^{-6}/y$ = objective for both old & new; $10^{-6}/y$ limit for all NPP's together. Both early and late fatalities.	The risk to the average individual in the vicinity of the plant within a radius of 10 miles should not exceed 0.1% of the sum of prompt fatality risks due to other causes. ( $<5.10^{-7}/y$ ) = Objective.
Late fatalities			
Societal Risk			
Prompt fatalities	CCDF charact. by: $<10^{-6}/y$ for $\geq 10$ early fatalities $<10^{-7}/y$ for $\geq 100$ early fatalities and $<10^{-8}/y$ for $\geq 1000$ early fatalities. De minimis value 2 decades lower in frequency scale. Applicable to all hazardous industries.	Societal risk is covered by the level 2 PSC and the dose criteria [Ref. 3]. In an earlier version of a policy paper of the Health & Safety Executive [Ref. 4] a PSC for the total nuclear industry was given: $<10^{-4}/y$ for about 100 immediate or eventual fatalities due to all NPP's together.	The risk to population near the plant should not exceed 0.1% of the sum of cancer fatality risks resulting from all other causes. ( $<2.10^{-6}/y$ ) = Objective.
Late fatalities			

**SOME REMARKS ON PROBABILISTIC SAFETY CRITERIA ON THE PUBLIC HEALTH LEVEL; ESPECIALLY ON APPLICATION TO THE NON-NUCLEAR INDUSTRIES.**

In some countries, like the Netherlands and the U.K., the usage of PSC on the public health level is not only restricted to nuclear activities, but is also applied to other potential hazardous industries and activities. See References 3 and 4 for a further discussion on the U.K. level-3 PSC. In the Netherlands, also the public health risks originating from the transportation sector is evaluated by means of probabilistic risk assessments and probabilistic safety criteria. Public health risks from possible airplane crashes in the vicinity of a major airports, or from a crash of a rail tank car containing hazardous materials on a railway shunting-yard, or from an accident related to the transportation of dangerous materials via inland waterways are currently a big issue. Several studies indicate that the risk levels in this non-industrial sector are significant higher than those in the industrial sector. See reference 5 for a further discussion on the Dutch PSC.

Because large economical interests are involved, there is in the Netherlands very much discussion on the actual applicability of societal risk criteria. Therefore, pressure is put on to

Table 4. Frequency-dose design objectives for accidental conditions including design basis accidents.

Country	Frequency range of occurrence (yr <sup>-1</sup> )	Dose limit (whole body) (mSv/event)	Remarks
Belgium	category 1 category 2 category 3	0.5 5 ≤20	implicit frequency definition category 1: Loss of Offsite Power category 2: e.g., Small LOCA, Steam Generator Tube Rupture, Uncontrolled Rod Assembly Withdrawal, Rupture of Gaseous or Liquid Waste Tank. category 3: e.g., Large LOCA, Steam Line Break Accident, Rupture of Feedwater Line Outside Containment.
Canada	3.10 <sup>-1</sup> - 3.10 <sup>-4</sup> < 3.10 <sup>-4</sup> ----- > 10 <sup>-2</sup> 10 <sup>-2</sup> - 10 <sup>-3</sup> 10 <sup>-3</sup> - 10 <sup>-4</sup> 10 <sup>-4</sup> - 10 <sup>-5</sup> < 10 <sup>-5</sup>	5 250 ----- 0.5 5 30 100 250	In place since 1972. 3.10 <sup>-1</sup> - 3.10 <sup>-4</sup> applies to single failures (process systems). For this frequency band also maximum total population dose limits are formulated: 100 man-Sv/y whole body dose. For the design base area < 3.10 <sup>-4</sup> a population dose limit of 10 <sup>4</sup> man-Sv/year applies. ----- Under trial use since 1980
Finland	Design Basis Accidents Severe Accidents	5 ≤20	Implicit frequency definition Assumed that the released source term contains ≤ 0.1% core content of Cs or equivalent.
France	10 <sup>-2</sup> - 10 <sup>-4</sup> 10 <sup>-4</sup> - 10 <sup>-6</sup>	5 150	Only used as guideline values
FRG	Design Basis Accidents	50	Implicit frequency definition
Italy	> 10 <sup>-3</sup> 10 <sup>-3</sup> - 10 <sup>-4</sup> < 10 <sup>-4</sup>	5 100 100	guideline values additional as target/ trend: 5 mSv/event for all DBAs.
Japan	Design Basis Accidents Siting Evaluation Accidents	5 250	Implicit frequency definition
Spain	as USA	as USA	
Sweden	Severe Accidents		Controlled by level - 2 PSC; implicit frequency definition
Switzerl.	1 - 10 <sup>-2</sup> 10 <sup>-2</sup> - 10 <sup>-4</sup> 10 <sup>-4</sup> - 10 <sup>-6</sup>	0.2 1 100	
Netherl.	10 <sup>-1</sup> - 10 <sup>-2</sup> 10 <sup>-2</sup> - 10 <sup>-4</sup> 10 <sup>-4</sup> - 10 <sup>-6</sup>	0.4 4 40	
U.K.	10 <sup>-2</sup> 10 <sup>-3</sup> 10 <sup>-4</sup>	0.1 - 1 1 - 10 10 - 100	Assessment reference levels (design targets)
USA	Design Basis Accidents	250	



add some flexibility to the concept of using societal risk criteria as a yardstick for licensing, siting and housing developments. Especially, the area around a major airport where elevated risk levels are identified, is in the order of 2500 km<sup>2</sup>. Cities, as well as the main international airport want to expand in this area. Ergo, a lot of problems and discussions. However, for the time being these criteria remain in force.

On the other hand, it has been recognized, that a societal risk criterion described by a Complementary Cumulative Probability/Density Function (CCDF) of the number of prompt fatalities might not be adequate enough to solely being used as a yardstick for societal disruption. Due to discussions in the parliament, additional level-3 PSC are being developed to judge the potential contamination of large areas of land in case of severe nuclear reactor accidents.

### SOME OBSERVATIONS

In general, the nuclear regulatory requirements in most of the surveyed member countries are deterministic, aided to limited extent by probabilistic ones. The most commonly used probabilistic requirements/rules refer to cut-off values for the consideration of initiating events especially of external origin and to the categorization of plant states for design considerations.

With regard to specific PSC, in general the frequency values set for them by different countries fall into a relatively narrow range, however the similarity may be more apparent than real due to possible differences in definitions, PSA scope, models and data bases used and calculational procedures employed.

The rationale given for the selection of uniform numerical values of PSC was very general, qualitative and based on a judgement of what is considered a tolerable or negligible risk. In the survey made, no specific reasoning could be revealed.

Because of the large uncertainties in PSA results, particularly if they refer to risks at the public health level, many countries found it advisable to define PSC as targets and not as acceptance criteria. In two countries, the U.K. and the Netherlands, limit values and objectives respectively de minimis values are formulated as PSC on the public health level. In both countries these higher level PSC are used for regulating other activities and/or industries as well.

In the USA the PSC for individual mortality risk refers to an average individual in the vicinity of the plant, whilst the Netherlands and the U.K. refer to the most exposed person.

A too stringent application of PSC, without the consideration of other than safety issues, might be counterproductive.

PSC are often of a political nature, and therefore often vaguely phrased. In order to show compliance with PSC, both PSA and PSC should be consistent in the definition of terms, boundary conditions, assumptions being made, etc. See further Reference 2 for a further discussion on the necessary compatibility between PSC and the associated PSAs to be used for showing compliance with these PSC.

### REFERENCES

1. S. Chakraborty, Y.G.Gonen and M.F.Versteeg, Technical Note: Quantitative Safety Guidelines (QSGs) and Probabilistic Safety Assessment (PSA) in the OECD Countries, *Nuclear Safety* 32-2: 184 (1991).
2. M.F.Versteeg, Showing Compliance with Probabilistic Safety Criteria and Objectives, *Reliability Engineering & System Safety* 35-1: 39 (1992).
3. Health & Safety Executive, Safety Assessment Principles for Nuclear Plants, HMSO, London (1992).
4. Health & Safety Executive, The Tolerability of Risk from Nuclear Power Stations, HMSO, London (1988, revised 1992).
5. M.F.Versteeg, The practise of zoning; how PRAs can be used as a Decision-making Tool in City and Regional Planning, *Reliability Engineering & System Safety* 26-2: 107 (1989).

## **RISK ASSESSMENT OF LARGE INDUSTRIAL COMPLEXES IN EASTERN EUROPE: A COMPARATIVE PROSPECTIVE**

**Adrian V. Gheorghe**

Swiss Federal Institute of Technology - ETH  
Polyproject "Risk and Safety of Technological Systems"  
ETH - Zentrum, 8092 - Zurich  
Switzerland

### **INTRODUCTION**

Industrial development is essential to the improvement of the standard of living in all countries. This entails the building of refineries, power stations and other large industrial complexes. However people's health can be affected directly or indirectly by routine waste discharges. The environment is often adversely affected by emissions from power stations and the accumulation of industrial wastes. Accidental releases of toxic materials can have disastrous effects on both health and the environment.

The UN-Inter-Agency Programme on the assessment and management of health and environmental risks from energy and other complex industrial systems aims at promoting and facilitating the implementation of integrated risk assessment and management of large industrial complexes and energy generation systems. This initiative includes the compilation of procedures and methods for environmental and public health risk assessment and the transfer of knowledge and experience amongst countries in the application of these procedures and in the implementation of an integrated approach to risk management.

The programme is being jointly undertaken by four UN organizations: United Nations Environment Programme (UNEP) within the framework of the Awareness and Preparedness for Emergencies at Local Level (APELL), the International Atomic Energy Agency (IAEA), the World Health Organization (WHO) and the United Nations Industrial Development Organization (UNIDO). The focus of the UN- Inter-Agency Programme is inter-related with the following areas of activities:

- i) The preparation and dissemination of methods and guidelines relevant to the integrated health and environmental risk assessment safety and management. A Procedural Guide on the topic has been published (in draft) as well as a manual for the classification and prioritization of risks for large industrial areas and energy production systems;
- ii) The development of models and computer codes to assist implementing different tasks of risk assessment / safety management methodology. A Decision Support System (InterCLAIR) and other software packages have been developed within this project. A working document on environmental models for risk assessment and management of air and surface water pollution in large industrial complexes has been recently published as reference manual for the above decision support system.

iii) Support to national case studies. A number of member states affiliated with the programme have requested that they be represented within the Inter-Agency Project with specific case studies of importance to their national economies.

iv) Training at national and regional levels with the main objectives being to transfere knowledge and building capabilities in participating countries.

The UN organizations sponsoring this programme have been involved for several years in activities that aim at environmental and health risk assessment and management, prevention of major accidents and emergency preparedness. Based on the experience within this Inter-Agency Project, a number of case studies are in different stages of finalization. Specific aspects related to risk assessment and management in a given area, highlighted different subjects related to complex *problematique* of integrated risk assessment and management of industrial systems.

First the paper introduces the guiding principles for developing integrated environmental and health risk and safety management studies in a large region as applied to all case studies reviewed in the present work.

Part one of this paper presents the find of a joint IAEA/UNIDO mission and introduces recommendations on the environmental and health situation for the area of Copsa Mica (Romania); Carbosin Chemical Plant and Sometra Non-Ferrous Metal Plant.

Part two is a report on the assessment and management of health and environmental risks from industrial systems in the North Bohemia area in the former Czechoslovakia; this study was developed by VUPEK-Prague following general procedural guidelines of the UN-Inter-Agency Project.

Part three introduces work done in the area of Zagreb (Croatia) for assessing different types of industrial risks (normal operation and accidental situations) in the town and its surroudings. New concepts are presented for the use of GIS (Geographical Information Systems) in the area for better documenting health and environmental risk assessment and safety management actions.

## **GUIDING PRINCIPLES FOR RISK ASSESSMENT: A BASE FOR COMPARATIVE ANALYSIS AND EVALUATION**

The UN - Inter-Agency Programme on Risk Assessment and Management of Large Industrial Areas and Energy Generation Systems (UNEP /WHO /IAEA/ UNIDO) brings together expertise in health, the environment, industry and energy. The purpose of the Inter-Agency Programme is to develop a broad approach to the identification, prioritization and minimization of important industrial hazards in a given area.

**Programme Activities:** The following tasks for the programme are identified:

i) preparation and publication of a Procedural Guide to Risk Assessment and Management;

ii) nine to twelve national case studies to test and demonstrate methodologies and thus contribute to the preparation of the *Procedural Guide* and to develop practical plans for risk management within the areas convened ( emphasis was placed on the need to improve communication with policy-makers and the public);

iii) development of databases, models and other analytical techniques; evaluation and publication of information and techniques considered to have wider application;

iv) active promotion of the area-wide approach to risk assessment and management with emphasis on professional training.

**Case Studies** activities related to the Programme have taken place in all the countries concerned. Not all have qualified as case studies for the programme in terms of initial criteria set. Reports are now available for the studies in North Bohemia (Czech Republic), Copsa Mica (Romania), Zagreb (Croatia) - countries with economies in transition, and for Kooragang Island Area (Australia), and Rotterdam region (The Netherlands).

Databases, analytical techniques and computer codes have been developed for risk assessment and management of air and surface waste pollution in large industrial complexes. **HERAMIS** (Health, Environment, Risk Assessment and Management of Industrial/Energy Systems) has been developed by the Programme as a pilot software package incorporating all the products of the Inter-Agency Programme to date, including the Procedural Guide and the available case study reports, in computer-useable form.

**HERAMIS** is a knowledge and decision support system and includes both databases and hyper-text form, and decision and modelling systems (e.g. risk prioritization and classification in an industrial area, effect of radionuclides released from accidental situation on the health of the different population groups at risk).

The integrated risk assessment approach: all health and environmental risks within an area should be systematically identified, analyzed and assessed in such a way that rational choices could be made about which risks should be reduced, weighing the social and economic costs of such risks, the benefits of risk reduction and associated costs and formulating the basis of an integrated environmental and safety management.

The integrated risk management approach: all options of risk management (locational, preventative, mitigating, protective and institutional) should be explored in a holistic way and used complementarily so that the resources committed in the safety management process are optimized. The methods and techniques of integrated environmental risk assessment and management are best applied to geographical areas that accommodate a number of industrial and related activities of a hazardous and/or polluting nature, also being areas of significance in terms of social and economic developments. The case may also be that serious risks to people and the environment already exist in a particular area and that decisions have to be made about the prioritization of the risks to be reduced, consistent with available resources.

Targets for risk are firstly, the people living in the study area under consideration. Very young and old people and people with different allergies and illnesses may be much more sensitive to certain contaminants than the general public; people outside the study area may also be at risk, due to transportation of contaminants through the air, by waterways or by contamination of agricultural products. Secondly the ecological systems in the study area or within the influence sphere of the study area may be at risk. The extermination of one or two species may disrupt a whole ecological food chain. Thirdly economic resources can be at risk. An accident at any industrial installation can destroy many others in its neighbourhood. Acid emissions may destroy forests, fisheries, historical buildings and monuments; pollution may have significant economic consequences to the tourist industry of an area.

## **CASE STUDIES: EASTERN EUROPE - ECONOMIES IN TRANSITION**

### **Copsa Mica - Romania**

Copsa Mica is located in the valley of the Timnava Mare river which flows in an approximately east to west direction. Two other streams, the Valea Viilor and the Visa run into the river at Copsa Mica. Settlements exist in the valleys of these streams, Valea Viilor and Motis in one, Agribiciu and Seica Mare in the other. In addition, the area has many streams and rivers and small population centers surrounding Copsa Mica. The Romanian Government Commission (1991) reports that the area affected by pollution due to industrial activities in the area extends from Dumbraveni to Blaj, a distance of about 50 km. This polluted area is quoted as being 180 750 hectares. Some 200 000 people are considered as being affected, with 75 000 living in the high pollution area.

The main activities in the region were forestry and agriculture until discovery of natural gas in the 1930's when industrialization began. The Sometra (lead, zinc) and the Carbosin (carbon black) plants were installed in the 1930's. The two plants located in this area grew in of economic importance to the country.

After the Second World War, successive governments placed high priority on production, whereas after the 1970's the Government did not keep up with the environmental technology developed in the rest of the world. Even the most essential repairs were not carried out.

At the request of the Government of Romania an UN- Inter-Agency team of international experts undertook in May 1991 an independent investigation of the environmental and public health situation in the Copsa Mica area.

The main conclusions are:

- The environmental situation in the Copsa Mica area is considered an environmental disaster, which requires immediate action by the Government and the international community. The levels of pollution of air, water, ground water and soil well exceed all international and Romanian standards.

- The existing environmental degradation and levels of pollution constitute a major risk to public health in the area. The main pollutants of concern are lead, cadmium and sulphur dioxide. The risk of a major accident with the release of ammonia, which could kill or affect hundreds of people, is high.

- The conditions of the Carbosin and the Sometra plants are very poor, from the point of view of maintenance, operation, safety and environment. This has resulted in the release of large quantities of toxic substances and the heavy contamination of the area. The technology used by both plants is similar to that adopted by other countries and if properly operated and maintained it should not cause such pollution.

The main strategy for the Government should be to reduce the risks to the population and the environment to an acceptable level by appropriate short and long term measures.

Among the practical recommendations are: alternative food supplies and information to the population about the hazards of eating locally grown vegetables; conditional measures for the local drinking water supply if the levels of lead and cadmium are too high; repair and rehabilitation of the Sometra and Carbosin plants; responsibility of the ministries of Industry and Environment; environmental legislation; inspection and monitoring; further studies.

#### **North Bohemia Area - Czech Republic**

The case study did not aim to be an exhaustive environmental risk study of the region. The work was done by Czech specialists in co-operation with the French research center CEPN (modelling tools- the immision model CALCONC and the Batex model on accidents consequences). The area has 7 820 km<sup>2</sup> and the resident population is almost 1.2 million inhabitants-average population density 153 inhabitants / km<sup>2</sup>.

Input data for the risk assessment models and their calculations were partially updated from the data obtained from The Northern Bohemian Brown Coal Union and from the data collection performed in 1990. Continuous emissions calculations included: air pollutants routinely emitted from smokestacks, tailpipes, and fugitive emissions from vents, open burning etc; water pollutants discharged to surface water from outfall pipes, routine overflow from waste ponds or lagoons, and non-point sources such as run-off urban roadways; emissions to ground water from landfill leachate percolation from surface ponds and lagoons, leakage from pipelines, and discharges from injection wells.

Continuous emissions lead to exposures that created chronic, long-term risks. Acute health effects may also result. Extended meteorological inversions, lead to acute exposures and acute effects from routine emissions

The region is characterized by a gradual decrease of water quality in water-courses. Nearly all water courses with high flows belong to the third and fourth class of the water quality (according to the national standards). Assessment of exposure: for the whole population of the district of Litomerice - the selected sample of territory in the investigated area-indicates the collective exposure, respectively  $0.425 \times 10^6$  man-ug/m<sup>3</sup> for SO<sub>2</sub>,  $0.145 \times 10^6$  man-ug/m<sup>3</sup> for NO<sub>x</sub>, and  $0.78 \times 10^6$  man-ug/m<sup>3</sup> for dust. Further work follows with assistance from Switzerland and other developed countries.

### **Zagreb Area - Croatia**

The project was officially introduced at the beginning of 1989; revisions were formally adopted by the end of 1991 by the Secretariat of the UN - Inter-Agency Project on Risk Management. The expected results of this work are:

- i) development of practical methods of risk management and the control of hazardous events and activities;
- ii) improvement of policies in the field of protection of human health and the environment;
- iii) establishing optimal allocation of funds intended for the reduction of risks to which the population and the environment of the Zagreb area are exposed.

The work is foreseen to be realized in four main phases mainly: i) establishment of a hazard - quantities database for the area of interest; hazard prioritization for various activities in the study area: ii) health and environmental risk analysis studies: iii) infra-structure and organizational safety analysis: iv) formulation and management of an integrated health/environmental and risk strategy with associated action plan (e.g. safety culture measurement and improvements).

The main results of the study are the development and implementation of a specialized data base for hazard identification and prioritization, risk classification of various installations which exist in the investigated area, health and environmental risk assessment and evaluation due to continuous emissions (epidemiological studies), introducing elements of safety culture in the overall risk assessment and safety management process for the study area.

By developing the model of epidemiological analysis for the City of Zagreb, a number of impact environmental and health indicators were considered. Various effects on human health of exposure to environmental pollutants considered in the study, can be summarized as follows: premature death of individuals, severe acute illness or major disabilities, chronic debilitating disease, minor disability, temporary minor illness, discomfort, behavioural changes, temporary emotional effects, minor physiological changes.

Different techniques were used to determine such indicators (e.g. "pars-pro-toto": one agent is taken to be representative for a group of pollutants, "indexes": pollutants are grouped together to combination rules depending on toxicity, "effect indicators": an effect caused by a pollutant or group of pollutants is taken to be the situation).

The study is using a complex set of urban environmental risk and impact indicators which are grouped into: housing concerns, services and employment concerns, ambient environment concerns and, social and cultural concerns.

**HEGIS** (Health, Environment Geographical Information System) computerized information system, which is now currently under development for the case study includes the following groups of indicators: environmental quality, public health, social conditions, demographic and social status, health service quality and quality and utilization.

The whole study is framed within the present legislation which was recently adopted in Croatia. To further develop a comprehensive health and environmental risk assessment and

i) be aware of the existing national and international agencies with health and the environment as target work and integrate their relevant activities, such as data collection sources and networks, GIS development and application, and the need for the development of standards,

ii) identify and recommend standards and guidelines specifically appropriate to *HEGIS* information system,

iii) provide accesible training and educational facilities and staff and,

iv) create an organizational network of national focal points and specialized collaborating centre (e.g. emergency risk center ) in the country.

## ACKNOWLEDGEMENT

Part of this work was done when the author was with the International Atomic Energy Agency, Safety Assessment Section acting as Scientific Secretary for the UN-Inter-Agency Project on Risk Assessment and Safety Management of Large Industrial Complexes and Energy Production Systems. Special appreciations are expressed to Dr. F. Niehaus and Mr. S. Haddad (now with the Department of Planning, NSW, Sydney, Australia) from IAEA and to Mrs. J. Aloisi de Larderel, Director IE/PAC, UNEP, Paris for their activity, interest and support given to the Inter-Agency Programme.

Acknowledgements are also addressed to Prof. Dr. Petre Roman, former Prime Minister of the Romanian Government, Mrs. M. Dreicer of CEPN - France, and Drs. D. Subasic and N. Malbasa - Zagreb, Croatia, for their political or professional involvement in different stages of work in the above presented regional case studies.

## REFERENCES

1. \*\*\* " Procedural Guidelines for Integrated Health and Environmental Risk Assessment and Management for Large Industrial Complexes and Energy Generation Systems", IAEA, Working Material, Vienna, Austria, 1991
- 2.\*\*\* "Integrated Health and Environmental Risk Assessment and Management. Case Studies", IAEA, Working Material, Vienna, Austria, 1992
3. \*\*\* "Risk Assessment and Management - Zagreb Area Case Study", ECONERG Report, Zagreb, Croatia, Phase 1 and 2, 1993

**075 Fire Risk Analysis for Engineered Systems**

*Chair: R. Friedman, NASA Lewis*

**Risk Analysis of Environmental Hazards at the High Flux Beam Reactor**

*J.L. Boccio (BNL), V.S. Ho, D.H. Johnson (PLG)*

**A Model for Fuel Fire Duration and Application to the B-1B Bomber**

*D.E. Magnoli (LLNL)*

**Implementation of the FIVE Methodology: Results and Lessons Learned**

*R.C. Lindquist, M.S. Powell (Arizona Pub. Serv.)*

**Fire Risk Assessments at Rocky Flats Plant**

*T.L. Foppe, E. Stahlnecker (EG&G Rocky Flats)*



## **RISK ANALYSIS OF ENVIRONMENTAL HAZARDS AT THE HIGH FLUX BEAM REACTOR\***

**J. L. Boccio, V. S. Ho,\*\* D. H. Johnson\*\***  
Brookhaven National Laboratory  
Upton, New York 11973

### **Introduction/Background**

In the late 1980s, a Level 1 internal event probabilistic risk assessment (PRA) was performed for the High-Flux Beam Reactor (HFBR), a U. S. Department of Energy research reactor located at Brookhaven National Laboratory. Prior to the completion of that study,<sup>1</sup> a level 1 PRA for external events was initiated, including environmental hazards such as fire, internal flooding, etc.

Although this paper provides a brief summary of the risks from environmental hazards, emphasis will be placed on the methodology employed in utilizing industrial event databases for event frequency determination for the HFBR complex. Since the equipment in the HFBR is different from that of, say, a commercial nuclear power plant, the current approach is to categorize the industrial events according to the hazard initiators instead of categorizing by initiator location. But first a general overview of the analysis.

### **Approach/Overview**

The overall HFBR environmental hazards analysis was performed in two steps: spatial interaction and detailed risk analysis. The first stage largely begins with the identification of potential environmental hazards at a broad level and ends with an extensive list of hazard scenarios at each location within the complex. These are scenarios that could be potentially significant to risk and their corresponding worst case impact. The results from the spatial interaction phase of the overall analysis<sup>2</sup> identified over one hundred hazard scenarios.

---

\* This work was performed under the auspices of the U. S. Department of Energy.

\*\* Pickard, Lowe and Garrick, Newport Beach, California

These were screened based on their conditional core damage frequency and a number of these scenarios were retained for a more detailed analysis.

The detailed risk analysis stage<sup>3</sup> is itself a two-phase process. First, occurrence frequencies for the retained scenarios were estimated using actual commercial nuclear industry experience and HFBR specific experience. The unconditional core damage frequency for each scenario was determined, and the scenarios were then evaluated for the importance based on this frequency. Those scenarios that remain were evaluated in further detail in the second phase of the analysis by now considering the interactions between the hazards, mitigation features and other facility recovery actions. This "top-down" approach to risk assessment minimizes the effort in quantifying the risk associated with unimportant locations. Therefore, the scenarios that are identified during the spatial interactions analysis are as comprehensive as possible, and they remain at a manageable number for the subsequent detailed analyses. In practice, experience has shown that the two stages of the analysis must be closely coordinated and that they are somewhat iterative.

Fourteen fire scenarios were retained as a result of this approach; only three flood scenarios were found to be quantitatively significant. This pruning process was based on the utilization of generic data collected from a variety of databases.

#### **Database Development/Utilization**

A PLG database for fire events<sup>4</sup> provided the generic input for the assessment of fire event frequencies. This database contains summaries of more than 400 fire events that occurred through July 1987 at more than 65 U.S. nuclear power plant sites. These event summaries were derived from U.S. Nuclear Regulatory Commission (NRC) Licensee Event Report (LER) data, American Nuclear Insurer data, and plant-specific data that have been collected by PLG during previous PRA studies. The internal flooding event frequencies were derived from a similar PLG database for plant flooding events.<sup>5</sup>

A thorough review of the industry experience was used to develop a "specialized" generic database that accounts for design features of the HFBR and characteristics of the associated hazard sources. Special efforts were made to categorize fire events that involve equipment and occupancy unique to the HFBR facility.

The specialized generic database contained only those hazards events that were relevant to the HFBR for the specific operating conditions being evaluated, and for the specific scope of the functional impact locations and hazard sources that were considered in this analysis. The fire events were categorized into the following fire hazards sources:

- Battery-Related Fires
- Battery Charger-Related Fires
- Control Room-Related Fires
- Heating, Ventilating, and Air Conditioning (HVAC)-Related Fires
- Human Error-Related Fires
- Logic Cabinet-Related Fires
- Motor Control Center (MCC)- Related Fires

- Power and Control Cables-Related Fires
- Pumps-Related Fires
- Switchgear-Related Fires
- Transformer-Related Fires

The fire events were categorized into hazard source types instead of by location of occurrence. This approach provides a more realistic categorization of past events. We refer to these fire hazard types as component-based fire hazard sources and to the associated occurrence frequencies as the component-based fire frequencies.

In previous fire risk analyses, the industrial events were categorized according to the location of fires regardless of the actual plant component that was involved. Events that were categorized as auxiliary building fire events usually consisted of pump-related fires, motor generator-related fires, cable fires, and MCC-related fires that occurred in the auxiliary buildings. Similarly, switchgear room fire events included switchgear fires and any other fires that occurred inside the switchgear rooms of different nuclear power plants. Such an approach assumed that plant-to-plant variability of the content in different plant areas was low. The applicability of this approach is uncertain to plants that have different component contents in different plant locations compared to a "generic plant" in the industrial event database. Since the equipment content in HFBR is different from that of a generic nuclear power plant, a more rational application of the industrial event database was needed. The approach used categorized industrial events according to the fire initiators instead of plant location. For example, a pump-related fire in the auxiliary building of plant X is categorized as a pump-related fire event, and a cable-initiated fire in the auxiliary building of plant Y is categorized as a cable-related fire event. As a result, the fire events included in the HFBR specialized industrial event database were categorized according to the above component-based fire hazard source categories.

A two-stage Bayesian analysis was performed to combine this industry data with actual experience at the HFBR. The first stage of this analysis developed a generic frequency distribution for each hazard source that consistently accounted for the observed site-to-site variability in the industry experience data. The second stage updated this generic frequency to account specifically for the actual historical experience at the HFBR.

To account properly for the observed site-to-site variability in the industry experience data, it was necessary to have detailed information about the specific sites at which each event has occurred; e.g., site X has had N1 fire events of hazard type A in X1 years; site Y has N2 fire events of hazard type A in Y1 years; etc. Unfortunately, some of the industry data sources that compile hazard event reports do not identify the specific sites at which these events have occurred.

A probabilistic weighing process was used to consistently account for these unidentified hazard events within the framework of the first-stage Bayesian analysis. Several hypotheses were developed for each unidentified event.

The actual number depended on factors such as the observed variability in the identified plant experience and the actual number of unidentified events. Each hypothesis can result in a slightly different allocation of the total number of documented hazard events among the available plant sites. Each allocation is then input to the first-stage Bayesian analysis to develop a probability distribution that would apply for the hazard frequency if the corresponding hypothesis were true. Thus, a number of possible generic event frequency distributions were developed that corresponded to the number of hypotheses for the unidentified events. Each distribution was assigned a probabilistic weight that accounts for the likelihood that the corresponding hypothesis is true. The final generic probability distribution for the component-based hazard event frequency was obtained by merging the hypothesis distributions in a manner that preserves the underlying database uncertainty.

The development and evaluation of these hypotheses added a degree of complexity to the frequency analysis for some hazards. However, this complexity is justified by the fact that most hazard events are quite rare. For many hazards, the entire industry experience database contains fewer than 10 events. This is in contrast to other types of data that are used in the PRA, such as internal initiating events, component failures, and component maintenance events, for which hundreds or thousands of individual events may be documented. Thus, a single, unidentified hazard event may represent a relatively large fraction of the total documented experience base. A consistently conservative assignment of these events to the worst plants results in cumulative hazard frequencies that do not represent actual industry experience. On the other hand, simple removal of these anomalies may result in frequencies that are too optimistic. Consistent accounting for the unidentified events in the hypotheses-based approach provides the best available generic data, including the inherent uncertainties in those data.

Because of the lack of available operational data from plants similar to HFBR, the specialized generic component-based frequency was adjusted according to the smaller scale of the HFBR. To account for the difference, an approach was adopted that assumes a worst case scenario by retaining the upper bound associated with typical nuclear power plant generic data while reducing the median (50th percentile) to reflect a more realistic model of the HFBR. Based on the revised parameters, a new value for the lower bound (5th percentile) is determined. The revised generic prior distributions were then combined with applicable HFBR plant-specific experience via a Bayesian update to obtain component-based fire or flood frequencies.

### **Summary/Conclusions**

The fire events database used in this study summarizes incidents from a variety of sources: an NRC License Event Report, the American Nuclear Insurer, and plant-specific data collected from previous PRA studies.<sup>4</sup> Over 400 fire events were screened for HFBR-specific applicability. In this case applicability is determined by the composition of the HFBR with a typical commercial nuclear power plant.

The result of this screening forms the specialized generic database, a sample of which is shown in Table 1. For each fire event listed, information is included about fire initiator (equipment or fuel), location, cause, ignition source and type, affected equipment and comments regarding the applicability of this fire event to the HFBR scenario analyses.

As indicated previously, fourteen fire scenarios were analyzed in depth. Three flood scenarios were found from the screening process to be quantitatively significant. The total mean core damage frequency due to environmental hazards was  $4.15(10)^{-5}$  per year. The contribution from internal events is approximately an order of magnitude higher.

**References:**

1. Brookhaven National Laboratory, "Level 1 Internal Event PRA for the High Flux Beam Reactor," prepared for the U. S. Department of Energy, Rev. 1, July 1990.
2. Johnson, D. H., et al., "Spatial Interactions Analysis of the High Flux Beam Reactor," prepared for Brookhaven National Laboratory, PLG-0823, PLG, Inc., August 1991.
3. Ho, V. S., et al., "Risk Analysis of the Environmental Hazards at the High Flux Beam Reactor, prepared for Brookhaven National Laboratory, PLG-0906, PLG, Inc., January 1993.
4. Pickard, Lowe and Garrick, Inc., "Database for Probabilistic Risk Assessment for Light Water Nuclear Power Plants," Proprietary, PLG-0500, Vol. 8, July 1989.
5. Pickard, Lowe and Garrick, Inc., "Database for Probabilistic Risk Assessment for Light Water Nuclear Power Plants," Proprietary, PLG-0500, Vol. 9, July 1989.

Table 1. HFBR Specialized Generic Fire Event Database

Category	PLG Index	Plant	Incident Date	Operation Mode	Fire Location	Fire Initiators	General Description	Comments
Battery	190	Robinson Unit 2	07/16/78	Power Operation	Battery Room	Battery	Plastic tops of two operation cells of a station battery caught fire; caused by resistance heating of a terminal connection during the heavy DC load of the emergency oil pump.	Include in HFBR fire empirical experience database.
	217	Palisades	04/04/79	Power Operation (100%)	Battery Room	Battery	A test lead being used to take battery voltage readings fell and struck a battery connector, causing a spark that ignited hydrogen gas.	Include in HFBR fire empirical experience database.
Battery Charger	320	Brunswick Unit 1	11/27/82	Power Operation (68%)	Battery Room	Capacitor	Battery charger capacitor caught fire for unknown reason.	Include in HFBR fire empirical experience database.
	357	Duane Arnold	08/02/85	Power Operation	Switchgear Room	Capacitor	A failing capacitor in an RCIC static inverter caused RCIC to be inoperable and failure of a reactor level indicator.	Include in HFBR fire empirical experience database.
Control Room	225	Three Mile Island Unit 2	07/12/79	Cold Shutdown	Control Room	Resistor	Overheated resistor caused rfire in a radiation-monitoring readout panel. Fire was extinguished immediately.	Include in HFBR fire empirical experience database.
	323	McGuire Unit 2	02/19/83	Construction	Control Building	Fan	Household fan caught fire in the control building. Smoke propagated to control room area.	Not applicable; construction event and fire-initiated equipment not found in HFBR.
	397	Dresden Unit 2	11/01/81	Power Operation	Control Room	Relay	Defective relay burnt out. Fuse blown. Relay replaced	Not applicable; factory defective relays, component failure only, not an actual fire event.
	398	Hatch Unit 1	12/01/81	Power Operation	Control Room	Relay	Loose terminal connection shorted; insulation overheated. No additional damage resulted.	Not applicable; fire precursor only, not an actual fire event.
HVAC	338	Unknown	04/22/84	Construction	Other Building	Air Conditioner	Short circuit in wall-mounted air conditioning unit caused the fire.	Not applicable; construction event.
	348	Unknown	11/21/84	Construction	Temporary Building	Air Conditioner	Air conditioner in trailer overheated and ignited.	Not applicable; construction event.
Logic Cabinet	129	Unknown PWR	05/15/76	Power Operation	Auxiliary Building	Cabinet Cover	Electrical short ignited a plastic covering on instruments. Fire put out by employees with portable dry chemical.	Include in HFBR fire empirical experience database.

## A MODEL FOR FUEL FIRE DURATION AND APPLICATION TO THE B-1B BOMBER\*

Douglas E. Magnoli

Lawrence Livermore National Laboratory  
P.O. Box 808, L-85  
Livermore, CA 94551

### INTRODUCTION

A model for determining the duration of a fuel-spill fire was developed. The scenario is that a parked fuel-and-weapon-laden system suffers damage that includes a hole in a fuel tank and that the spilling fuel ignites. Duration of the whole fire is not the focus of the model. What is of interest is duration at a nearby weapon storage point, which may be significantly remote from the spill location.

The model derives duration as a function of several parameters, including the size of the fuel spill hole, the distance between the spill point and the point of interest, the amount of fuel available, and the form of the fuel tank that is spilling fuel. The effects of wind and of fire-fighting efforts are not considered in this study. Spilling from more than one fuel tank is not examined.

The model is applied to the B-1B bomber. Model application to a specific system fixes some of the parameters. Fire duration at the weapons bays can thus be derived as a function of (1) the size of the hole from which the fuel is spilling and (2) the spill location on the aircraft. Parameter 1 determines how fast the fuel spills and thus how large the fire will be. Parameter 2 determines which tank the hole is in and therefore how much fuel is available, how much hydrostatic head there is, and how far the hole is from the weapons bay.

### METHOD

#### Spill Rate as a Function of Time

Assuming a cylindrical fuel tank with a hole in the bottom, define

- $S = S(t)$  = fuel spill rate as a function of time
- $h_0$  = initial average height of fuel in tank
- $h = h(t)$  = average height of fuel in tank at time  $t$
- $t_{final}$  = time at which tank is empty
- $A_1$  = tank area in a plane parallel to the ground
- $A_2$  = area of hole
- $v_1 = -dh / dt$

---

\* Work performed by Lawrence Livermore National Laboratory under the auspices of the U.S. Department of Energy under contract number W-7405-ENG-48.

$v_2 = v_2(t)$  = velocity of fuel through the hole  
 $g$  = acceleration due to gravity

then continuity requires that

$$S = A_1 v_1 = -A_1 \frac{dh}{dt} = A_2 v_2. \quad (1)$$

Assuming atmospheric pressure inside the tank\* and that  $A_2 \ll A_1$ , then

$$v_2 = \sqrt{2gh} \quad , \quad (2)$$

which leads, after substitution into equation 1, to

$$\frac{dh}{\sqrt{h}} = \frac{-A_2 \sqrt{2g}}{A_1} dt. \quad (3)$$

Integrating and setting the constant of integration gives

$$2\sqrt{h} + 2\sqrt{h_0} = \frac{A_2}{A_1} \sqrt{2g} \, t \quad , \quad (4)$$

which can be solved for  $h$  and substituted, via equation 2, into equation 1 to give spill rate as a function of time

$$S = A_2 v_2(t) = A_2 \sqrt{2gh} = A_2 \left( \sqrt{2gh_0} - \frac{gA_2}{A_1} t \right). \quad (5)$$

The duration of the spill can be determined by recognizing that  $h = 0$  when  $t = t_{final}$ , i.e.,

$$t_{final} = \frac{A_1}{A_2} \sqrt{\frac{2h_0}{g}} \quad . \quad (6)$$

### Fire Radius

In the absence of wind, and on a level surface, it is assumed that the fire will be circular, centered around the spill location. Because fuel from a spill will spread very fast, it is assumed that the fire radius reaches its equilibrium size instantaneously; that is, that fuel is consumed by the fire at the same rate that it is supplied to the pool. It is also assumed that the burn rate, the height of the pool burned per unit time, is constant, so that the equilibrium size of a fire depends only on spill rate.<sup>1-5</sup> When this is true,

$$S = \pi r^2 \dot{v} \quad , \quad (7)$$

where

$$r = r(t)$$

= fire radius

$\dot{v}$  = burn rate of fuel, expressed as pool height burned per unit time

---

\* The fuel tanks on many vehicles (including the B-1B) are connected to the atmosphere via a valve that allows air to flow in or out of the tanks to adjust for changes in fuel volume due to thermal expansion.



Solving for  $r$  and substituting from equation 5,

$$r = \sqrt{\frac{S}{\pi \dot{v}}} = \sqrt{\frac{A_2}{\pi \dot{v}}} \left( \sqrt{2gh_0} - \frac{gA_2}{A_1} t \right)^{\frac{1}{2}} \quad (8)$$

Assuming that the fuel pool is always at equilibrium size, then the behavior of the pool radius follows that of the spill rate. The pool radius is maximum at  $t = 0$  and decreases thereafter. A more detailed analysis\* shows that the equilibrium-size assumption is reasonable.<sup>6</sup>

If the weapons are stored at a known distance from the position of the fuel leak, then the time that the weapons will be engulfed in the fire can be determined. Solving equation 8 for  $t$  gives

$$t = \frac{A_1}{gA_2} \left( \sqrt{2gh_0} - \frac{\pi \dot{v} R^2}{A_2} \right), \quad (9)$$

where

$R$  = distance from the spill point to the weapons.

**Determination of the Value of  $\dot{v}$ .** Available values for  $\dot{v}$  vary within a narrow range. Literature values<sup>1,2</sup> range from about 0.3 cm/min to about 0.6 cm/min. Mansfield<sup>3</sup> has empirically discovered the relation

$$D = 3.5\sqrt{S}, \quad (10)$$

where

$D$  = pool diameter in feet

$S$  = spill rate in gallons/minute

which gives a value for  $\dot{v}$  of 0.42 cm/min, about the average of the other two values. Except for cases where  $R$  is small, examination of the behavior of theoretical fires with values for  $\dot{v}$  of 0.3 cm/min and 0.6 cm/min shows only slight variations in the results.<sup>6</sup> This indicates that fire duration at larger distances is not greatly sensitive to the precise value used for  $\dot{v}$ . Examination of equation 9 reveals that, according to this model, the duration of a spill fire is dependent only on the rate at which the tank empties, not on the burn rate. The consequence of a smaller burn rate is not a longer fire, but a larger one (see equation 8), and therefore one that may persist at a distance for a longer time.

## APPLICATION TO THE B-1B BOMBER

### Description of the B-1B

The B-1B has ten fuel tanks as shown in Table 1. For this model, the important parameters for each tank are volume, area perpendicular to the ground, average fuel height, and tank footprint, i.e., where the tank begins and ends on the aircraft. This data is shown in Table 1.

The B-1B also has three nuclear weapons storage areas, each capable of carrying one rotary launcher. Table 1 also gives the locations of the weapons bays on the aircraft.

\* Reference 6 provides much more detail on the work presented here.

**Table 1.** Characteristics and positions of fuel tanks and weapons bays of the B-1B bomber.

Tank or weapons bay (number)	Volume (m <sup>3</sup> )	Avg. Height (m)	Average Area (m <sup>2</sup> )	Start Position (ft) <sup>a</sup>	End Position (ft) <sup>a</sup>
Forward (2)	9.1	1.5	6.1	37.6	63.4
Forward intermediate (2)	11.0	1.5	7.3	63.4	79.6
Main (2)	6.0	1.5	4.0	79.6	84.6
Aft intermediate	13.8	1.8	7.7	88.8	111.2
Wing (2)	8.8	0.5	17.6	See note b	See note b
Aft	30.2	1.8	16.8	112.2	132.0
Forward weapons bay	—	—	—	47.4	62.4
Intermediate weapons bay	—	—	—	63.9	78.9
Aft weapons bay	—	—	—	96.9	111.9

<sup>a</sup> Start and end positions measure how far along the fuselage from the nose of the aircraft a tank or weapons bay begins and ends.

<sup>b</sup> Wing tanks show no entries in these columns because they are not located along the fuselage. These tanks are neglected in this treatment because of the small amount of fuel they hold.

## Results

A computer model was constructed to examine fire duration at the centerpoint of both the intermediate and aft weapons bays as a function of hole size and position of the fuel leak along the fuselage. Because the fuselage is only 14.5 ft wide, leak position perpendicular to the length of the fuselage was not considered.

Intuition suggests that if the hole is small, it will result in a fire that lasts a long time but never gets very large. Conversely, if the hole is large, the fuel will spill quickly, resulting in a large fire that does not burn for very long. The danger zone will lie between these extremes. Experimenting with the model reveals that hole sizes less than 1 cm<sup>2</sup> always give rise to fires of radius  $\leq 0.25$  m. Furthermore, holes larger than 100 cm<sup>2</sup> always result in fires that include the weapons bays for under 20 min.

To provide a statistical analysis of fire duration, it is necessary to have statistical distributions that describe the frequency of different hole sizes and spill position. In the absence of such data, uniform distributions were assumed for hole size (varied from 0.1 cm<sup>2</sup> to 100 cm<sup>2</sup> in 0.1-cm<sup>2</sup> increments) and for spill position (varied from 38 ft to 132 ft from the nose of the aircraft, spanning the entire fuel-carrying portion of the fuselage, in 1-ft increments). Fire durations were calculated for each pair of parameter values; i.e., for 91,000 fires.\* Calculations were done for values of  $\dot{v}$  of both 0.3 and 0.6 cm/sec for both the aft and intermediate weapons bays. One set of these results is presented in Table 2. Notice that small hole sizes give rise to fires that do not extend very far, whereas large hole sizes result in fires of short duration.

The results were sorted to determine what fraction of the 91,000 fires engulfed at least one weapons bay for various lengths of time. Results of this analysis are presented in Table 3. It is important to recognize that the *absolute* values of these results are influenced by the set of fires examined. For example, if hole sizes had been chosen over a range of 0.001 cm<sup>2</sup> to 1 m<sup>2</sup>, the fraction of fires engulfing the weapons bays would have been different from that found here. However, the differences would arise from contributions due to very small hole sizes and from very large hole sizes, so that the resulting distribution would

\* There is no fuel tank between 84.6 and 88.8 ft from the nose of the aircraft (see Table 1).

**Table 2.** Fire duration (minutes) at aft weapons bay of B-1B as a function of hole size and leak position (distance from aircraft nose) for the case when  $\dot{v} = 0.6$  cm/min.

Position (ft)	Hole size (cm <sup>2</sup> )						
	0.1	0.32	1	3.2	10	32	100
88	0	0	0	0	0	0	0
92	0	0	0	0	19	19	7
96	0	0	0	0	51	22	7
100	0	0	36	171	70	24	8
104	7150	2393	770	245	78	25	8
108	0	0	281	196	73	24	8
112	0	0	0	25	56	22	8
116	0	0	0	0	57	42	16
120	0	0	0	0	0	33	15
124	0	0	0	0	0	22	14
128	0	0	0	0	0	7	12
132	0	0	0	0	0	0	11

**Table 3.** Cumulative probability function of fire durations at B-1B bomb bays: proportion of 91,000 fires having a duration longer than a specified time at any weapons bay.

Duration	$\dot{v}=0.3$ cm/min	$\dot{v}=0.6$ cm/min
Fire never reaches weapons bay	0.0652	0.1309
> 0 min	0.9348	0.8691
> 30 min	0.1752	0.1181
> 1 hr	0.0590	0.0383
> 2 hr	0.0192	0.0114
> 3 hr	0.0095	0.0062
> 4 hr	0.0057	0.0040
> 5 hr	0.0040	0.0028
> 6 hr	0.0031	0.0022
> 7 hr	0.0024	0.0017
> 8 hr	0.0020	0.0014
> 9 hr	0.0017	0.0012

show more very long fires and more very short fires. However, the *relative* values of fraction of fires of a given duration would remain the same for fires longer than 20 min and for fires shorter than several hours. Comparisons among the data thus remain valid.

Notice that Table 3 shows the expected behavior of fire duration at the weapons bays with variation of  $\dot{v}$ : the larger value of  $\dot{v}$  results in fires that are larger and therefore burn out more quickly, so that the weapons are exposed to fire for a shorter period of time.

It is useful to compare the results of this model with actual data. Overall fire duration data for civilian aircraft fires was used for comparison because such data are more available than data for military aircraft.<sup>7</sup> This comparison is presented in Fig. 1, which also shows total fire duration derived from this model. The figure demonstrates reasonable agreement between the results of the model and the data.

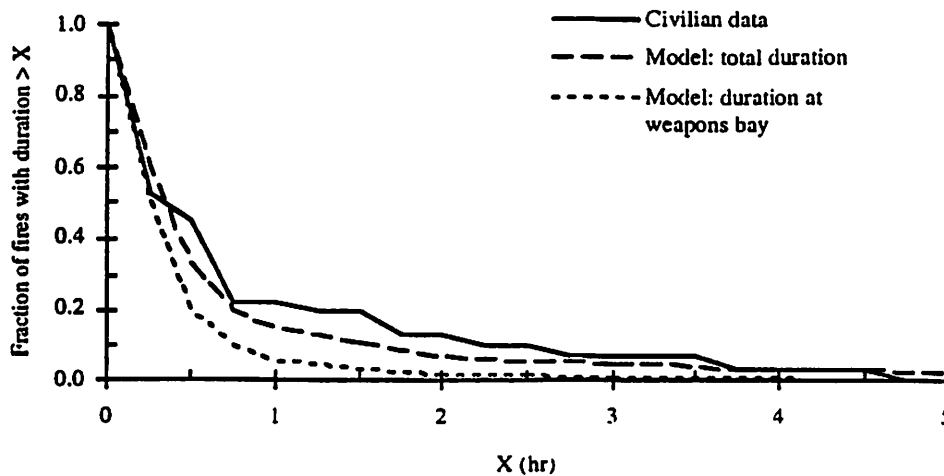


Figure 1. Comparison of model results for fire duration with duration of civilian aircraft fires. Model results shown here are for the case where  $\dot{V} = 0.3$  cm/min.

## CONCLUSIONS

Given a fuel fire of consequence,\* the frequency of fires that engulf the weapons bays for under an hour is relatively large—on the order of 0.95 for the cases considered here. However, fewer than 6% of the fires engulf a weapons bay for over an hour, and fewer than 2% engulf a weapons bay for over 2 hr. From the point of view of designing fire-resistant nuclear warheads, increasing fire resistance from 1 hour to 2 hours, for example, results in resistance to approximately 4% more fires [i.e.,  $(0.06 - 0.02) / 0.95$ ]. Because this conclusion depends on exactly which fires are deemed “of consequence,” a more valid conclusion, drawn only from comparing data for different durations, is that such an increase in fire resistance capability makes the weapon able to withstand about 70% [i.e.,  $(0.06 - 0.02) / 0.06$ ] of the fires to which a 1-hr fire-resistant weapon is vulnerable.

## ACKNOWLEDGMENTS

The efforts of Werner Stein and Al Kaufman, both of Lawrence Livermore National Laboratory, are gratefully acknowledged. Messrs. Stein and Kaufman helped to develop some of the concepts used here and provided some of the mathematical relationships.

## REFERENCES

1. M.E. Schneider and L.A. Kent, *Measurements of Gas Velocities and Temperatures in Large Open Pool Fire*, Sandia National Laboratories (undated).
2. Blinov and Khudyakov, *Proc. Acad. Sci. USSR*, 113:241 (1957).
3. J.A. Mansfield and L.J. Linley, NWC TP 7061, *Measurement and Statistical Analysis of Flame Temperatures from Large Fuel Spill Fires* (1991).
4. W. Stein, Lawrence Livermore National Laboratory, private communication.
5. H. Kölbl, *Chem.-Ing.-Tech.*, 50:573 (1978).
6. D.E. Magnoli, *A Model for Fuel Fire Duration and Application to the B-1B Bomber*, Lawrence Livermore National Laboratory, UCRL-ID-112576 (1992).
7. R. Mensing, Lawrence Livermore National Laboratory, private communication.

\* Arbitrarily defined here as a fire greater than 0.25 m in initial radius and lasting longer than 20 minutes, and therefore arising from a hole between 0.1 and 100 cm<sup>2</sup> in size.

## **IMPLEMENTATION OF THE FIVE METHODOLOGY: RESULTS AND LESSONS LEARNED**

Robert C. Lindquist<sup>1</sup> and Michael S. Powell<sup>2</sup>

<sup>1</sup> Reliability & Risk Analysis Group

<sup>2</sup> Nuclear Projects Department

(formerly Manager Fire Protection Support Service)

Arizona Public Service Company

P. O. Box 52034

Phoenix, Arizona 85672-2034

### **INTRODUCTION**

On July 5, 1990, the NRC issued a draft Generic Letter 88-20, Supplement 4 and NUREG-1407, which detailed the procedural and submittal guidance for responding to the Individual Plant Examination for External Events (IPEEE). As a result, the Nuclear Management and Resources Council (NUMARC), through its Severe Accident Working Group (SAWG) coordinated the investigation of the scope of severe accident risk from fires, fire protection design and programmatic features in nuclear power plants and concluded that:

1. Certain aspects of current fire PRA methods are not as robust as those for internal event PRAs, and
2. Each plant has already expended tremendous analytical and plant change efforts enhancing their fire protection capabilities in response to the 10 CFR 50 Appendix Rule.

The NUMARC SAWG concluded that development of a more cost-effective and efficient examination methodology based on implementation as an alternative to the normal PRA process would be of benefit to the industry. At the request of NUMARC, the Electric Power Research Institute (EPRI) sponsored the preparation of the Fire Induced Vulnerability Evaluation (FIVE) as acceptable methodology for examining the potential for severe plant accidents for fire-initiated events. The Palo Verde Nuclear Generating Station (PVNGS) was the lead PWR demonstration plant for implementation of FIVE. The procedures and worksheets provided in the FIVE methodology were used extensively as the basis for the PVNGS fire evaluation. The FIVE Methodology provided the guidance for performing the examination of potential plant severe accidents caused by fire-initiated events. FIVE uses a general industry fire events database in combination with deterministic and probabilistic techniques for examining a power plant's fire probability and protection characteristics.

## METHODOLOGY

The FIVE Methodology consists of a two-phase progressive screening method and a third phase consisting of a plant walkdown/verification process. The first two phases are composed of a fire area screen and a critical compartment screen.

The initial phase or fire area screen assumes an exposure fire in each fire area and then looks at the ability of the plant to achieve and maintain a safe shutdown given that the normal redundant or alternate safe shutdown path is assumed to be unavailable as described in reference 1. The Appendix R safe shutdown analysis is used in this phase, since the equipment and circuits have been separated, protected and/or analyzed such that a single postulated fire would not impact the redundant safe shutdown path. Fire areas are then screened out if the area did not contain Appendix R safe shutdown components or a postulated fire in the subject fire area does not cause a demand for safe shutdown. Table 1 provides a listing of those fire areas screened out during the Phase I evaluation. Table 2 provides those fire areas which could not be screened out during the Phase I evaluation.

The second phase, or fire compartment screen, begins with taking each fire area in Table 2 and subdividing them into compartments where a fire's hot gas layer would be confined as stated in reference 2. The objective of this phase is to estimate the temperature rise and likelihood of damage to those safe shutdown components in the subject fire compartment or the likelihood of the fire spreading to an adjacent compartment as described in detail in reference 1. During this phase, fire compartments are to be screened out based upon configuration (e. g. concrete walls prohibit the spread of fire; low combustible loading, etc...). This phase also identified those fire compartment boundaries with the potential for fire spread (e. g. cable trays through unsealed openings; high combustible loading, etc...) as well as those fire areas with multi-compartment potential. Fire compartments unscreened at this stage are then analyzed using probabilistic risk assessment techniques to determine a core damage frequency (CDF) based on the effects of a fire originating in each compartment, assuming everything in the compartment is destroyed by the fire, and the unavailability of the redundant or alternate safe shutdown equipment. As a result of this phase, Table 3 provides those fire compartments that could not be screened out after completion of the Phase II evaluation.

## RESULTING EVENT SCENARIO

During the Phase II analysis it was determined that because Palo Verde Nuclear Generating Station (PVNGS) Unit One has the controls for all the intermediate switchgear breakers and most of the 525kV breakers, a postulated fire in certain areas of Unit One could have an impact on the operation of the other two PVNGS units. Subsequent evaluations have confirmed that the potential exists for a fire to trip all 525kV breakers, except the Unit Two and Unit Three generator output breakers. Figure 1 illustrates the potential effect of tripping these breakers. Units Two and Three would remain tied to the West Wing (WW) 2 and North Gila lines, respectively, and they would be paralleled on the West Bus. The potential exists though for a loss of offsite power to the Units Two and Three and their respective ESF Busses.

The areas within PVNGS Unit One where such a postulated fire could have this impact are the Board One (B01) area of the Control Room, the upper cable spreading room directly above B01 and over to the east wall, and the BOP cable shaft in the Corridor Building. Applying the FIVE methodology to the Cable Spreading Room eliminated this area as a significant core damage contributor. This left the Control Room and the BOP cable shaft as areas that deserved further consideration.

## **ACTIONS TO ADDRESS THE POTENTIAL VULNERABILITIES**

Although the probability of most of the switchyard breakers opening is remote, we took the following actions to address the potential vulnerability that was identified.

1. Performed a grid stability analysis to show that the grid would remain stable and that the other two PVNGS units can remain on line with house loads supplied by their own generation through the auxiliary transformer.
2. Included the Corridor Building within the site programs that control combustible material and ignition sources.
3. Developed procedures for both PVNGS and Salt River Project (operator of the switchyard) to disconnect the 525V breaker remote circuitry to Unit One and reclose the breakers locally in a systematic manner to restore the proper switchyard breaker alignment and offsite power to the units.

These actions were implemented in order to minimize the probability of occurrence and to optimize the response to mitigate the vulnerability.

## **LESSONS LEARNED**

1. FIVE allows quick screening of fire areas with very low fire-induced risk using the conservative Appendix R analyses.
2. Just as in the internal events IPE, off-site power plays a crucial role in mitigating any transient or accident. A fire-induced loss of off-site power has a significant impact on CDF. Fire in areas or compartments where the availability of off-site power may be impacted should be examined when performing FIVE, even if no Appendix R safe Shutdown equipment is impacted.

Table 1:

PHASE I FIRE AREAS SCREENED OUT		
FIVE FIRE AREA	DESCRIPTION	REASON
VI	Fuel Building	Separate Bldg. with No Safe Shutdown Components
VI	Diesel Gen. - A	Fire will not result in demand for shutdown
V	Diesel Gen. - B	Fire will not result in demand for shutdown
VII	Spray Pond Pumphouse - A	Fire will not result in demand for shutdown
VIII	Spray Pond Pumphouse - B	Fire will not result in demand for shutdown
IX	CST Pumphouse	Separate Bldg. with No Safe Shutdown Components
X	Radwaste Building	Separate Bldg. with No Safe Shutdown Components
XI	Containment Building (See 5.1)	Fire Events Database indicated a very low fire frequency in Containment while the plant is operating.
XVIII	Diesel Fuel Storage Tank - A	Fire will not result in demand for shutdown
XIX	Diesel Fuel Storage Tank - B	Fire will not result in demand for shutdown
	General Outdoor Areas	No Safe Shutdown Components or exposure to important bldgs.



Table 2:

PHASE I - SIGNIFICANT FIRE AREAS REQUIRING FURTHER EVALUATION	
APPENDIX R FIRE AREA	DESCRIPTION
I	Control Building - A
II	Control Building - B
III	Control Room
XII	Main Steam Support Structure
XIII	SI-HPSI/LPSI-A (Zones 30A, 31A, 32A)
XIV	SI-HPSI/LPSI-B (Zones 30B, 31B, 32B)
XV	Auxiliary Building - General
XVI	Electric Pen. Rooms - A (Zones 42A, 47A)
XVII	Electric Pen. Rooms - B (Zones 42B, 47B)
--	Corridor Building
--	Turbine Building
--	Turbine Switchgear/DC Equipment Building
--	Station Transformers

Table 3:

FIRE AREA	FIRE Compt.	DESCRIPTION
II	86B	Gap Between Aux. & Cont. Bldg.
--	--	Corridor Building Cable Shaft
--	--	Corridor Building
--	TB-4	Turb. Bldg. Switchgear/DC Equipment Room
--	--	Turbine Building
--	--	Outdoor Walkway
II	-- 86B	Corridor Building/Gap between Aux. & Cont. Bldg.
--	--	Corridor Building
--	--	Corridor Building Shaft

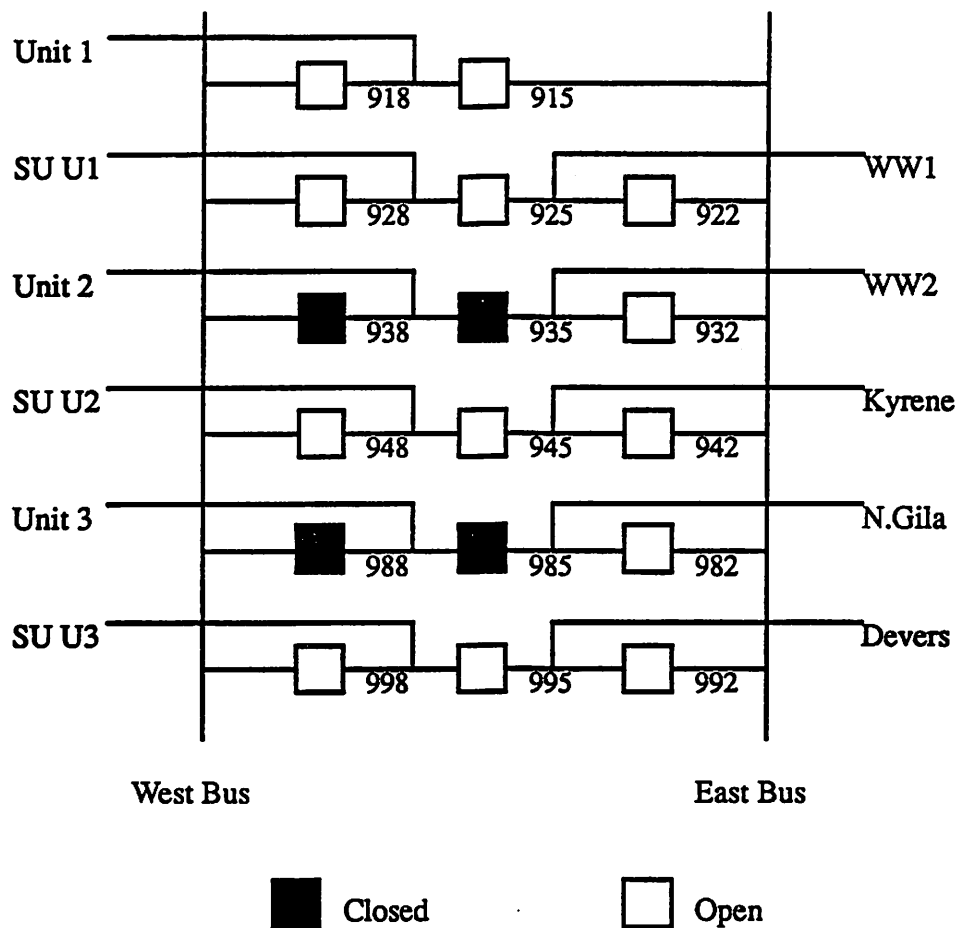


Figure 1 - PVNGS Switchyard

## REFERENCES

1. Professional Loss Control, Inc., "Fire Induced Vulnerability Evaluation (FIVE)", EPRI Report TR-100370 April 1992
2. C. A. Ksobiech, L. P. Herman, "Fire Induced Vulnerability Evaluation (FIVE) for Palo Verde Nuclear Generating Station Arizona Public Service Company" Draft (1991)

## **FIRE RISK ASSESSMENTS AT ROCKY FLATS PLANT**

**Terry L. Foppe and Edwin Stahlnecker**

**Nuclear Safety Engineering Department  
EG&G Rocky Flats, Inc.  
P.O. Box 464, Building T886B  
Golden, CO 80402-0464**

### **INTRODUCTION**

The Rocky Flats Plant (RFP) is a government-owned and contractor-operated facility, which is part of the nationwide nuclear weapons production complex managed by the U.S. Department of Energy (DOE). RFP is located in Colorado about 16 miles northwest of downtown Denver. The plant site encompasses about 10 square miles of federally-owned land with the major structures located within a half square mile section. The remainder of the land serves as a buffer zone between the processing facilities and the general public.

RFP was primarily involved with metal fabrication, assembly, and chemical processing associated with the nuclear weapons program and other work directly related to national defense. Activities included numerous metalworking, fabrication, and assembly shops; chemical recovery and purification processes; and associated quality control functions. This involved materials such as plutonium (Pu), enriched and depleted uranium, beryllium, and various alloys of stainless steel.

The hazards and associated risks from potential accidents involving the handling of fissile or other hazardous materials have been analyzed. One of the greatest hazards is that of fires due to the pyrophoric nature of certain forms of Pu. RFP has had a high frequency of small fires that did not result in the loss of confinement of radioactivity. However, two significant industrial fires involving Pu manufacturing occurred in 1957 and 1969. Lessons learned from these events resulted in substantial upgrading of fire prevention and fire protection programs, such as providing an inert atmosphere for operations that involved pyrophoric forms of Pu, eliminating combustibles inside gloveboxes and within the production areas, installing fire detection systems (e.g., contact heat detectors for storage locations, ambient atmosphere detectors inside gloveboxes), and installing fire suppression systems (e.g., wet pipe sprinklers for production areas and automatic deluge systems to protect exhaust high efficiency particulate air [HEPA] filter plenums). Additionally, administrative controls

were enhanced (e.g., training, procedures, hot work permits) and response capabilities were strengthened (e.g., building fire brigades, full time onsite fire department).

The success and failure of these engineered and administrative controls were evaluated in the process of assessing risk from Pu fires to the public for the facilities' Final Safety Analysis Report (FSAR) required by DOE Orders 5481.1B (DOE, 1987) and 5480.23 (DOE, 1992). Since the FSARs were approved by DOE, additional fire risk assessments were performed which include: (1) an Unreviewed Safety Question Determination (USQD) addressing redundancy of glovebox heat detectors; (2) rebaselining risk estimates for resumption of Pu production operations; and (3) assessing the risk for thermal stabilization of Pu to support RFP's changing mission of decontamination, decommissioning, and environmental restoration. The probability of occurrence, radiological consequence, and risk of Pu fires were assessed using probabilistic risk assessment techniques.

## FSAR FIRE RISK ASSESSMENTS

Fire risks were assessed for the FSARs by application of event tree analyses. Initiating event probabilities of occurrence and mitigating system (e.g., vital safety systems or administrative controls) failure probabilities (e.g., unavailabilities) were determined by fault tree analysis or statistical analysis of RFP incident or surveillance data. Methodologies were documented in the *Rocky Flats Risk Assessment Guide* (EG&G, 1992) which was developed from commercial nuclear reactor and chemical industry risk assessment techniques. Fire hazards and their controls were identified and grouped into categories that would be representative in terms of likelihood and consequences. Those potential fires which would result in negligible consequences, or whose probability of occurrence was not considered credible (i.e.,  $> 1 \times 10^{-6}$ /year) were screened from further evaluation. These grouped initiating events requiring further evaluation included fires initiated in similar processes in gloveboxes, fires in other inert atmosphere gloveboxes, fires in air atmosphere gloveboxes, fires in process rooms, fires in utilities areas, and fires on shipping and receiving docks. The success and failure of mitigating systems modeled included absence of combustible materials in gloveboxes and rooms to propagate a fire, confinement capability of gloveboxes, emergency responses by operators or the Building Emergency Support Team, emergency response by the RFP Fire Department, and suppression by the room wet-pipe automatic sprinklers. Other safety systems were assumed to function because including their failure would result in accident sequences with such low probabilities that they would not be risk significant. These systems included heat detection in gloveboxes, exhaust plenum automatic deluge systems, glovebox and room ventilation and filtration systems, and normal and emergency power, and room fire barriers to limit damage to one fire zone.

Accident sequences were defined by a particular path through the event tree based on either the success or failure of the mitigating systems. However, considering the uncertainty of the calculated probabilities, those sequences with a probability of occurrence greater than  $1 \times 10^{-8}$ /year were included if they increased the overall risk for the accident scenario by more than 10%. Those accident sequences which were determined to be credible were then analyzed for radiological consequences and risks.

Radiological consequences were determined by estimating an amount of material at risk as determined by the accident sequence, appropriate release fractions (i.e., fraction that becomes airborne due to the thermal stress and behavior of the form of Pu involved) which were based on experimental results or recommended in the literature, and applying leakpath factors from the glovebox. This initial source term

released to the room was used to assess risk to the workers, and was also modified by a leakpath factor from the building (e.g., two or four stages of high efficiency particulate air filtration) to estimate the building source term released to the environment. Mean dose to a hypothetical maximum offsite individual and health effects to the population were modeled with Gaussian dispersion methods based on a "star deck" of wind speed, stability class, and direction.

Mean doses and health effects were combined with the probability of occurrence of the accident sequence to establish a mean risk estimate. Accident sequence risks were summed to establish mean risk for the accident scenario and a composite risk estimate for all accidents. Distributions of radiological consequences were combined with the probability of occurrence to present risk curves. Risk comparisons were then made by comparing mean risks to risks from background radiation, and by comparing risk curves to those from the WASH-1400 Reactor Safety Study (NRC, 1975).

## **REDUNDANCY OF GLOVEBOX HEAT DETECTORS**

Lack of redundant ambient atmosphere heat detectors was analyzed as part of a USQD risk assessment. The USQD process complies with DOE Order 5480.21 (DOE, 1991a) to assure that proposed changes to the facility and procedures are appropriately evaluated and approved. This process maintains the safety envelopes defined by the facilities' FSAR accident analysis. The current USQD approach used at RFP is based on the commercial nuclear power industry standard NSAC/125 (EPRI, 1989).

The USQD dealing with the lack of redundant ambient atmosphere heat detectors was initiated as the result of an audit that challenged the FSAR redundancy assumption of detector placements, and that some gloveboxes only had a single heat detector. Performance of the USQD risk assessment included an assessment of the availability of either single or redundant heat detectors by use of a fault tree analysis, evaluating both hardware failures and human errors during periodic surveillances.

Also questioned was the validity of using historical plant surveillance data in calculating the unavailability for ambient atmosphere heat detectors. This resulted in a re-evaluation of the unavailability for ambient atmosphere heat detectors using commercial industry failure rates and surveillance intervals as inputs to the fault tree analysis. A sensitivity analysis on the effects of having supervisory circuitry and other features were also modeled in the fault trees.

Results of the fault tree analyses were then incorporated into existing event tree analyses to determine the affect on the probability of occurrence and risk of accident sequences. The adjusted probability of occurrence and risk values were compared to the original values to see if significant changes had occurred.

Based upon the fault tree analyses and the dominant accident sequence probabilities of occurrence and risk estimates, it was concluded that an unreviewed safety question did not exist. This was because the revised risk estimates related to glovebox fires were bounded by risks from dock fires.

## **REBASELINING FIRE RISK ESTIMATES FOR RESUMPTION OF PU PRODUCTION OPERATIONS**

Pu production operations at RFP were curtailed in late 1989 by DOE so that a new operating contractor, EG&G Rocky Flats Inc., could assess the safety of resuming Pu operations and implement a new safety culture. In order to establish an

interim authorization basis to allow resumption of Pu operations, several facilities' FSARs were reviewed. Several resumption teams were established to assess the safety of resuming Pu operations, and the adequacy of their safety analyses, Operational Safety Requirements, and vital safety systems. Specifically, Resumption Team 3, assessed RFP Pu operations to provide assurance that resumption of operations would be in a manner consistent with the approved radiological consequence safety envelopes. Other resumption teams and efforts concentrated on enhancing or establishing programs to effect a new safety culture consistent with commercial and government nuclear industry practices for power reactor facilities.

A risk assessment was performed in support of resuming Pu production operations. Part of this resumption effort involved the rebaselining of several Pu facility safety analyses. This effort included documenting the original FSAR risk assessment assumptions and calculations concerning fire risk estimates. If inconsistencies or errors were identified, risk estimates were rebaselined and a sensitivity analysis was performed to determine their impacts. Event trees were updated or new ones were developed to reflect changes in assumptions on accident progression and availability of more recent data on failure probabilities or initiating event probabilities of occurrence. Radiological source terms were revised to reflect changes in assumptions for the amount of material at risk, accident release fractions, and building leakpath factors. Radiological consequences and risks were analyzed with the MELCOR Accident Consequence Code System (MACCS) computer code (Chanin, 1990) to estimate impacts to the public.

The major changes to fire risk involved a significant increase in probabilities of occurrence for some fire scenarios. However, this did not substantially impact fire risks because of a substantial decrease in the probability of occurrence of a dock fire which was the dominant contributor to the overall fire risks. The revised risk curves were compared to the reactor accident risk curves from NUREG-1150 (NRC, 1990).

## **FIRE RISK ESTIMATES FOR THERMAL STABILIZATION OF PU**

The latest fire risk assessment was performed in support of the changing mission for RFP to one of decontamination, decommissioning, and environmental restoration. An operation to support this mission is the thermal stabilization of Pu by electrical heating in an air environment to eliminate its pyrophoric hazards. Fire risks associated with this process, as well as other activities to maintain the buildings safety envelope, were assessed as an addendum to the rebaselining effort for the resumption of Pu production operations mentioned above.

Accident scenarios analyzed in the rebaselining for resumption of Pu production operations were assessed for applicability to the new mission. Fire scenarios analyzed originally considered to be applicable to the new mission were fire inside inert gloveboxes, fires in process rooms, and fires on docks. In addition to these fire scenarios, several additional fire scenarios were developed during the rebaselining of risk for resumption of Pu production operations. This included a fire in one and multiple gloveboxes either caused by loss of inerting or internal initiation of potentially pyrophoric plutonium.

The fire scenarios affected by the new mission were assessed for changes in the event tree logic, probabilities of occurrence, and mitigating system failure probabilities. This was performed for the risk-dominant fire scenarios determined in the rebaselining assessment.

Source terms for the fire accident scenarios were determined by updating those determined in the rebaselining assessment as necessary to accurately reflect the

circumstances associated with the new mission. Release fractions associated with the various materials were reviewed for applicability. Radiological consequences associated with the releases from various fire scenarios were calculated using the MACCS code.

Additionally, risk estimates and risk curves were presented. The most significant fire scenario in terms of risk to the public is due to an assumption that potentially pyrophoric plutonium would spontaneously ignite upon loss of power which results in loss of inerting, even though this has never occurred in the past. The mean risk estimates were demonstrated to be orders of magnitude below the quantitative safety goals promulgated by DOE (DOE, 1991b).

Radiological consequences and risk to co-located workers were assessed by modifying an atmospheric dispersion factor. Consequences were calculated for individuals gather outside of the facility and for individuals inside adjacent facilities for having an active ventilation system, or taking credit for emergency actions to reduce outside air intake. These assessments were used for on-site emergency planning purposes.

## SUMMARY

Fire risks involving plutonium processed or stored at the RFP have been quantitatively analyzed for safety analysis reports. Operational Safety Requirements have been established on those mitigating systems (e.g., fire alarms, fire suppression systems, emergency response groups) that were credited in the risk assessment. These OSRs establish the minimum operating requirements and also mandate periodic surveillances.

## REFERENCES

- Chanin, D. I., L. L. Sprung, L. T. Ritchie, H-N Jow, and J. A. Rollstin, 1990, "MELCOR Accident Consequence Code System (MACCS). Volume 1: User's Guide; Volume 2: Model Description; Volume 3: Programmer's Reference Manual," NUREG/CR-4691, Sandia National Laboratories, published by the U.S. Nuclear Regulatory Commission, Washington, D.C.
- DOE, 1987, Safety analysis and review, *DOE Order 5481.1B*, U.S. Department of Energy, Washington, D.C.
- DOE, 1991a, Unreviewed safety questions, *DOE Order 5480.21*, U.S. Department of Energy, Washington, D.C.
- DOE, 1991b, Nuclear safety policy, *Secretary of Energy Notice SEN-35-91*, U.S. Department of Energy, Washington, D.C.
- DOE, 1992, Nuclear safety analysis reports, *DOE Order 5480.23*, U.S. Department of Energy, Washington, D.C.
- EG&G, 1992, "Rocky Flats Risk Assessment Guide," EG&G Rocky Flats, Inc., Golden, Colorado.
- EPRI, 1989, "Guidelines for 10 CFR 50.59 Safety Evaluations," NSAC-125, Nuclear Management and Resource Council and Electric Power Research Institute, Palo Alto, California.
- NRC, 1975, "Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400, NUREG-75/014, U.S. Nuclear Regulatory Commission, Washington, D.C.
- NRC, 1990, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, U.S. Nuclear Regulatory Commission, Washington, D.C.

**076 Risk-Based Regulation (I)**

*Chair: V. Joksimovich, Accident Prevention Group*

Application and Extension of Formal Decision-Making Methods to Generic Safety Issue  
Decisions

*M.P. Bohn (SNL)*

Risk-Based Regulation Using REVEAL

*H. Dezfuli, J. Meyer (SCIENTECH); M. Modarres (U. Maryland), H. Specter (RBR  
Conslts.)*



# APPLICATION AND EXTENSION OF FORMAL DECISION-MAKING METHODS TO GENERIC SAFETY ISSUE DECISIONS

Michael P. Bohn

Sandia National Laboratories  
Albuquerque, New Mexico 87185

## INTRODUCTION

The U.S. Nuclear Regulatory Commission is moving towards a more agency-wide use of probabilistic risk assessment (PRA) in its decision-making role. One broad set of responsibilities of the US NRC is the resolution of "Generic Safety Issues". A number of these generic safety issues have been identified, and it is the NRC's task to evaluate the potential risk impact of each of these issues, to identify potential plant modifications or changes in procedures to mitigate these safety issues, and then evaluate whether any particular safety issue should be implemented on an industry-wide basis to reduce the overall risk to the public. In the evaluation and prioritization of these generic issues, the US NRC has been investigating use of decision making methodologies and the direct use of probabilistic risk assessment in evaluating the potential impacts of the safety issues involved. This paper reports on work performed for the Generic Issues Branch of the US NRC's Office of Nuclear Regulatory Research. The goal of this work was to identify the applicability of formal decision making methods to the US NRC's decisions involving generic issues and to explicitly consider how various sources of uncertainty could be factored into the decision-making process. The results of this work, including a number of example applications to Generic Issue 57, "Effects of Fire Protection System Actuation on Safety Related Equipment," are contained in Reference 1.

Currently, in evaluating a generic issue, the US NRC uses a cost-benefit ratio as a criteria to justify the need for plant modifications. In this process, the risk to the public due to scenarios involving the safety issue is evaluated using probabilistic risk assessment techniques and a resulting risk increment to the public (expressed in terms of Person-REM) is computed. Then, a number of plant modifications or other changes are hypothesized which could prevent the occurrence of the scenarios involved in the generic issue and the cost of these modifications is evaluated. Finally, based on the value of the cost-benefit ratio, defined as

$$\text{CBR} = \frac{\text{Cost of Plant Modification}}{\text{Averted Risk to Public (Person-REM)}}$$

the decision is made as to whether the proposed modification is viable. Currently, the US NRC views a modification as viable if the cost-benefit ratio is less than \$1000/Person-REM (It should be noted that other deterministic aspects of the modification and generic issue may enter into the decision to take into account the need for defense in depth, etc.)

## UNCERTAINTY CONSIDERATIONS AND THE COST-BENEFIT RATIO

Inasmuch as this work was directed towards consideration of the impact of uncertainty on the US NRC's Generic Issue decisions, the role of uncertainty in the cost-benefit approach to decision making was first examined. As originally formulated, the criteria of \$1000/per Person-REM was selected without direct consideration of typical uncertainties in the cost or the risk. It was envisioned as being a point estimate in which

a mean value of the cost of a modification would be divided by the mean value of the risk averted increment.

However, in realistic accident scenarios involving the generic issues, the uncertainty in risk (the denominator) is typically orders of magnitude and quite skewed. By contrast, the uncertainty in the cost (the numerator) is much smaller and is, say, approximately, plus or minus 25%. Hence, if the distributional forms of the numerator and denominator are known, the true mean value of the cost benefit ratio can be evaluated and it is found to be on the order of 10 to 50 times larger than the point estimate value (ie, the mean cost divided by the mean risk averted). Thus, the viability of any particular retrofit could be very much determined by the manner in which the cost-benefit ratio is computed. The observation then is, when formulating numerical criteria for a decision-making process, it is essential to consider the nature and sources of the uncertainty when defining such decision-making criteria.

## FORMAL DECISION METHODOLOGIES

There are a number of different formal approaches to decision-making. The methodology discussed here is based on the use of decision trees and the classic use of utility functions. The steps involved in making a decision are as follows:

- 1) Identification of actions (eg, backfits or retrofits)
- 2) Identification of one or more consequence attributes which characterize the results of each action.
- 3) Input of the decision maker's preferences as to the relative desirability of the consequence attributes. These are expressed mathematically in terms of objective functions or utility functions.
- 4) Calculation of the consequences including uncertainty.
- 5) Ranking of the actions using the mean value of the scalar objective function.

The general model is a branching tree of actions and consequences as shown Figure 1. In this figure is depicted a decision to be made between two actions (a' and a'') and the consequence of each action is uncertain. For example, as shown on this tree, with probability  $p_1'$  there results the vector of consequences  $C_1'$ . Similarly with probability  $p_2'$ , there results the vector of consequences  $C_2'$ , etc. Thus, for each action, there results a spectrum of consequences each of which has a known probability of occurrence. Each vector of consequences is then mapped to a single scalar value by use of a utility or objective function. Thus, the vector of consequence attributes  $C_1'$  is mapped to the scalar value  $U_1'$  by use of an appropriate objective function, and so forth. Then, according to the classical utility theory as developed in Reference 2, the choice between actions a' and a'' is made by comparing the expected values of the scalar utilities of each of the two actions and choosing that action which has the maximum expected value of scalar utility. That is, we choose action a' over action a'' if

$$\sum p_i' U_i' > \sum p_i'' U_i''$$

The general model selected is thus an example a multi-variate decision analysis as discussed, for example, in References 2 and 3.

The choice of the consequence attributes associated with each action is critical in an effective decision making process. Several potentially useful multi-attribute

consequence vectors are discussed in Reference 1 involving quantities which are of direct concern in the US NRC's regulatory process. For the sake of the example to be presented below, an attribute vector which separates out the sources of the total computed radiation dose is considered, as shown below:

$$C = \left\{ \begin{array}{l} \text{Radiation dose due to Internal events} \\ \text{Radiation dose due to Fire} \\ \text{Radiation dose due to Earthquakes} < \text{SSE} \\ \text{Radiation dose due to Earthquakes } 2 < \text{SSE} < 6 \\ \text{Radiation dose due to Earthquakes} > 6 \text{ SSE} \end{array} \right\}$$

The first element in this vector is the increment of risk averted due to internal event scenarios which could be mitigated by a given retrofit. Similarly, the second element is that risk which could be averted arising from fire scenarios. The last three elements are the radiation dose (averted) due to earthquakes having different peak ground acceleration levels relative to the Safe Shutdown Earthquake level (SSE) for which the plant is deterministically designed.

It should be noted that each element of the consequence attribute vector above is a natural product of a probabilistic risk assessment which can be performed for any power plant. This set of attributes is somewhat different than has been used in past applications of multi-variate analysis in that the sum of the attributes (the total radiation dose) is the quantity of fundamental interest to the regulator. However, in making decisions as to which retrofits should be used to avert this risk, it is our experience that the US NRC has significantly different views as to the relative importance of accident scenarios due to different sources (internal events versus fires, or fires versus earthquakes, etc). Thus by breaking the total dose down into contributions due to different types of scenarios, the regulator may express his preference as to the relative desirability of the different modifications. For example, if the total dose were dominated by that dose due to earthquakes occurring above the 6 SSE level and contributions to the total dose from all other categories were very small, it is likely that the regulator would view any modification aimed only at mitigating the effects of such earthquakes with some degree of reluctance. By contrast, however, if a given modification were to avert risk from a number of internal event scenarios, fire event scenarios, and small earthquake scenarios (but still resulting in the same total dose) then the regulator is likely to view such a modification as being very robust and desirable. Thus, this particular consequence attribute vector is appropriate for the type of decisions involved in identifying retrofits for resolving generic issues.

## MULTI-VARIATE OBJECTIVE FUNCTIONS

As described above, a multi-variate objective function is required to map each vector of consequence attributes to a single scalar utility value. Determination of the appropriate multi-variate objective function is based on a querying of the decision-makers both as to the marginal utilities of each of the attributes as well as a scaling of the various attributes relative to one another. It can be shown (see, for example, Reference 2) that the form of the multi-variate objective function is determined by the concepts of a) Preferential Independence b) Weak Difference Independence c) Utility Independence d) Additive Independence. Whether or not one or more of these independent conditions hold is determined in the querying process. Depending on which combination of independence conditions is satisfied, the form of the multi-variate utility function can be prescribed to

within a number of constants which are then determined by the decision-makers' relative preference for the individual attributes. As described in Reference 1, we shall assume that all marginal utilities are linear (risk neutral) and assume that the decision-makers prefer to avert risk due to internal events or fires in the ratio of 10:1 to seismic averted risk and further assume that the decision-makers prefer modifications affecting the risk averted from the three seismic levels in the ratio of 10:5:1. Then, assuming the appropriate additive independence conditions have been established, the additive multi-variate utility function for these preferences is given by

$$U [ \{C_i\} ] = 10 \text{ M-R(internal)} + 10 \text{ M-R (Fire)} \\ + \text{M-R(Seis 1)} + 0.5 \text{ M-R(Seis 2)} + 0.1 \text{ M-R(Seis 3)}$$

This objective function will be used in the next example.

### APPLICATION TO A GENERIC ISSUE RETROFIT ANALYSIS

In this example, we will illustrate the explicit inclusion of modeling uncertainty and its impact on the decision-making process. In the study of Generic Issue 57, thirteen different types of scenarios associated with inadvertent actuation of fire protection systems and their resulting increase in risk to typical commercial power plants were analyzed. For each scenario identified, a probabilistic risk assessment was performed. This risk assessment included the impact of the scenario on internal events, fires and the three increasing earthquake levels described in the consequence vector above (denoted below as Seis 1, Seis 2, Seis 3). A full certainty analysis was performed and an estimate of the risk to the public in terms of Person-REM was computed. The results of this analysis for a particular B & W Plant are shown on Table 1. The various accident scenarios associated with the inadvertent fire suppression actuations and their causes are described in detail in Reference 1. In addition, for each of the scenarios studied, a number of different plant modifications were identified which would prevent or seriously lower the likelihood of the accident scenarios studied. The cost of each of these modifications (on a plant specific basis) was also determined. For both the risk averted and the cost, a full uncertainty analysis was performed. The results of the analysis for the B & W plant are shown in Table 1. In this case, five different modifications were hypothesized. For example, one modification included re-routing certain critical safety system cabling so as to remove a vulnerability due to inadvertent fire suppression actuation. Another modification involved upgrading the actuators of a fire suppression system so that it would not be vulnerable to seismic events. A description of the modifications is given in Reference 1. However, when the impact of the modification was input to the risk assessment of each of the scenarios, an increment of risk averted and its uncertainty was computed. This data is shown in Table 1. Thus, for example, the first column shows that modifications 1 and 10 (which both had the same impact on the risk assessment) gave rise to a total averted risk of 4.8 Person-REM. This total was broken down into no contributions due to internal events and fire sequences, while the lowest seismic level (Seis 1) contributed 3.1 Person-REM, etc. Similarly, columns 3, 4 and 5 gave corresponding increments of averted risk due to other modifications. The cost of these modifications are also shown on this table. Finally, the lowest row indicates the cost/benefit ratio based only on the total risk averted and the cost of each modification. Recalling the criterion of a modification viability as requiring a cost benefit ratio less than \$1000/Person-REM, it can be seen that both modifications 5 and 7 would be considered viable. Further, modification 7 would be selected over modification 5 due to its more advantageous cost/benefit ratio.

However, in the course of this analysis, it was noted that a significant modeling uncertainty issue arose. In fact, at the B & W plant studied in the GI-57 program, one significant modeling uncertainty issue arose. This issue had to do with the ability of the fire growth and damage computer code COMPBRN to model damage to essential cables in a room whose configuration is much more complicated than the single compartment geometry for which COMPBRN is designed. Depending on the assumptions that are made in modeling this multi-compartment situation, significant differences in the calculated person-REM averted result.

Table 1

## B &amp; W Plant - Benefits and Costs With Uncertainty

	MOD 1 & 10	MOD 3	MOD 5 & 11	MOD 7	MOD 5*
INTERNAL	0	0.9	0	0	0
FIRE	0	0.1	0	0	0
SEIS 1	3.1	0	6.8	6.4	54.8
SEIS 2	1.7	0	53.2	52.1	315.0
SEIS 3	0	0	17.0	16.9	68.5
TOTAL	4.8 P-R	1.0 P-R	77.0 P-R	75.5 P-R	438.3P-R
COST	\$14k	\$250k	\$40k	\$15k	\$40k
CBR	2.9	250.0	0.5	0.2	

where P-R denotes Person-REM

Thus, on Table 1, an additional column denoted as Mod 5\* is shown. This column presents the benefit (in terms of person-REM averted) which would accrue given that Modification 5 has been put in place, and also given that pessimistic assumptions as to the growth and spread of the seismically induced fire were made in performing the COMPBRN fire growth calculations. Thus, in this case (Mod 5\*), the benefit is significantly greater than was originally shown for Mod 5 when a more optimistic calculation was made using the COMPBRN code.

The decision tree associated with the two actions Mod 5 and Mod 7 (which are the only two viable modifications identified for the B & W plant) is shown in Figure 2. In this figure it can be seen that there is no uncertainty associated with the consequence of Mod 7. However, there are two uncertain outcomes associated with Mod 5. Judgmentally, one must assign a relative probability to the two uncertain consequences which reflects the decision maker's (or the fire phenomenology analyst's) relative confidence in the two sets of code calculations and the resulting consequences. For the sake of this example, it was assumed that the most optimistic COMPBRN code calculation had a probability of 0.67 whereas the most pessimistic calculation was associated with a probability of 0.33 as shown in this figure. Also shown in this figure are the consequence vectors associated with the outcomes of Mod 5 and Mod 7. Using the example additive multi-attribute utility function developed earlier, each consequence vector is mapped into a scalar utility and the mean of the normalized scalar utility is then computed using the probabilities of the uncertain outcomes. As shown in this figure, the expected value of the normalized utility of Mod 5 has a numerical value of 0.137, whereas

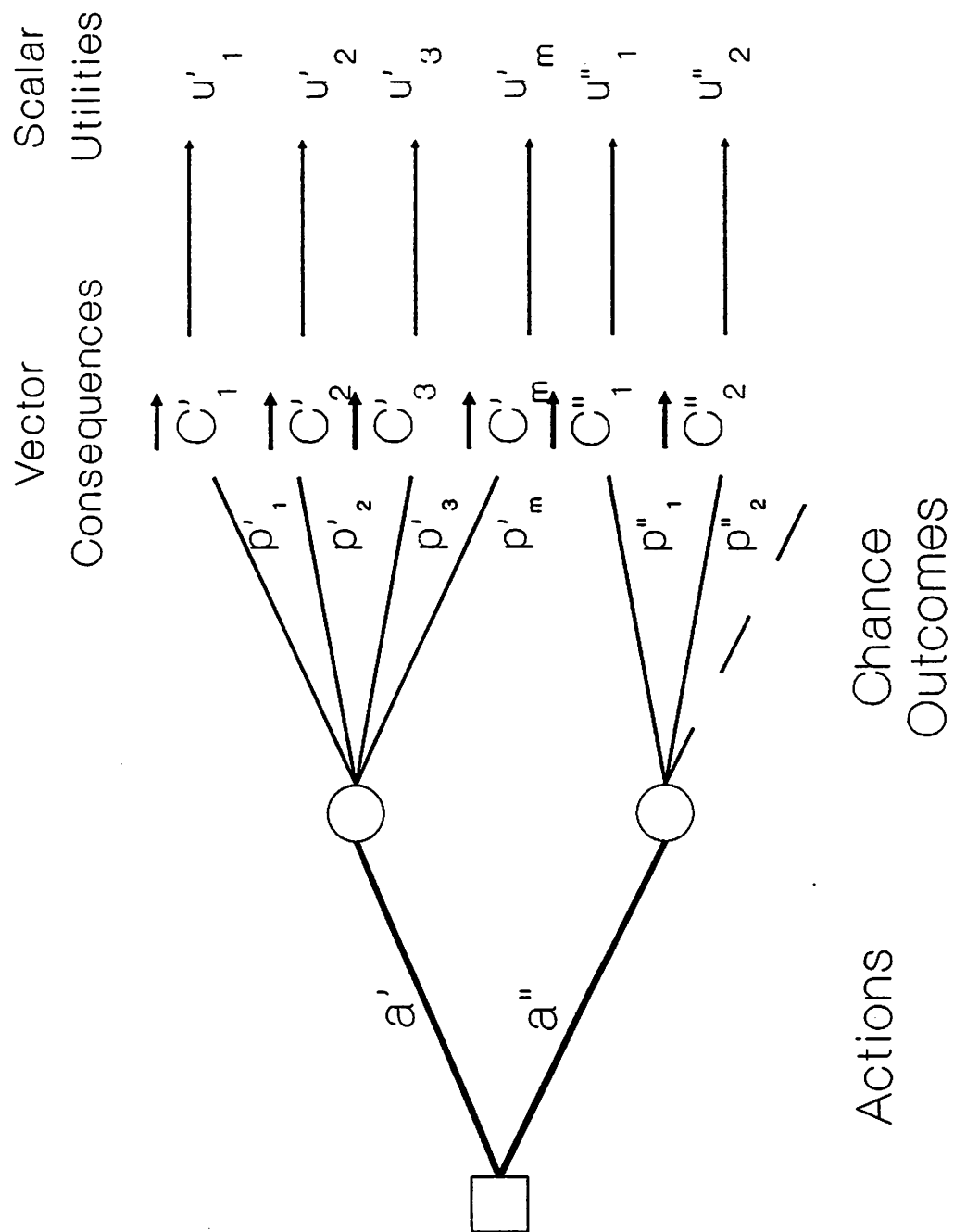
the expected value of the normalized utility of Mod 7 has a value 0.124.

As noted earlier, based on the usual cost/benefit ratio analysis, Modification 7 would be selected over Modification 5. However, when the critical nature of the geometry of the vital area is recognized and the uncertainties in the code modeling of the damage to the critical cables is explicitly included in a multi-variate utility analysis, then the preferred choice is now Modification 5. Physically, the reason for this change in the order of ranking of the modifications is the fact that, when one includes the more pessimistic COMPBRN code calculation, a greater benefit results from Modification 5 due to the fact that - with finite probability -- it is possible that the more pessimistic COMPBRN code calculation is indeed the correct analysis. Thus, Modification 5 is chosen because it protects against an unlikely (but still possible) accident.

This fairly general analysis highlights the potential usefulness of a formal decision-making methodology in the face of significant and unquantifiable uncertainty, which is often the situation faced by NRC regulators. Regulators always must work with uncertain tools and uncertain assumptions and the impact of the modeling uncertainties can often outweigh the impact of the propagation of random uncertainties in the calculation process.

#### REFERENCES

1. Bohn, M. P., Decision Making Under Uncertainty: An Investigation Into The Application Of Formal Decision-Making Methods To Safety Issue Decisions, NUREG/CR-5906, December, 1992.
2. Keeney, Ralph L., and Howard Raiffa, Decisions with Multiple Objectives: Preferences and Value Tradeoffs, John Wiley & Sons, New York, 1976.
3. Benjamin, Jack R., and C. Allin Cornell, Probability, Statistics, and Decision for Civil Engineers, McGraw-Hill, Inc., 1970.



**Figure 1** General Decision Tree with Multiple Uncertain Consequences of Each Action



## RISK-BASED REGULATION USING REVEAL™

Homayoon Dezfuli<sup>1</sup>, Mohammad Modarres,<sup>2</sup> Jim Meyer,<sup>1</sup> Herschel Specter<sup>3</sup>

<sup>1</sup> SCIENTECH, Inc., 11821 Parklawn Drive, Rockville, MD 20852

<sup>2</sup> University of Maryland, Department of Materials and Nuclear Engineering,  
College Park, MD 20742

<sup>3</sup> RBR Consultants, Inc., P.O. Box 8185, White Plains, NY 10602

### INTRODUCTION

Over the past two years, the concept of risk-based regulation has been introduced to the U.S. Nuclear Regulatory Commission (NRC) and the nuclear industry. Converting much of the current, deterministically based regulation of nuclear power plants to risk-based regulation can result in lower levels of risk while relieving unnecessary burdens on power plant operators and regulatory staff. Risk-based regulation of nuclear power plants means regulating plant configurations based on their risk significance.<sup>1</sup> Within the risk-based regulation framework, regulatory requirements for plant configurations are coupled to the risk significance of those configurations. High-risk configurations will be subjected to more stringent regulatory requirements that will either eliminate the critical configurations or reduce the amount of time the plant can be in those configurations. On the other hand, regulatory requirements for low-risk configurations could be relaxed. Implementation of risk-based regulation therefore depends on the availability of a risk-based configuration control system.

A functioning risk-based configuration control system should be able to effectively support the assessment of configurations in a meaningful manner so the information generated is understandable to the end users. The assessment of risk should not be limited to the calculation of conditional core melt frequency. It is probably more important for the plant's maintenance and operating staff to comprehend the status of the plant once the plant enters a configuration, that is, to know the safety systems or functions affected or unaffected by the configuration. This information is essential for a configuration control system.

Configuration control systems based on traditional probabilistic safety assessment (PSA) models are not very effective. Incorporating changes to the risk model to reflect changes in plant operation and configuration requires substantial effort, making it difficult to effectively use the traditional PSA in configuration management. The primary objective of traditional PSA models for nuclear power plants has been to develop and analyze the plant logic model for a base configuration—the configuration in which equipment outages due to maintenance and testing are random phenomena. In reality, this base configuration does not exist; usually several components undergo scheduled maintenance or testing simultaneously, during which time those components are unavailable. Their unavailability in turn causes the unavailability of other equipment due to functional dependencies. This situation, rather than the base configuration, represents the typical, routine configuration of a plant.

The base configuration has been the basis for many of the current studies on risk-based configuration control.<sup>2</sup> That is, the cut sets of the base configuration logic model are used to determine risk-important systems, structures, and components (SSCs). Once these SSCs are identified, all combinations of two and three failures are found for analysis. For each



combination, a conditional probability of core damage is calculated using the base configuration logic. This process has three important shortcomings:

1. SSCs have different importance rankings in different plant configurations.
2. There is no assurance that all risk-significant configurations are identified.
3. Quantification of a large number of combinations using traditional PSA methods requires a prohibitive amount of time.

We believe that PSA models in their present form are not suitable for performing configuration control because they are not flexible enough to be used effectively and efficiently. If we expect to use the risk model in routine, day-to-day evaluation tasks, such as risk-based configuration control, the model must be transparent and user-friendly. For this reason, we propose the use of risk models based on REVEAL™ (formerly known as SMART) for configuration management to support risk-based regulation.<sup>3,4</sup>

The risk models produced by REVEAL™ are highly modularized and are based on success trees and logic networks. This modularity, combined with the use of a highly graphic Windows™ environment, allows the user to easily construct logic models and to change a portion of the plant logic, based on a change in configuration, and observe the effect of the change on the entire plant logic. That is, the risk model is an intelligent logic model that can dynamically show changes in the logic of the plant as a result of changes in plant configuration. This capability makes REVEAL™ a suitable advisory tool for the regulatory body and the plant's maintenance and operating staffs, who can use it to analyze the impact of various maintenance practices or surveillance tests on the plant's risk profile. The analytical capability built into REVEAL™ is generic, so the software can support different types of risk-based evaluations.

## REPRESENTATION OF A LOGIC MODEL IN REVEAL™

Figure 1 shows the representation of a typical logic in the REVEAL™ environment. At the top of the hierarchy are groups that correspond to the highest level of modularization. A group must be tagged as "frontline" or "support" to reflect the properties of lower level logic modules in terms of whether they are related to frontline systems or support systems. (Examples of groups include the emergency core cooling group, electric power group, and actuation group.) The user can define many frontline and support groups based on preference. Within each group is a lattice and a list of "tree windows." The user can define multiple tree windows within a group. Each tree window contains multiple logic trees. No limitations exist on the number, size, or complexity of the logic trees in a tree window.

The logic trees, which are success-oriented, are composed of Boolean gates and "blocks." The Boolean gates used in REVEAL™ are "AND," "OR," "K/N," "NOR," "NAND," and "NK/N." The last three are negated gates. The types of blocks used include goal, function, system, intermediate, limiting condition for operation (LCO), accident sequence, condition, test and maintenance, initiating event (IE), composite, and basic blocks. A "basic block," which resembles a basic event in a traditional PSA, constitutes the lowest level of decomposition of the logic, for example, a pump or valve. A composite block can represent a collection of components, for example, a pipe segment. Probabilities can be assigned to basic blocks, composite blocks, and condition blocks.

The modeling of functional dependencies between blocks is deferred to a lattice structure belonging to that group. One lattice exists for each group. The lattices are used to relate the logic trees within each group to logic trees in other groups. *Collectively*, these lattices carry information about the nature of interrelationships between blocks within groups. Within each group, the user can also define common-cause families. A common-cause family is a set of basic blocks that are potentially subject to common-cause failures. Dezfuli et al.<sup>3</sup> provide a more detailed explanation of modeling in the REVEAL™ system.

## FEATURES OF REVEAL™-BASED LOGIC

REVEAL™ has unique qualitative features, including the Windows™ environment in which it runs. Most of the Windows™ features—such as the mouse-driven menu bars, various tools, and the ability to run other Windows™ applications concurrently—can be used in REVEAL™. In addition, the logic is represented graphically. The blocks are color coded

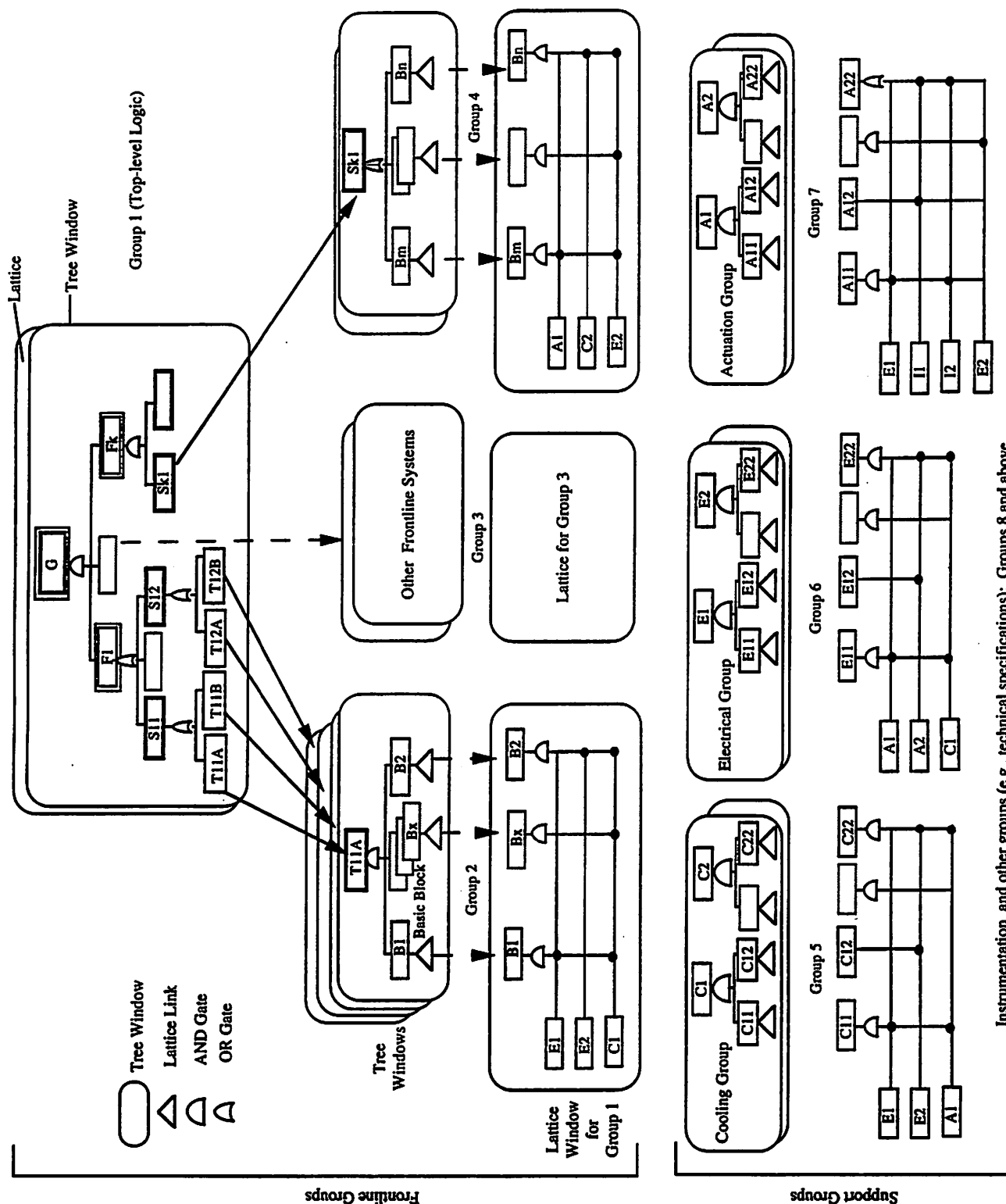


Figure 1. This example represents a typical logic layout in the REVEAL™ environment.

and detailed information about the blocks is stored in a structured manner, creating an easily accessible database. To take advantage of the dynamic data exchange (DDE) capability of the Windows™ operating system, the user can transfer the results of any analysis performed in the REVEAL™ environment to any Windows™-based application, such as an EXCEL® spreadsheet, to perform specific tasks. In effect, this feature makes REVEAL™ a generic logic analysis tool. Several qualitative features are described below.

Visibility of the Logic. One of the major shortcomings of traditional PSA models is their lack of transparency. If a risk model is to be used by a plant's operational staff, most of whom probably are not PSA practitioners, it must be easy to understand. With REVEAL™, the interrelationships between logic trees are presented via lattices, which communicate dependencies very effectively.

Success-oriented Logic. Traditional PSAs are performed in the fault domain. In the REVEAL™ system, the logic structures are defined in the success domain. The intent is for REVEAL™ to be used by the plant staff as a tool for monitoring the availability of safety functions based on operator input that specifies which components are out for maintenance or are found in a failed state.

Speed in Implementing Changes in Logic. With the REVEAL™ software, implementing changes in the logic is an effortless task. This is due to the modularity of the logic and the user-friendly Windows™ graphic environment. The entire logic structure, although constructed and shown in modules in many windows, is a very large intelligent network that can instantaneously propagate any change in any part of the network throughout the entire network. In effect, the logic can be updated instantaneously to reflect the immediate status of the plant. This updating can be done by personnel who are not PSA practitioners.

Local Loss Propagation. A powerful feature of REVEAL™ is its capability to propagate the effect of a local loss on the entire logic. A local loss can be a hardware failure or an outage due to scheduled maintenance. Using the mouse, the user can disable a block. The block becomes solid red, indicating unavailability of the block. Any block within the entire logic model that has a functional relationship with the disabled block will appear in hatched red color to signify a causal loss. The ease of evaluating the effect of a local loss on baseline safety functions results in effective assessment of the safety implications of plant changes, which routinely affect the plant's risk profile. For example, using the block overview module, the user can tag a pump as inoperable without accessing the logic tree and lattice that contain the pump. REVEAL™ dynamically shows all of the causal losses and whether the plant has entered an LCO. The user can easily move through the relevant logic trees and lattices to study the path of the failures.

Determination of LCO Configurations. Limiting conditions for operation (LCOs) represent the lowest functional capability of equipment required for safe operation of a facility. It is desirable to be able to determine, in advance of taking an action, whether that action will result in a configuration that puts the plant in an LCO. The modeling of LCOs as part of the risk model is not trivial; it requires the modeling of complex conditions of the plant normally characterized by the availability of some equipment and the unavailability of other equipment. With REVEAL™, the logic of the plant can easily be extended to include LCOs because REVEAL™ allows the use of negated Boolean gates. This capability makes REVEAL™ very effective in monitoring compliance with technical specifications. Figure 2 contains a typical screen shot from the REVEAL™ environment. The figure shows how local loss of the block "UPS-TSW-620/1" resulted in the causal loss of the block "UPS Through Inverter T-160-620-1," which in turn caused the plant to enter a 7-day LCO.

## RISK-BASED AND PERFORMANCE-BASED EVALUATIONS

REVEAL™ propagates almost instantaneously the impact of losses associated with a specific configuration on the entire plant logic. It makes sense to take advantage of this unique property to conduct risk-based evaluations. Unlike traditional PSAs, REVEAL™ does not convert the plant logic into Boolean equations to generate cut sets. Rather, REVEAL™ relies on a powerful combinatorial algorithm to exhaustively generate all probabilistically significant failure combinations and subsequently search the entire logic to identify the impact of each failure combination. The failure combinations generated by REVEAL™ are all mutually exclusive. The quantification based on these combinations is

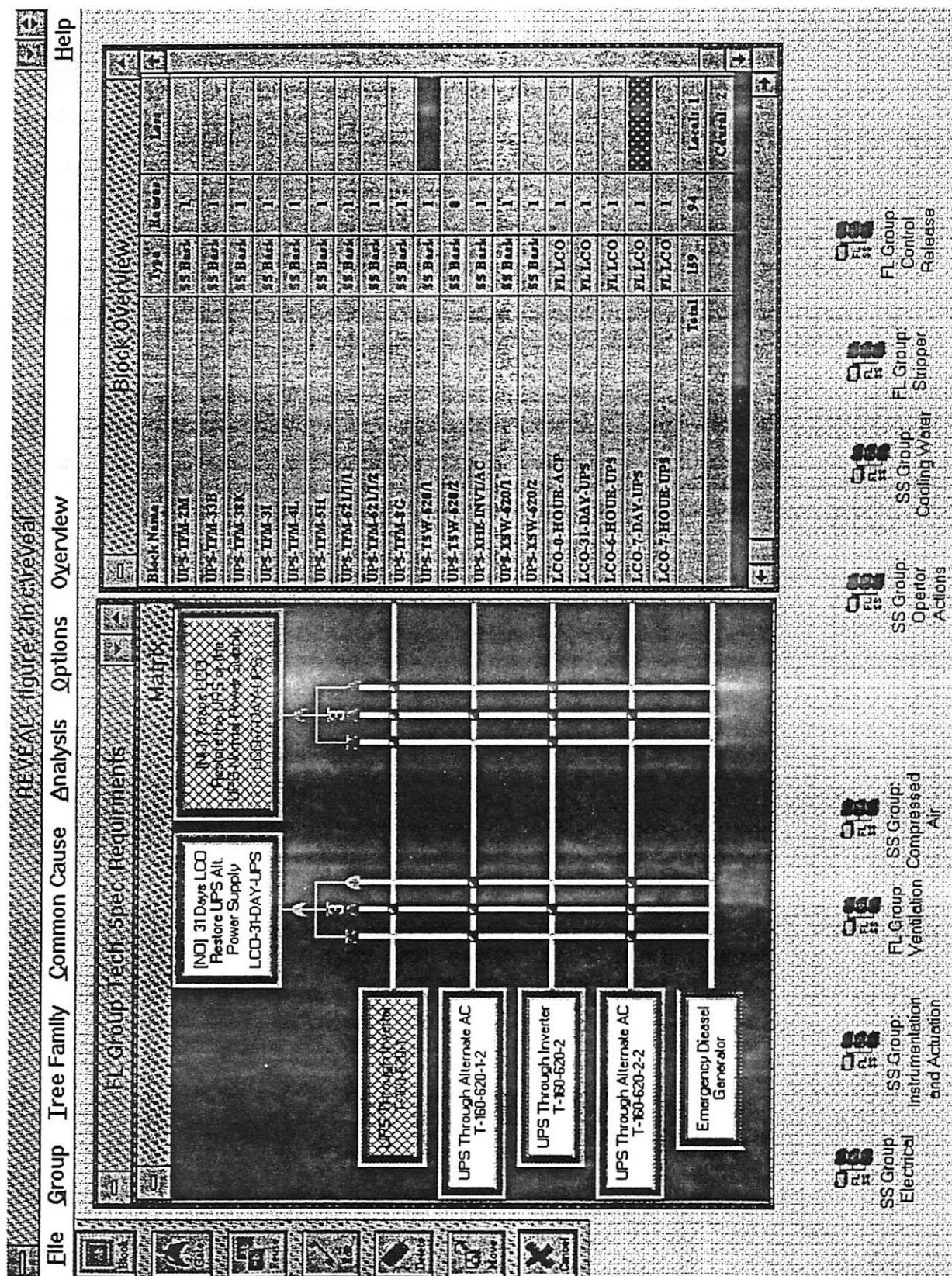


Figure 2. REVEAL shows local losses and causal losses in both graphical and tabular formats.

more accurate than traditional calculations based on cut sets. Generally, risk-based evaluations fall into one of two categories:

1. Efforts to design regulatory requirements
2. Efforts to demonstrate compliance with regulatory requirements.

The efforts to design regulatory requirements typically involve risk-based ranking of equipment. This ranking is often based on the risk contribution of the equipment, event, or some other factor to a plane of reference. For example, maintenance downtimes can be ranked relative to the frequency of core damage, or equipment unavailabilities in a system can be ranked with respect to the system's unavailability. We designed the REVEAL™ analytical capabilities to support various risk-based evaluation tasks at different levels of abstraction. A ranking technique for optimizing Allowed Outage Times (AOTs) and Surveillance Test Intervals (STIs) is discussed in Dezfuli et al.<sup>4</sup>

REVEAL™ is designed so that non-PSA practitioners can easily conduct evaluations to ensure compliance with regulatory requirements. Examples of such applications include:

- Ensuring that goals (e.g., availability goals) set as part of the maintenance rule are achieved or are not violated;
- Ensuring that configurations requiring or leading to an immediate plant shutdown are avoided as a plant moves from one configuration to another;
- Analyzing events that have actually occurred to determine their risk significance and developing strategies to avoid their recurrence.

## REFERENCES

1. H. Specter, "PSA, calculus, and nuclear regulation," paper presented at the Probabilistic Safety Assessment International Topical Meeting in Clearwater Beach, Florida, January 26-29, 1993.
2. P.K. Samanta, W.E. Vesely, and I.S. Kim, "Study of operational risk-based configuration control," NUREG/CR-5641, August 1991.
3. H. Dezfuli, M. Modarres, W. Martchenko, J. Meyer, and A. Amir-Ghassemi, "Probabilistic safety assessment using SMART™ [REVEAL™]," paper presented at the Probabilistic Safety Assessment International Topical Meeting in Clearwater Beach, Florida, January 26-29, 1993.
4. H. Dezfuli, M. Modarres, and J. Meyer, "Application of REVEAL™ to risk-based configuration control," paper accepted for 1994 publication in the special issue of *Reliability Engineering and System Safety* on the use of advanced techniques in safety and reliability.

**078 Process Safety Management**

*Chair: R.L. Cummings, Interstate Assessment Technologies*

**Integrating Compliance Efforts for Process Safety Management Regulations**  
*D.A. Moore (Primatech)*

**OSHA PSM: Impact on Accident/Incident Investigation**  
*D.A. Wetzel, S. Hall (Wetzel, Herron & Drucker); R.E. Rimkus, J.C. Clark (Rimkus Consulting)*

## **INTEGRATING COMPLIANCE EFFORTS FOR PROCESS SAFETY MANAGEMENT REGULATIONS**

David A. Moore, PE, CSP

President & CEO  
Primatech Inc.  
100 Pine Street, Suite 2240  
San Francisco, CA 94111

### **INTRODUCTION**

The introduction of the OSHA 29 CFR §1910.119 regulations for Process Safety Management (PSM) in February of 1992 provided industry with a Federal regulatory model for PSM. This rule has some objectives that overlap with those of the proposed Federal EPA rule 40 CFR Part 68, "Risk Management Programs for Chemical Accidental Release Prevention." The similarities among the issues addressed by these regulations are causing industry concern that some duplication of effort may be required in order to achieve compliance. This paper briefly outlines the requirements of the regulations, and discusses an approach for minimizing the potential for overlapping efforts and unnecessary expense. Industrial companies should take a systematic, holistic approach towards addressing these and other similar regulations, in order to reduce compliance costs. Furthermore, industry would be prudent to anticipate the future directions that the regulations may take. However, even though some economies are possible, compliance with the proposed EPA RMP rule will inevitably require significant work beyond the 29 CFR §1910.119 compliance efforts.

### **BACKGROUND OF THE PSM REGULATIONS**

Recent significant accidents involving chemical process facilities have prompted industry to address more formally the concerns of controlling major hazards involving highly hazardous chemicals. Industries handling hazardous chemicals are working to upgrade current safety practices by adopting a comprehensive Process Safety Management (PSM) program.

The Clean Air Act (CAA) amendment of 1990 Section 304 requires OSHA to promulgate, under the Occupational Safety and Health Act (29 U.S.C. 655), a standard in order to protect employees from hazards associated with accidental releases of highly hazardous chemicals in the workplace.<sup>1</sup> OSHA promulgated its standard for PSM on February 24, 1992 (57 FR 6356).

In addition, Section 112(r)(7) requires EPA to promulgate "reasonable regulations and appropriate guidance to provide for the prevention and detection of accidental releases and for responses to such releases" by November 15, 1993. A draft copy of the proposed rules was available at the time this paper was written, although it had not been published in the Federal Register.<sup>2</sup>

EPA estimates that approximately 140,000 facilities would be affected by the proposed rule. Approximately 87,800 of those facilities would also be covered by OSHA's PSM standard.

## ELEMENTS OF PSM REGULATIONS

A PSM program encompasses various elements, or program components, each of which must be implemented and integrated with the others to minimize process risk. While all of the guidance documents and regulations are different, the fourteen elements from the OSHA regulations shown in Table 1 are typical of those recommended.

Table 1  
OSHA 29 CFR §1910.119 PSM Elements

1	Employee participation
2	Process safety information
3	Process hazard analysis
4	Operating procedures
5	Training
6	Contractors
7	Pre-startup safety review
8	Mechanical integrity
9	Hot work permit
10	Management of change
11	Incident investigation
12	Emergency planning and response
13	Compliance audits
14	Trade secrets

<sup>1</sup>29 CFR §1910.119, Process Safety Management of Highly Hazardous Chemicals, Federal Register, February 24, 1992, U. S. Occupational Safety and Health Administration.

<sup>2</sup>40 CFR Part 68, Risk Management Programs for Chemical Accidental Release Prevention, Proposed Rule, September 1993 draft, U. S. Environmental Protection Agency.



Although this list has many similarities to the OSHA 119.119 list of highly hazardous substances, it is also fundamentally different. Since the emphasis of the RMP regulation is prevention of accidents involving highly hazardous chemicals which might effect the public or the environment, the substances and the thresholds were selected based on environmental exposure outside of the facilities, rather than worker exposure within the facility.

### **SIMILARITIES AND DIFFERENCES OF OBJECTIVES BETWEEN THE OSHA AND EPA PROGRAMS**

The EPA rule adopts and builds on OSHA's PSM standard and covers nine procedural areas for the proposed prevention program requirements. The CAA mandates that the risk management plan document three elements: a hazard assessment, a prevention program, and an emergency response program.

The primary differences in the EPA and OSHA regulations are described in Table 2. Contractors, trade secrets, employee participation, and hot work permits are not included in the EPA rule. By expanding the current program for PSM to include the additional requirements planned for EPA compliance for each element, companies can achieve economies by avoiding redundant work or rework. Some suggestions are presented in Table 2.

In February 1993, EPA proposed a list of regulated substances and thresholds. Although this list has many similarities to the OSHA 119.119 list of highly hazardous substances, it is also fundamentally different. Since the emphasis of the RMP regulation is prevention of accidents involving highly hazardous chemicals which might affect the public or the environment, the substances and the thresholds were selected based on environmental exposure outside of the facilities, rather than worker exposure within the facility.

**Table 2**  
**Comparison of the EPA and OSHA Regulations**

<b>OSHA PSM Element</b>	<b>Changes from OSHA PSM Standard</b>	<b>Recommended Action</b>
<b>Process Hazards Analysis</b>	(1) The priority for conducting the analysis would consider offsite consequences rather than the number of potentially affected employees.	The priority for conducting the PHA's for OSHA PSM should also include offsite consequences to pre-invest analysis time.
	(2) EPA has a three year implementation rather than five year schedule.	Due to the 3- versus 5-year schedule, consider giving high priority to the processes with offsite consequences, and start to conduct PHA's of units containing substances regulated under EPA RMP.

**Table 2 (continued)**  
**Comparison of the EPA and OSHA Regulations**

OSHA PSM Element	Changes from OSHA PSM Standard	Recommended Action
Process Hazards Analysis (continued)	(3) Previous incidents are limited to those with offsite consequences rather than only to employees.	Identify previous incidents involving both onsite and offsite potential.
	(4) Qualitative evaluation of safety and health impacts concentrates on public health and the environment rather than worker safety.	Determine the possible public and environmental safety and health effects of regulated substances at the facility, and consider these consequences in all PHA's.
	(5) Requires the evaluation of monitors, detectors, containment or control devices, and mitigation systems.	Based on the importance EPA is expected to place on detection devices and mitigation systems, evaluate their need and plan to install as required prior to the release of the RMP.
Process Safety Information	Requires that the evaluation of the consequences of process deviations include those affecting public health and the environment rather than workers.	Expand the scope of the evaluation of the consequences of process deviations to include public health and the environment.
Operating Procedures	Minor editorial changes only.	Ensure that operating procedures address prevention of specific offsite scenarios.
Training	Requires that facilities evaluate the effectiveness of their training programs and revise the programs, if necessary, based on the evaluation.	Ensure that training includes consideration of prevention or emergency response to offsite scenarios.
Mechanical Integrity	(1) Referred to as "maintenance" requirements in the EPA proposed rule rather than "mechanical integrity" and requires the facility to develop a list of equipment that requires maintenance.	Evaluate the difference, if any, in the PSM program requirements if maintenance is required on a regular basis.
	(2) Adds the word "maintenance" before inspection and testing throughout the paragraph to clarify that equipment should be maintained on a regular basis.	Establish a list of equipment, particularly those that could be associated with potential offsite impacts, that would require maintenance and define a schedule.
	(3) Clarifies that training of maintenance workers would be documented as for other training.	

**Table 2 (continued)**  
**Comparison of the EPA and OSHA Regulations**

<b>OSHA PSM Element</b>	<b>Changes from OSHA PSM Standard</b>	<b>Recommended Action</b>
<b>Pre-Start-up Safety Review</b>	(1) Requires that maintenance as well as operating employees are trained prior to startup .	Evaluate the difference, if any, in the PSM program requirements if maintenance employee training is required prior to startup.
	(2) Requires that all employees are trained on any new emergency response procedures.	
<b>Management of Change</b>	EPA adds a paragraph defining alterations that do not constitute a change. Specifically, "replacement is not a change if the design, materials of construction, and parameters for flow, pressure, and temperature satisfy the design specifications of the device replaced."	Evaluate the impact of the proposed change, and adopt the more stringent of the requirements.
<b>Auditing</b>	Minor editorial changes only.	Ensure that the EPA RMP regulatory requirements are included in the audits.
<b>Incident investigation</b>	(1) EPA requires that the accident investigation procedures are written.	Prepare written incident investigation procedures, if not provided.
	(2) Incidents that require investigation are those that caused or could have caused offsite consequences rather than catastrophic releases in the workplace.	Establish procedures for investigation of all offsite potential incidents.
	(3) Investigation has to include the identification of root causes.	Add root cause analysis to the investigation procedure.
<b>Emergency Planning and Response</b>	(1) Requires that facilities develop more extensive emergency response plans that detail how to respond to a release to limit offsite consequences.	Expand the scope of the emergency response plan to include offsite considerations.
	(2) Requires coordination with LEPC's.	Begin an active dialogue with LEPC's to establish a strong relationship.
	(3) Requires periodic drills.	Begin planning and conducting offsite emergency response exercises.
<b>Contractors</b>	Not included in EPA rule.	
<b>Trade secrets</b>	Not included in EPA rule.	

## CONCLUSION

While some details are not available at this time since the EPA rule has not yet been formally proposed, much can be done to prepare for the future. The activities necessary for compliance with the regulations need to be identified by facility operators and an approach defined which minimizes duplicate tasks and identifies needs based on unique tasks.

Not all requirements of the existing 29 CFR §1910.119 and the future EPA RMP rule are compatible. These will require special efforts as outlined in the paper, and should be planned and resourced accordingly. However, some elements are nearly identical and can serve all regulations. It is better to plan now and pre-invest some effort in those elements which are nearly common to avoid rework. Certain economies of scale may be possible by including the requirements of the EPA rule which focus on offsite impacts while conducting the PHA's required for the OSHA PSM standard.

Some pre-investment in effort is justified since, holistically, offsite impacts are but one of the consequences which may be possible at the facility and these hazards need to be responsibly managed by the facilities. Future requirements for process safety are likely to become more comprehensive and more challenging, including offsite transportation risk assessment and health impacts of toxic releases, or more quantitative. It is prudent for all facilities subject to such rules to develop a proactive approach to process safety, rather than one oriented to minimum regulatory compliance and reactive to every development in the regulations. The evolution of U.S. environmental regulations in the period 1970 to present, and in European process safety regulations over the last decade is indicative of the potential future direction in U.S. process safety regulations and public expectations.

## OSHA PSM: IMPACT ON ACCIDENT/INCIDENT INVESTIGATION

Don A. Wetzel<sup>1</sup>, Stephanie Hall<sup>2</sup>

<sup>1</sup>Managing Partner

<sup>2</sup>Associate

Wetzel, Herron & Drucker, L.L.P.  
Houston, Texas

R.E. Rimkus<sup>1</sup>, Jon C. Clark<sup>2</sup>

<sup>1</sup>President

<sup>2</sup>Senior Consultant

Rimkus Consulting Group, Inc.  
Houston, Texas

### I. INTRODUCTION

Refinery and chemical plant accidents are frequently catastrophic in nature and high profile in publicity. New OSHA Process Safety Management (PSM) rules require substantial documentation of contractor and employee safety programs, process hazard prioritization and analyses, pre-startup safety reviews, and emergency plans just to name a few. For the purposes of this paper, the incident/accident investigation requirement and its legal implications regarding privileges will be examined. The new OSHA PSM rules require that each employer investigate each incident/accident which resulted in, or could reasonably have resulted in a catastrophic release of highly hazardous chemical in the work place. Incident/accident investigations are required to begin within 48 hours of occurrence, and the investigation reports must deal with factors contributing to the incident/accident in order to prohibit their reoccurrence.<sup>1</sup>

Generally, the types of investigations anticipated under the new OSHA PSM rules can be privileged or protected from civil litigation discovery either by the attorney-client privilege, trade secret privilege, attorney work product privilege, or other rules of discovery that preclude the production of documents. It is important for all employers who are affected by this new OSHA regulation to understand the manner in which the investigation must take place in order to keep opinions and formulations privileged. The way in which this information can remain confidential and privileged may vary depending upon which state or federal law would be involved in future litigation.

### II. OSHA PSM - INDUSTRY APPLICATION

The Clean Air Act Amendments of 1990 required OSHA to implement a comprehensive process safety management standard to substantially reduce the number and consequences of incidents/accidents involving highly hazardous chemicals. OSHA PSM became law on May 26,

1992. OSHA PSM impacts approximately 25,000 locations in 127 industry subgroups including, but not limited to, refineries, petrochemical plants, paint manufacturing, electrical services, water and wastewater plants, plastic monomer and polymer plants, perfume and toiletry plants, soap and detergent plants, semiconductor manufacturing, meat packers and paper mills. Over three million workers, including 500,000 contractor employees are affected.<sup>2</sup>

OSHA PSM applies to any facility which contains an above threshold quantity of one or more of 136 highly hazardous chemicals; threshold quantities may vary from as low as 100 pounds to as high as 15,000 pounds. Any facility with 10,000 pounds of gaseous or liquid flammable hydrocarbon is covered. OSHA PSM defines a process as "any activity involving a highly hazardous chemical including using, storing, manufacturing, handling or moving such chemicals at the site, or any combination of these activities."<sup>3</sup>

### III. OSHA PSM - ATTORNEY-CLIENT PRIVILEGE

Accident/incident investigations are normally conducted under attorney-client privilege. The attorney-client privilege generally protects attorney-client communications from disclosure if the communications are confidential. A "confidential" communication is one that is "not intended to be disclosed to third persons other than those to whom disclosure is made in furtherance of rendering legal services".<sup>4</sup>

An attorney representing a company that is required to adhere to the OSHA PSM regulations needs to anticipate the jurisdiction in which future litigation could possibly be initiated in the event a civil lawsuit is filed after an "accident." For instance, OSHA is a federal regulation and should, upon first glance, be governed by the federal rules and laws. The federal rule of evidence that applies to attorney-client privilege, however, also provides for the determination of privilege questions in accordance with state law.<sup>5</sup> This means that the federal court may apply state privilege laws in cases where the claimant has raised an additional cause of action that is not a federal claim. Because future claimants could bring state common law tort actions as well as federal claims against an alleged OSHA PSM violator, in-house or outside counsel should be well versed in federal and applicable state privilege law in developing policies and plans regarding the implementation of OSHA PSM regulations.<sup>6</sup>

In a corporate setting the attorney-client relationship can be dubious. During an investigation it is possible that legal counsel may be asking questions of an employee who is the culpable party and may have been performing tasks that were outside of his employment duties. In this regard, there is no attorney-client privilege, and the in-house counsel may even have the duty of informing the employee that he may need to retain his own counsel.

The legal system has determined that not all employees enter into an attorney-client relationship. Some federal courts have recently held that only top management was protected by the attorney-client privilege; this approach was labeled the "control group" approach.<sup>7</sup> Other jurisdictions have held that only communications that an employee knew in the course of his employment, that were communicated confidentially to in-house counsel, were privileged; this approach was labeled the "subject matter" approach.<sup>8</sup> The United States Supreme Court in 1989 finally rejected these theories and outlined the criteria necessary to invoke the attorney-client privilege in federal court.<sup>9</sup> Many state courts may still recognize the "control group" or "subject matter" theories of determining whether a privilege attaches, and the counsel representing the company should keep this in mind before implementing any policies or procedures regarding the incident/accident investigation process.

In *Upjohn*, the IRS demanded the production of Upjohn's investigative documents including the questionnaires sent to employees from Upjohn's in-house counsel as well as interview notes and memoranda of the meetings that the in-house counsel had drafted regarding the various Upjohn employees. The court stated that the purpose of the attorney-client privilege "... is to encourage full and frank communication between attorneys and their clients and thereby

promote broader public interest in the observance of law and administration of justice."<sup>10</sup> The court also recognized that regulatory legislation, in particular, forces corporations and their employees to turn to attorneys on a regular basis in order to determine "how to obey the law."<sup>11</sup> The court found that the privilege extends to all employees of the company no matter what the rank; however, the privilege protects the disclosure of the communications and not the underlying facts.<sup>12</sup> For instance, the *Upjohn* court stated:

The client cannot be compelled to answer the question, "What did you say or write to the attorney?" but may not refuse to disclose any relevant fact within his knowledge merely because he incorporated a statement of such fact into his communication to his attorney.<sup>13</sup>

The court found that the questionnaires and memoranda and notes concerning communications were privileged because *Upjohn* issued a policy statement regarding the legal implications of the investigation and because *Upjohn's* in-house counsel took an active role in soliciting the information from the employees in order to render proper legal advice.<sup>14</sup>

Taking the applications of *Upjohn* into the arena of incident/accident investigation required by OSHA PSM, it is important that the incident/accident investigation be conducted either through in-house counsel or through outside counsel, and that the legal counsel closely monitor the investigation and document the monitoring of the investigation. Second, a policy statement explaining the purpose of the investigation should be drafted and implemented. The following are pertinent criteria that should be considered:

1. The company should assign counsel, either outside or in-house, to direct and coordinate all investigative activities in connection with the incident/accident investigation.
2. The company should distribute a policy statement to all employees, agents, and/or representatives participating in the investigations. The policy statement should include at least the following:
  - a. The investigation is being conducted and/or coordinated by the company's counsel and said counsel should be named.
  - b. The parameters of the investigation should be indicated.
  - c. The purpose of the investigation is to provide the company's in-house and outside counsel with information concerning the incident/accident investigation so that they will be in a position to render legal advice to the corporation in the ongoing litigation and/or to prepare the required OSHA PSM incident/accident investigation report.
  - d. Information discovered during the investigation is intended to be confidential and shall be disclosed only to those persons necessary to conduct the investigation.
  - e. Any and all documents generated during the investigation should bear the following legend:

"Privileged and Confidential - Prepared at the Request of Counsel in Connection with the Prosecution, Investigation, and Defense of the pending litigation or for the purposes of the required OSHA PSM incident/accident investigation and report."

- f. The results of all investigations should be communicated to the company in-house attorney responsible for directing or coordinating the same.
3. The company should establish a limited hierarchy through which all communications should pass to insure that the information is only available to persons necessary for the communications so that it is not inadvertently disclosed in order to prevent a waiver of any privilege.

Third, all investigative documents (notes, reports, and correspondence) should be directed to in-house or outside counsel. Finally, all communications arising out of the investigation should only be distributed to a limited number of persons.

Precautions should also be taken by in-house counsel or outside counsel in naming and retaining expert witnesses during litigation. Designation of a person as an expert, including agents of a party, may waive some discovery privileges. Counsel should thoroughly research the applicable law as it relates to experts in order to avoid waiving any privileges.

#### IV. OSHA PSM - WORK PRODUCT PRIVILEGE

The attorney-client privilege and the work product privilege are often confused. The attorney-client privilege protects communications between the client and attorney that are confidential. Generally, the work product privilege covers all work relating to the preparations of the lawsuit. The Federal Rules of Civil Procedure provide that documents and tangible things are discoverable in litigation, if prepared in anticipation of litigation, *only upon a showing that* the party seeking discovery has substantial need and that the party is unable to obtain the equivalent without undue hardship.<sup>15</sup> In other words, investigatory reports made in anticipation of litigation are discoverable if the claimant can prove undue hardship and substantial need. The question then becomes whether the work product doctrine is applicable to materials prepared in anticipation of previous litigation. Some courts have taken the position that the materials prepared in anticipation of terminated litigation are discoverable.<sup>16</sup> Other courts require a close relationship between the cases, either by subject matter or party similarity.<sup>17</sup> Again, in-house or outside counsel must be kept abreast of the applicable law that may affect the company that must abide by the OSHA PSM regulation.

#### V. OSHA PSM - TRADE SECRET PRIVILEGE

The OSHA PSM regulation also states that employers can enter into confidentiality agreements with any of the persons who have access to trade secret information through the process of developing the government-required documentation.<sup>18</sup> It is, therefore, important for counsel to be kept informed of the current law relating to confidentiality agreements, current contract law that would apply to the jurisdiction in question, and the judicial enforcement of such confidentiality agreements.

#### VI. THE OSHA PSM INCIDENT/ACCIDENT REPORT

The report that is to be drafted at the conclusion of the investigation must state the following:

1. Date of incident/accident;
2. Date investigation began;
3. A description of the incident/accident;
4. The factors that contributed to the incident/accident; and,
5. Any recommendations resulting from the investigation.<sup>19</sup>



The report is also to be reviewed by "all affected personnel whose job tasks are relevant to the incident/accident findings," and must be retained for five years.<sup>20</sup> It is, therefore, important that management and counsel determine which personnel, including contract employees, have job tasks that are "relevant" to the incident/accident findings. This could mean disclosure of the report to nearly every employee in some cases. For this reason, the report should contain only facts, be concise and accurate, and not contain any opinions or subjective thought to the extent possible.

## VII. CONCLUSION

The OSHA PSM regulations regarding the reporting of incident/accident reports has far-reaching consequences. Any OSHA violation may actually close a business down. Not being prepared for the consequences of the new OSHA PSM regulations can also create damaging results if a company is not fully prepared in a legal sense. Companies which must abide by these new regulations must start making the following immediate plans:

The task force team that will be need to be assembled in the event of an accident of "near-miss" incident should be determined as soon as possible. The team should be composed of the smallest number of individuals who can get the job done properly.

Legal counsel should research law pertinent to confidentiality agreements, draft confidentiality agreements with the task force members regarding trade secrets, and obtain the task members' signatures on the confidentiality agreements.

Legal counsel should prepare a policy statement as outlined above that demonstrates an "attorney-client" relationship.

Once the team is compiled and the legal counsel have developed a policy statement and researched the appropriate law, the company that must comply with the OSHA PSM regulations is in a better position to protect any privileged communications from future civil litigation. The report that is generated by the task force should be brief, concise, and factually accurate. No opinions, surmises, guesses, or conjectures should be included in the report. It should be remembered that the privilege rules and laws will only protect attorney-client communications, and any underlying facts are always discoverable. The OSHA PSM regulations were developed to better protect society from hazardous chemical accidents. These laws must be strictly followed and a litigation nightmare will be averted if legal counsel and management are fully prepared.

1. 29 C.F.R. § 1910.119(m)(1)(3) (1992).
2. Thompson Publishing Group. "Chemical Process Safety Report." December, 1992
3. U.S. Department of Labor, Occupational Safety and Health Administration. OSHA 3132, "Process Safety Management," pgs. 5 & 61-63.
4. FED. R. EVID. 501.
5. Fed. R. Evid. 501.
6. The following cases decided under Federal Rule of Evidence 501 hold that the existence of a pendant state claim does not require the recognition of a state privilege. *See Robinson v. Magovern*, 83 F.R.D. 79 (W.D. PA 1979); *Perrignon v. Berger Brunswick Corp.*, 77 F.R.D. 455 (N.D. Cal. 1978). The following cases decided under Federal Rule of Evidence 501 hold that state law of privileges was applicable. *See Samuelson v. Susen*, 576 F.2d 546 (3d Cir. 1978); *Metroflight, Inc. v. Argonaut Ins. Co.*, 403 F.Supp. 1195 (N.D. Tex. 1975); *Scott v. McDonald*, 70 F.R.D. 568 (N.D. GA 1976); *Commercial Union Ins. Co. v. Talisman, Inc.*, 69 F.R.D. 490 (E.D. MO 1975). The following cases decided under Federal Rule of Evidence 501 hold that state law as to evidentiary privileges was not applicable. *See Garrity v. Thomson*, 81 F.R.D. 633 (D.C. N.H. 1979); *Robinson v. Magovern*, 83 F.R.D. 79 (W.D. PA 1979); *Lewis v. Radcliff Materials, Inc.*, 74 F.R.D. 102 (E.D. LA 1977).
7. *In re Grand Jury Investigation*, 599 F.2d 1223 (3d Cir. 1979); *Natta v. Hogan*, 392 F.2d 686 (10th Cir. 1968); *In re Grand Jury Subpoena*, 81 F.R.D. 691 (S.D. N.Y. 1979), Rev'd on other grounds 599 F.2d 504 (2d Cir. 1979); *Virginia Electric & Power Co. v. Sun Shipping and Dry Dock Co.*, 68 F.R.D. 397 (E.D. VA 1975); *Honeywell, Inc. v. Piper Aircraft Corp.*, 50 F.R.D. 117 (M.D. PA 1970); *Garrison v. General Motors Corp.*, 213 F.Supp. 515 (S.D. CA 1963); *City of Philadelphia v. Westinghouse Electric Corp.*, 210 F.Supp. 483 (E.D. PA), Mandamus denied sub nom. *General Electric Co. v. Kirkpatrick*, 312 F.2d 742 (3d Cir. 1962), *Cert. denied* 372 U.S. 943, 83 S.Ct. 937, 9 L.Ed.2d 969 (1963).
8. *Diversified Industries, Inc. v. Meredith*, 572 F.2d 596 (8th Cir. 1977) (En banc); *Harper & Row Publisher, Inc. v. Decker* 423 F.2d 487 (7th Cir. 1970) (Per curiam), Aff'd without opinion by an equally divided Court, 400 U.S. 348, 91 S.Ct. 479, 27 L.Ed.2d 433 (1971); *Hickman v. Taylor*, 329 U.S. 495, 508, 67 S.Ct. 385, 392, 91 L.Ed. 451 (1947).
9. *Upjohn Co. v. United States*, 449 U.S. 383, 395 (1981).
10. *Id.* at 387.
11. *Id.* at 391.
12. *Id.* at 394.
13. *Id.* citing *Philadelphia v. Westinghouse Electric Corp.*, 205 F.Supp 830, 831 (E.D. PA 1962).
14. *Upjohn Co. v. United States*, 449 U.S. at 394.
15. FED. R. CIV. P. 26b(3).
16. The following cases decided under Federal Rule of Civil Procedure 26(b)(3) hold or imply that the work product privilege litigation is applicable to work product produced in anticipation of terminated litigation. *See Duplan Corp. v. Moulinage et Retorderie de Chavanoz*, 487 F.2d 470 (4th Cir. 1973); *Burlington Industries v. Exxon Corp.*, 65 F.R.D. 26 (D.C. MD 1974); *United States v. Leggett & Platt, Inc.*, 542 F.2d 655 (6th Cir. 1976), cert. denied, 430 U.S. 945 (1977); *United States v. O.K. Tire & Rubber Co.*, 71 F.R.D. 465 (D.C. Idaho 1976).
17. The following cases hold that materials prepared for a previous case are protected by the work product doctrine of Federal Rule of Civil Procedure 26(b)(3) where the previous case and the present case are closely related. *See Midland Investment Co. v. Van Alstyne, Noel & Co.*, 59 F.R.D. 134 (D.C. NY 1973); *Re Murphy*, 560 F.2d 326 (8th Cir. 1977).
18. 29 C.F.R. 1910-119(p)(1)(2)(3) (1992).
19. 29 C.F.R. 1910-119(m)(4)(i)-(v) (1992).
20. 29 C.F.R. 1910-119(m)(6)(7) (1992).

**079 Impact of Different PRA Methodologies on the Results of Nuclear  
Power Plant PSAs (I)**  
*Chair: F.R. Hubbard, FRH*

**Risk Assessment Impacts on Risk Management**  
*K.I. Kiper (N. Atlantic Energy Service)*

**Comparison of PRA Event Tree Approaches - Some Thoughts and Reflections**  
*D.M. Rasmuson (USNRC)*

**On Encountering Small Numbers: How Good Models Go Bad**  
*D.C. Bley, D.H. Johnson (PLG)*

**Completeness and Complexity of PSA: Do They Need it?**  
*A.D. Chambardel, L. Magne (EDF, France)*

## RISK ASSESSMENT IMPACTS ON RISK MANAGEMENT

Kenneth L. Kiper

North Atlantic Energy Service Corp.  
P.O. Box 300  
Seabrook, NH 03874

### INTRODUCTION

This paper describes some insights and issues in risk management that have been identified as a result of applying risk assessment results to real world problems at a nuclear utility.

A number of probabilistic safety assessments (PSAs) has been performed over the last ten years to assess the severe accident risk at Seabrook Station. The initial study was the Seabrook Station Probabilistic Safety Assessment<sup>1</sup>. This study was completed in 1983 as a full scope, Level 3 assessment of the risk from power operation, covering Modes 1, 2, and 3. This assessment has been updated several times by the utility to reflect changes in plant design and operation and in modeling. The 1990 update, titled the SSPSS-1990, was the basis for the IPE Report<sup>2</sup> and the IPEEE Report<sup>3</sup>. In addition, an assessment of shutdown risk was completed in 1988: the Seabrook Station Probabilistic Safety Study - Shutdown<sup>4</sup>. It is a full scope, Level 3 assessment, covering plant operation while in Modes 4, 5, and 6.

These studies have been used in a variety of risk management applications. These have included significant efforts in the areas of:

- Risk based technical specifications,
- Emergency planning strategies, and
- Outage risk management.

As a result of these assessments and applications, insights have been identified for effectively applying the results of risk assessments. Also, several issues have been recognized that will affect the future uses and limitations of risk management.

### RISK ASSESSMENT VS RISK MANAGEMENT

The use of PSAs has brought into focus the distinction between *risk assessment*, the analysis to estimate the level of risk, and *risk management*, understanding the basis for the risk and applying this knowledge to make decisions. It is clear that risk assessment, by itself, does not make the plant safer. It requires applying the insights to modify hardware (system design, component type, etc.) or software (procedures, administrative controls, etc.). The product of risk assessment has often been a report that looks good on the shelf and that is useful for external consumption - e.g., NRC review. Risk assessment tends to concentrate on areas such as more elaborate data analysis, expanding the detail of plant modeling to assure completeness, and refining the treatment of uncertainty.

Risk management, by contrast, tends to be less tidy and more difficult to document in neat reports. The issues of configuration control, model updates, limits of the model, etc. must be addressed. Even with the most detailed risk assessment, the models often do not have sufficient detail in the areas where applications are being evaluated. The risk assessment needs to be expanded "locally" in order to adequately model the change, especially to show that a change is not significant.

While risk management is the ultimate objective, it is imperative to have a quantitative risk assessment in order to do adequate risk management. The most important products of assessment are the risk insights that it reveals, but these insights are not possible without an effort to assemble our knowledge down in numerical form.

Risk assessment needs to focus on the creation of a tool to assess risk, as the logic and data change, rather than a static result.

## **RISK VARIABILITY**

One of the important insights from the shutdown risk assessments performed on Seabrook is the variability of risk with time and plant configuration at shutdown. At times during shutdown (e.g., midloop), the risk approaches or exceeds the at-power risk; at other times, the risk is minimal (e.g., with the fuel in the spent fuel pool). In general, the *average* risk, as calculated in most risk assessments, is not a useful concept for risk management during shutdown. Based on our experience in outage risk management, the dynamic nature of risk has focused increased attention to configuration control and contingency planning.

The risk at-power has much less variability with time than at shutdown. Risk variability does exist, however. For example, the ATWS risk peaks at the beginning of the fuel cycle, while at the same time, the fission product source term is at a minimum. The tornado and hurricane occurrence is random but has seasonal variations in expected frequency. Considerations of this time and configuration dependence on plant risk may become important to safety, especially as risk assessments are used to make decisions over a shorter time period.

## **AVERAGE RISK VS ACTUAL (INSTANTANEOUS) RISK**

The risk that has been calculated in most current risk assessments is average risk - the risk over a long period of time (e.g., the plant lifetime) and over a large set of equipment. The basis for the systems analysis quantification is the assumption of constant, random failure rate. In reality, equipment does not fail randomly; it fails because of a manufacturing flaw, an installation error, a maintenance or operation error, or a wear out failure. However, if the model is averaged over long enough time period, the assumption of a constant, random failure rate is appropriate. The use of such average risk assessments has generally been to make decisions for the long term - e.g., Technical Specification changes that will apply for the life of the plant.

However, the issue of the variability of risk raises the possibility of making risk management decisions based on the specific instantaneous plant configuration. In order to be useful to the operators as a "risk meter", the risk model would have to reflect the actual plant configuration, the status of variables such as the time in

cycle, and the state of knowledge of the operators about equipment conditions. Even with that detail, instantaneous risk raises questions about the validity of modeling assumptions. For a short period of time, random failure rate may not accurately describe the operators' true state of knowledge. He may know, for example, that the diesel has just been tested successfully or that a service water pump has higher than normal vibrations.

## UNCERTAINTY VS SENSITIVITY STUDIES

The most complete risk assessments take careful account of uncertainty in all inputs to the quantification. This is a proper consideration because uncertainty is the basis of risk. However, while an uncertainty distribution is a better statement of risk than a single number, it does not tell the analyst what contributes to that uncertainty. Of more value in using the results are sensitivity studies on the important parameters in the assessment. This can tell the analyst where there is margin (where changes can be made without influencing the overall results) and what inputs are important and possibly should be examined in more detail.

The traditional method of quantifying the uncertainty is by estimating the upper and lower ranges of the variables in the model. This assumes that the major uncertainty is in the value of the parameters. It is possible that the assumptions built into the model - e.g., random failure rate - may dominate the uncertainty and may not be reflected in this estimate of uncertainty. The risk manager is cautioned to treat the results of all risk assessments with some skepticism, to assure that the model accurately reflects reality.

## RISK STABILITY AND LIVING PSAS

In order to make the risk assessment usable over the life of the plant, a living PSA will be needed. The Seabrook PSA updates have included hardware and procedural changes, generic and plant specific data updates, considerations of new failure modes and phenomena, and changes in modeling techniques. As a result of these updates (due primarily to modeling changes, not hardware changes), the core damage frequency has decreased by about a factor of 2.5; however, the dominant risk contributions have remained unchanged from the original SSPSA to the current SSPSS-1993. Thus, the risk assessment has been *stable* with regard to major insights. However, for specific systems or operator actions, changes have occurred in the updates that change their relative importance. This is expected to continue for the future as the plant design evolves, plant data is available, and new phenomena are identified. A proper risk assessment can be expected to maintain *global* stability as minor changes to the plant and models are made. *Local* stability, i.e., the relative importance of a specific system, is not so certain.

For example, the success criteria for feed-and-bleed cooling was changed in the latest SSPSS update, based on a more detailed thermal-hydraulic analysis. As a result, the feed-and-bleed capability is quantified as more reliable, which has the effect of making secondary cooling (EFW) relatively less important. The importance of EFW changed from about 15% contribution to core damage frequency to about 5%. However, the overall risk profile did not significantly change.

The local stability of risk raises the issue of risk management decisions. Do

these decisions need to be reconsidered when the update is made? This is related to the criteria used to make risk decisions.

## **ABSOLUTE VS RELATIVE RISK ACCEPTANCE LIMITS**

In order to make risk management decisions, a criteria has to be used for the level of risk change that is judged not significant. Generally, it is difficult to quantify all the impacts of a change - e.g., the improved component reliability from less testing. Because of this limitation, the quantitative results often tend to show a numerical increase in risk. Some criteria is needed to make consistent risk management decisions. There are two general criteria - absolute, e.g., use of a screening frequency, and relative, e.g. a small percentage change. The advantage of the first is that it remains unchanged as the model is updated. The relative change, however, is affected by the changes to the rest of the model. As the total CDF is decreased, the relative change may increase in size, raising questions of the stability of risk management decisions.

## **CONCLUSION**

A number of issues have been identified as a result of experience applying risk assessment. These issues will need to be addressed as the field of risk management matures.

## **REFERENCES**

1. "Seabrook Station Probabilistic Safety Study", PLG-0300, Pickard, Lowe and Garrick, Inc. for Public Service Company of New Hampshire (1983).
2. K. L. Kiper, P. J. O'Regan, D. M. Kapitz, and J. F. Bretti, "Individual Plant Examination - Report for Seabrook Station," New Hampshire Yankee (1991).
3. K. L. Kiper, P. J. O'Regan, V. B. Dimitrijevic, "Individual Plant Examination, External Events - Report for Seabrook Station," North Atlantic Energy Service Corp. (1992).
4. K. L. Kiper, J. H. Moody, W. Doskocil, T. J. Casey, and K. N. Fleming, "Seabrook Station Probabilistic Safety Study - Shutdown Modes 4, 5, and 6," New Hampshire Yankee (1988).

## COMPARISON OF PRA EVENT TREE APPROACHES - SOME THOUGHTS AND REFLECTIONS<sup>1</sup>

Dale M. Rasmuson

Division of Safety Programs  
Office for Analysis and Evaluation of Operational Data  
U.S. Nuclear Regulatory Commission  
Washington, D. C. 20555

### INTRODUCTION

The author recently published a comparison of the large event tree (LET) and small event tree (SET) approaches used in probabilistic risk analysis (PRA). In that paper<sup>1</sup>, he showed that both approaches produce the same cut sets and same quantitative results when identical models and assumptions are used. In that analysis, the only variation in the analysis was the solution method. The component failure probabilities, the system success criteria, and the modeling detail were identical. These are areas that can greatly influence the results of the analysis.

In this methods comparison, the same numerical results and the same cut sets were obtained. The number of core damage sequences was smaller in the SET approach (2) than in the LET approach (8). Thus, the minimal cut sets were partitioned in a different way, but the identical cut sets were generated by both methods.

Today the two approaches are producing results which are more consistent with each other and produce similar insights. One reason for this is that more detail is being put in the fault tree and event tree models. The models for both approaches

---

<sup>1</sup> The opinions and viewpoints contained in this paper are the author's personal ones and do not necessarily reflect the criteria, requirements, and guidelines of the U.S. Nuclear Regulatory Commission.



contain more details - in the event trees, the fault trees, and Boolean equations. Conservative approximations in both approaches have been replaced with more realistic and better computer techniques for solution. However, the basic difference between the two approaches still exists, i.e., the LET approach develops event trees which contain dependencies, while the SET approach models the dependencies, in general, on the fault trees.

The SET approach produces large numbers of cut sets which the analyst must look at. Because the analyst cannot look at all of them, the cut sets are ranked by probability (frequency), and only those which contribute to the accident sequence core damage frequency are kept and analyzed. The LET approach produces a large number of sequences. The logic for the sequences must be checked. The accident sequences need to be ranked by probability (frequency) because the analyst cannot examine all of them. (The number of accident sequences in an event tree can potentially be in the millions as can the number of minimal cut sets.) Thus, both approaches produce lots of cut sets or sequences that the analyst must deal with.

Most PRA analysts agree that the most important results obtained from a PRA are the qualitative insights gleaned during the analysis. These insights are identified in each step of the analysis. These steps are: system and plant familiarization, modeling, failure data preparation, quantification, common cause failure analysis, human reliability analysis, and uncertainty analysis. This paper discusses some important items that can have a great influence on the qualitative and quantitative results of a PRA. Many of these items are not new. Yet, PRAs and Individual Plant Examinations (IPEs) continue to be produced which do not address many of these concerns.

## MODELING AND QUANTIFICATION

In Reference 1, the author showed that the two principal approaches to event tree modeling, the large event tree and the small event tree approaches, produce the same numerical results if consistent assumptions are maintained throughout the analysis. However, this may not be true in practice. Most discrepancies usually arise because of differences in the basic assumptions about system success criteria, treatment of support systems, and treatment of dependencies in the modeling. For example, the FSAR system success criterion for a certain plant is 2-out-of-3 pumps, which was used in a PRA of the plant. In an update of the PRA, other analysts utilized a new success criterion of 1-out-of-3 pumps for the system. The justification for the change in the success criterion was that thermal-hydraulic analyses indicate the system will perform its design function with only 1 pump.

Such changes in assumptions can affect the sequence minimal cut sets, the quantitative results, and the insights. The basis for these changes may be results from a computer code which has not been fully validated, or which may not contain as much detail as other computer codes that model the same phenomenon. In these cases, it

may be helpful to perform sensitivity calculations using the thermal-hydraulic code to investigate the effect of the code on the PRA assumptions, especially if the assumptions involve dominant accident sequences.

Examples of PRAs that have been done in recent years are the NUREG-1150 studies for Surry, Sequoyah, Peach Bottom, and Grand Gulf. The IPE submittals for these plants contain different core damage frequencies and insights. Different assumptions were made and levels of detail were included in the logic models.

## **PARAMETER ESTIMATION**

Data collection and parameter estimation are probably two of the weakest areas in the PRA. One reason for this is that reliability data collection and analysis are expensive. Managers do not realize that the same data can be used for other activities, such as maintenance and technical specification modifications, besides the PRA itself.

### **Initiating Event Frequencies**

Many of the recent NRC-sponsored PRAs have used generic initiating event frequencies. This may be all right for certain applications, but it should not be a general practice. Two reasons for this are: (1) plants are operated and maintained differently and thus have different initiating event occurrence rates, and (2) some initiating event frequencies have improved over time. Consider reactor scrams. The average industry scram rate (related to transient initiating event frequencies) has decreased by a factor of two or three over the last six years.

### **Maintenance Unavailability Data**

In the IPEs, some plants used maintenance logs and spent considerable time estimating component unavailability due to maintenance. In other studies, the PRA analysts polled maintenance personnel and asked them how long it would take to repair a component. They would obtain two estimates by asking how long it would take to fix the equipment or how fast the equipment could be restored to service. These estimates were treated as percentiles of a lognormal distribution. With this information, the parameters of the lognormal distribution were estimated.

### **Generic Versus Plant-Specific Data**

Many IPEs and PRAs have used generic estimates of basic event failure probabilities. In other cases, the analyses have included plant-specific failure data based upon a time period that does not represent the time period of the plant configuration being modeled. For example, data from 1982 through 1987 may be used when the models represented the plant as configured in 1991. The extent to which a PRA of a plant uses plant-specific data is directly proportional to the usefulness of the PRA to that particular plant.

## COMMON-CAUSE FAILURE ANALYSIS

Common-cause failure analysis (CCFA) has matured in the last five years. Reference 2 provided a focal point for CCFA by unifying important work in this area. During the preparation of Reference 2, it became evident that the real benefit from a CCFA was an understanding of the common-cause failure mechanisms and defenses to reduce common-cause failures. This led to the development of the ideas in Reference 3. It also became apparent that the guidance contained in Reference 2 was not clear enough or explicit enough. This led to the publication of Reference 4.

The guidance provided for performing CCFA in the IPEs was that the ideas and concepts contained in Reference 2 should be followed. Few, if any, IPEs really followed all of the guidance. Most identified sets of redundant and similar components to be modeled as common cause basic events in the logic models. Few followed the guidance of developing a pseudo plant-specific common cause event data base tailored for the plant from the industry common cause events. Thus, many of the IPEs used generic beta factors or other estimates (e.g., gamma and delta of the Multiple Greek Letter Method).

CCFA is resource intensive, and there is a lack of data. These factors discourage analysts and sponsors from doing a thorough CCFA. However, performing a quality CCFA will result in qualitative insights that will help improve plant safety and help achieve more efficient operation.

## HUMAN RELIABILITY ANALYSIS

Human reliability analysis (HRA) is very controversial. Some HRAs contained in the IPEs were performed very rigorously and thoroughly by qualified personnel. Many HRAs are performed by system analysts who try to apply the HRA concepts in a consistent way, but they lack the training and experience to obtain the qualitative insights which are produced from a task analysis and other human performance evaluations performed by human performance specialists. Some IPEs used generic human error probabilities (HEPs) throughout the analysis. Others used several HEP quantification methods and then selected the largest HEP to use in their analysis.

HRA is another resource intensive area of the PRA which seems to produce little return for the expenditure. This is probably true if it is not done systematically. This is also an area that needs considerable methods development and data collection. Studies have shown that different analysts and models produce results that vary by orders of magnitude for the same situation. This is one area that needs additional research and data collection.

## UNCERTAINTY ANALYSIS

No PRA is really complete without an uncertainty analysis. First, the uncertainty analysis provides an interval estimate for the core damage frequency. Secondly, it produces an estimate of the mean core damage frequency that is closer to the true value than the point estimate obtained using the mean values of the basic events in the minimal cut sets.

A common situation in which dependencies are introduced into the model occurs when two components have the same failure rate or demand probability and this probability is estimated from a single data source. In the uncertainty analysis the failure probability of both components is represented by the same random variable. This practice of using the same uncertainty distribution for a group of similar components has been common since the Reactor Safety Study.<sup>5</sup> The PRA Procedures Guide<sup>6</sup> recommends this practice as well. Several philosophical arguments have been given to support this practice. (See, for example Reference 7.) The following helps to clarify this practice.

Consider a simple example involving a cut set with two components. Let  $q_1$  and  $q_2$  denote the unavailability of the two components in the cut set. If the components are independent, then

$$Q = q_1 q_2. \quad (1)$$

The expected value and variance of  $Q$  are given by:

$$E(Q) = E(q_1)E(q_2) = \alpha^2 \quad (2)$$

where  $\alpha$  is the expected value of  $q_i$ .

If the unavailabilities are not independent, which is the case when the common unavailability is estimated from the same data source, then  $q_1 = q_2 = q$ , and Equation 1 becomes

$$Q = q^2. \quad (3)$$

Equation 2 reduces to:

$$E(Q) = E(q^2) = \alpha^2 + \beta^2 \quad (4)$$

where  $\alpha$  is defined as above and  $\beta$  is the variance of  $q_i$ .

Thus, for the case of identical components we see that we should really be estimating  $q^2$  instead of  $q_1 q_2$ . Equation 4 should be used especially when the point estimates are the means of highly skewed distributions. If we simply square the mean of this skewed distribution, the estimate of  $Q$  will be very biased. This is why the point

estimate and the mean of the uncertainty distribution are not equal in PRAs.

## SUMMARY

The paper has presented some examples of areas that can greatly influence the results, both qualitative and quantitative, of a PRA. These areas are modeling and quantification, parameter estimation, common-cause failure analysis, human reliability analysis, and uncertainty analysis. As reliability techniques and PRAs become more integrated into the regulatory process, the importance of providing better guidance for performing these tasks grows.

## REFERENCES

1. D. M. Rasmuson, "A comparison of the small event tree and large event tree approaches used in PRAs, *Reliability Engineering and System Safety*, 37, 79-90 (1992).
2. A. Mosleh, et al, *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, NUREG/CR-4780, Volume 1 (January 1988) and Volume 2 (January 1989).
3. H. Paula, et al, *A Cause-Defense Approach to the Understanding and Analysis of Common Cause Failures*, NUREG/CR-5460, March 1990.
4. A. Mosleh, *Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis*, NUREG/CR-5801 (April 1993).
5. U. S. Nuclear Regulatory Commission, *Reactor Safety Study--An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*, WASH-1400, NUREG/75-014 (October 1975).
6. J. W. Hickman, *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*, American Nuclear Society and Institute of Electrical and Electronic Engineers, NUREG\CR-2300, Volumes 1 and 2 (January 1983).
7. G. E. Apostolakis and S. Kaplan, "Pitfalls in Risk Calculations," *Reliability Engineering*, 2, 135-145 (1980).

## ON ENCOUNTERING SMALL NUMBERS: HOW GOOD MODELS GO BAD

Dennis C. Bley and David H. Johnson

PLG, Inc.  
4590 MacArthur Boulevard, Suite 400  
Newport Beach, CA 92660-2027

Good engineering practice requires that we revisit modeling techniques and assumptions at regular intervals. Reflecting on the status of PSA modeling, a variety of factors may be converging to threaten the credibility of our studies:

- Forgotten Assumptions
- Model Expansion/Fragmentations
- Cookbook Rules for Analysis
- Plant Improvements
- New Generation Plant Designs
- Things that Were Never Done Well

We say this because we see the results of PSA studies presenting smaller and smaller numbers (lower frequencies of damage). When the question is raised—Are these results appropriate?—the answer may be no. When that happens, some combination of the above factors has led the analyst astray. This paper will provide examples of these effects.

Analytical limitations in the early days of risk assessment demanded the use of pragmatic simplifications to model large systems. Failures of passive equipment such as pipes, wiring, and multiple check valves were excluded from the quantitative analyses since they generally represented a very small contribution to system failure. Computational tools were just being developed, and our understanding of key phenomena such as human actions and success criteria was characterized by large uncertainty. Much of the bookkeeping associated with the complex risk assessment process was performed manually. While attempting to derive as realistic a measure of the risk as possible, the results for quantified scenarios were often rather conservative. The impact of the unquantified scenarios is nonconservative but was assumed to be small.

The assumptions of the time were checked against the results of that time and found to be reasonable. However, they have passed into general practice and have become rules of analysis. When plant improvements reduce the surrounding sea of risk, or when new systems with different design bases are examined, analysts all too often apply these "rules" without retesting their validity.

If core damage frequency is reduced by a factor of 10, and that is observed in recent studies,<sup>1</sup> many assumptions must be revisited. If we are to analyze the new design

proposals for passive reactors, we must go further and look for new questions: probably a focus on the physical phenomena that make the passive safety features effective must be developed. We need to raise questions about how the passive process can be interrupted. For example, is external cooling of low points in a natural circulation loop possible?

Two events have had significant impact on the direction of PSA—improvement in computational tools and expansion of risk management activities. Modern calculational tools have allowed us to create models that provide substantial detail. At the same time, our understanding of the behavior of plant systems and operators in response to plant upsets has improved. It is now possible to create models that are more realistic and complete. In addition, many facilities have performed PSA studies and used the results to manage the risk; i.e., modifications to the plant design and operating practice have been based on the PSA results.

The effects of these changes is that we see larger but often fragmented PSA models and that the risk at old and new facilities is improving. The fragmentation of our models means that it is more difficult to survey the impact of assumptions, calculational tricks (e.g., frequency cutoffs in fault tree and event tree analysis), and sequential dependencies among equipment failures and sequential human actions.

The quantitative impact of these tricks is not easy to obtain. However, it has been shown that frequency cutoffs can lead to severe underestimates of core damage frequency.<sup>2</sup>

In addition to the changing environment for PSA, there is a class of things we have never done well. In the beginning, we did not know how, assumed that they were of minor impact, or had not even thought of them. A recent paper<sup>3</sup> identified a number of cases, as follows:

- Aging degradation of active and passive components.
- Common cause failures in multiple systems.
- Causal models of human reliability.
- Organizational and management factors affecting plant safety.
- Arrest of core degradation before vessel breach.
- Software and computer reliability.
- Design and construction errors.

While analysis of some of these factors has been performed, this has not yet become general practice,<sup>4</sup> and some available techniques are still quite premature.

As we enter this new era of risk assessment, we need to have a firm understanding of the implications of our commonly used modeling assumptions and techniques. Now is not the time for the blind application of prescriptive techniques. It is as relevant as ever to attempt to avoid including unnecessary events that do not contribute "significantly" to the results in models. However, at what point do these residual events become collectively important? Practical considerations often dictate that some form of truncation be made during the quantification process, but at what point does this impact the resolution of the results?

PRA analysts can provide an impressive amount of information to decision makers. As in any activity, it is all too easy for the analysts to lose a measure of perspective. Our main message in this paper is to remind PRA practitioners of the importance of identifying and understanding the bounds and limitations of the tool that they have created. We believe that this understanding begins with the exercise of developing an understanding of small numbers: what they mean, what they can imply, and what they may hide.

As plants are improved to minimize the detrimental effects of what is modeled in PSA, PSA analysts must ensure that the facilities do not become more vulnerable to those hazards that have been excluded from the models. The spotlight that we shine on plant vulnerabilities creates shadows that must be continually reexamined. A major clue to keep our models from going bad is found in the numbers we produce.

## REFERENCES

1. "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," Final Summary Report, NUREG-1150, Vol. 1, U.S. Nuclear Regulatory Commission, Washington, D.C. (1990).
2. R.K. Virolainen and I.M. Niemelä, "Implementation and Introduction of Living PSA in Co-Operation with Finnish Utilities and Authorities," Proceedings of the International Topical Meeting on Probabilistic Safety Assessment, pp. 273-277, Clearwater, Florida (1993).
3. S. Hirschberg, "Prospects for Probabilistic Safety Assessment," *Nuclear Safety*, Vol. 33, No. 3, pp. 375-380, Switzerland (1992).
4. D. Bley, S. Kaplan, and D. Johnson, "The Strengths and Limitations of PSA: Where We Stand," *Reliability Engineering and System Safety*, 38, pp. 3-26 (1992).



## COMPLETENESS AND COMPLEXITY OF PSAS: DO THEY NEED IT?

A. Dubreuil Chambardel and L. Magne

Electricité de France (EDF),  
Research and Development Division,  
Safety and Reliability Department  
1 avenue du Général de Gaulle  
92141 Clamart (France)

### A COMPLETE PSA

The primary objective of a PSA is to assess the risk of core meltdown (Level-1 PSA) or of discharge of radioactive elements into the environment (Level-2 PSA). The assessment must have a good "value for money" ratio. But how can one guarantee that the level of accuracy is sufficiently high? How can one certify that nothing major has been overlooked?

As an example, the PSA conducted by EDF on the Paluel power station in France was done in three phases: accident scenarios were assessed three times, but some of the major scenarios, like those concerning coolant dilution at the RHRS low level threshold were only discovered at the end of the third phase [1]. It appears to be important, therefore, in order to have a certain confidence in the results, to have a relatively advanced level of detail by virtue of which the PSA does not overlook any accident scenarios, and to devote a substantial amount of time and work to looking for new scenarios, or "inconceivable" events (refer to the work of Östberg on this point [2]).

This is especially true for the most recent reactors or those still on the drawing boards which have been "optimized": in these reactors, the "defects" detected by feedback from older reactors or by PSAs have been remedied, so that what were major accident scenarios in the first PSAs have now become improbable or even impossible; the risks are not the same, and what was negligible for the oldest reactors can now be major. The exhaustivity of PSAs must therefore be constantly enhanced, and this becomes increasingly complex when you are looking at core-melt risks of around  $10^{-7}$ /year.

A second objective of PSAs is to make it possible to use them as a tool in design or operation of nuclear power stations. Such applications include, for example, analysis of technical operating specifications, optimization of maintenance through greater reliability (Reliability Centered Maintenance - RCM) and incident or accident precursor analysis.

The first application involves calculating the maximum time authorized for continued operation with a particular equipment item inoperable, and the second involves calculating the importance of the failure modes of that

equipment item with respect to core meltdown in order to determine whether or not it should be given preventive maintenance. In both cases it is vital for the equipment item to be modelled in the PSA with a sufficient degree of accuracy, for in the case of the first application, the inoperability of the equipment goes from a low value to 1. It is therefore important to ensure that scenarios that could have been negligible, but which are no longer negligible in this sensitivity study, are indeed modelled. Moreover, the use of importance factors like the risk achievement worth, which is calculated on the basis of a limited minimum cut set, could be an important cause of mistake.

Analysis of precursors involves estimating the potential consequences of incidents in order to learn lessons that can be usefully applied to operation and design. The analysis must be qualitative and quantitative. It sets out to determine all the major scenarios that could have brought about a deterioration in the situation and led to the core melt. It puts the spotlight on all the "barriers" (automatic systems, engineered safeguard systems, procedures, operator's interventions, etc.) between the incident and core meltdown, and assesses their effectiveness. To extract really relevant information from this feedback on experience, it is vital to perform very finely detailed analysis of these incidents. It is easier to start from detailed PSAs. Engineers from Duke Power have demonstrated the value of using plant-specific PRA models in analyzing the potential consequences of the incidents their units have experienced [3]. These models are necessarily more detailed than the very generic models used in the US NRC ASP programme<sup>1</sup>. They give much more conservative results.

For all the applications of PSAs aimed at loosening regulations, one has to start with realistic PSAs that are neither too conservative (in which case nothing at all can be relaxed!) nor too optimistic (in which case the demonstration would not be credible). That is how EDF came to study reactor shutdown statuses (indispensable for determining technical operation specifications or organizing maintenance programmes) and long-term scenarios. The long-term scenarios were particularly valuable, enabling assessment of the benefits of medium-term emergency action between low-pressure safety injection and containment spraying; without this mutual emergency action, the medium-term risk (beyond 14 hours) is far from negligible. These fine features of modelling result in not only a relatively advanced level of detail, but also a varied choice of methods, as is explained hereafter.

However, despite all the effort one can put into making PSAs as detailed as possible, they will never be exhaustive, and uncertainty will remain important (be it relative to the human factor, common-cause failures, or external influences like earthquakes). This considerably reduces the power of PSAs as decision-support systems, and requires a lot of skill on the part of users if they are to appreciate whether their application of PSAs is relevant or not.

## A COMPLEX PSA

The desire to study long-term scenarios after a LOCA without being excessively conservative, to finely model the operation of an electrical power distribution system and intermediate cooling systems (CCS and ESWS) and their multiple configurations, or the operation of systems alternating operation and test phases (automated I&C), led EDF to make use of Markovian techniques [4],[5], something that is in fact recommended by the IAEA [6].

<sup>1</sup> ASP (Accident Sequence Precursor) models consist of eight sets of event trees. These eight sets represent all the nuclear power stations in the United States (five sets for PWRs, and three for BWRs).

Similarly, we developed a technique for quantification of accident sequences in event trees. This technique is based on the result of convolution of reliability or system-repair laws against time in order to take account of [7] the fact that i) in some accident scenarios one system will operate in normal-emergency mode with another, which means its operating time is random, depending on the duration of correct operation of the first system, and ii) that the duration of correct operation of the systems and the length of time (increasing with time) between the moment of failure of a system and the moment when the core starts to be uncovered can be put to good use to repair equipment that is out of order, and thus prevent core meltdown.

These methods taking account of sequence dependencies certainly allow for finer analyses by more realistically modelling the operation of systems, and result in more robust reliability models since they contain practically no reliabilistic simplification. They do, however, have some disadvantages:

1. they often result in complex reliability models, because of the method itself<sup>2</sup> or because they make it possible to take account of a large number of parameters (like changes in system configuration, repairs, tests and system maintenance, and changes in the status of the unit in the case of substantial deterioration of the system) that cannot be taken into account by other means;
2. PSAs involve the management of several Boolean and sequential methods, which considerably complicates the PSA processing tool, particularly when it comes to processing results;
3. it is not possible to simultaneously take account of sequence and functional dependencies, e.g. it is not possible to have a Boolean reduction of two Markov graphs; what accuracy is gained in one respect is lost in another.

For the moment we have the choice of three approaches for dealing with a PSA.

The first is entirely Boolean (fault and event trees): it is the most common.

The second involves Boolean processing of the generic events of event trees, with numerical linking of the results of fault trees in order to avoid combinatorial explosion of Boolean processing of event trees, and thereby to allow for a high level of detail in the fault trees; but this method developed by PLG calls for prior detection of dependencies between generic events.

The third approach developed by EDF uses fault trees and Markov graphs to model the generic events of event trees, and uses numerical linking of the results of these models: this makes it possible to take account of the sequence dependencies and the most important functional dependencies detected previously.

Each of these approaches has its advantages and disadvantages in terms of design (simplicity and ease of processing results in the case of a "pure Boolean" approach, degree of detail in the case of numerical linking, and accuracy and robustness of models in the case of an approach combining Boolean and sequential methods) as well as of the organization set up to conduct the PSAs. Approaches using numerical linking of models make the studies relatively independent of each other, and thus provide greater flexibility in organization: "pure" Boolean processing requires perfect coherence of models, which is a factor in quality but one which implies more stringent organization, probably entailing small numbers of people working on the reliability models.

These approaches are complementary, and it would be interesting to merge them. Such a merger could cover several aspects, including "juxtaposition" and "integration" of tools.

In "juxtaposition" of tools (one for Boolean processing and one taking account of sequential aspects) the second tool would enable detection of key sequence dependencies and would help and validate construction of a Boolean PSA model sufficiently robust to handle the applications. This model would be processed by the first tool.

<sup>2</sup> Which is why some people use these methods for studying simple systems only [8].

Real "integration" of both tools would result in there being a single tool. Parts of the PSA would be entirely processed by Boolean logic, and others would be processed sequentially. The best-suited method would be chosen for each case.

As part of international co-operation procedures, EDF is to start work on comparing these different approaches and defining the areas to which they can best be applied, with a view to specifying and then "merging" the respective tools. The ambitious aim of this work is to develop, insofar as possible, a methodology for drawing up PSAs and a tool for processing them so that sufficiently thorough, accurate, robust, and user-friendly PSAs can be made and applied in the manner referred to at the start of this article by persons not involved in the creation of those PSAs. It would very likely lead to PSAs dedicated to each application.

## A NECESSARY COMPROMISE

PSAs are generally first drawn up to demonstrate safety. They are often unsuited for applications aimed at helping in design or operation, for they need "fine tuning" and amendments. Moreover, as the number of applications increases, they can no longer be the responsibility solely of reliability engineers, and they are gradually transferred to "design" or "operation" experts who are not necessarily operating-safety specialists. It is therefore clear that these "thorough" and "complex" PSAs made principally for safety assessment are not easily mastered by people not involved in their development.

It is therefore necessary to find an optimum level of detail. The detail must be sufficiently thorough for analysts to find the information they require. And it must also be sufficiently restricted so that the model remains within the range of individual understanding, allowing an "occasional" user to correctly and successfully use the model for his own applications. The degree of detail must also be uniform, for if the processing of a PSA uses probabilistic truncation thresholds that vary from one sequence to another, there is a risk of introducing equipment with low contributions into the minimum cut set while other equipment with a greater contribution is eliminated elsewhere. In an RCM programme, improper interpretation of results could result in maintenance being upgraded on equipment with relatively insignificant safety functions, to the detriment of much more vital equipment.

In fact, the main concern should be to have a robust model, i.e. to ensure that everything that is modelled and quantified is modelled and quantified correctly. In other words, only the most significant human errors and equipment failure modes should be included, and the major sequences where these events occur should be modelled and quantified.

It is better for an equipment item not to be modelled than to be modelled incorrectly. In the first case there will be no PSA conclusions on the matter, and other decision-support systems will have to be applied, or a special model will have to be developed in response to the problem; in the second case, erroneous conclusions could be made, with possibly drastic consequences on plant safety, availability, or operating costs.

To minimize the risk of improper use of these studies by persons not involved in their creation, it may be very useful to draw up "operating instructions" for the studies. "Operating instructions" would be based on intensive use of the graphic interfaces of the PSA model. All the basic events, generic events, and probabilities of accident sequences should be featured and commented. The main assumptions necessary for building fault or event trees should be described. There could also be a summary presenting the PSA architecture, i.e. the various families of accident scenarios, the systems involved, the links between these systems and the accident sequences (which sequences a given system or equipment item might be involved in). This document could also specify the scope of validity of the PSA (which data or

assumptions can be varied and still provide a valid result). This is certainly a critical sort of document to draw up, but it would be a most precious aid to PSA users [9].

Sequential methods are often more complex to use than Boolean methods, and can give rise to models which are more difficult to use in applications. They do have the advantage of not requiring simplifying assumptions to take account of sequential aspects, and therefore make more robust models with fewer implicit assumptions, so they are more easily traceable, though often less legible<sup>3</sup>. Sequential models must be used appropriately. EDF has therefore decided to run two PSAs (one on its 900 MW plants, and one on its future 1450 MW "N4" plants) chiefly using Boolean models in order to have as much experience with "Boolean" PSAs as with "sequential" PSAs. At the outcome of these two studies, EDF will be able to specify the "tool of the future" referred to above.

The development of applications implies a growing number of users on a variety of sites. These applications can enable PSAs to be enriched [10]. Incident analysis, for example, makes it possible to validate or invalidate PSA incident scenarios by matching PSAs against reality; it also makes it possible to detect any initiating events not taken into account in the PSA, or to recalculate the probability of occurrence of an event. To make it easier to achieve coherence between these applications and to enable each to benefit from the lessons learnt from others, it would be advisable for applications to be able to communicate with each other. EDF has therefore developed its PSAs on networked work stations, and attributes much importance to the management of data and models: studies of sensitivity to a change in models or data are performed without "overwriting" the results of the "reference study". This organization makes it possible for each developer to work on his own applications with the same reference model as other developers. The reference model approved by the safety authorities is updated from time to time, taking account of new feedback on experience, amendments to design or operating procedures, and the contribution of the various applications to the PSA models.

## CONCLUSION

But whatever the progress made in reduction of uncertainties, in the robustness of models, and in the user-friendliness and management of PSAs, they are nonetheless a complex and approximated modelization of reality. They could be a powerful analysis tool ("What would the risk be if ...?"), but a dangerous one if incorrectly used. That is why it is necessary to make advances in the completeness and robustness of models, in the accurate definition of their scope of validity, and in facilitating operational familiarity with them so that PSAs can be correctly applied. This requires optimization of the level of detail, use of complex methods only when absolutely necessary, and preparation of manuals for use of these studies. A compromise must be made between complete but complex models and models that can really be used.

Furthermore, even complete and detailed PSAs do not give answers to all questions on safety. New approaches that complement PSAs - particularly human factors (psychological, cognitive) or organizational factors (with respect to operation and maintenance) - must be explored in order to arrive at a global approach to safety. Progress must also be made in what is known about PSAs so that their relevant applications and the fields in which they are of no relevance can be defined in detail. These studies still need to be matured

<sup>3</sup> For the same modelling precision, sequential models like Markov graphs are more traceable than Boolean models in the case of consideration of time dependencies. However, when a Markov graph is used, the opportunity is taken to model a large number of time dependencies whereas normally, with a Boolean model, the model would be restricted to the most important time dependencies; Boolean models therefore appear to be more simple and more legible than the graph.

before they can achieve recognized status in the same way as thermohydraulics, mechanics, or neutronics.

What is at stake in the nuclear industry deserves every ounce of this work!

## REFERENCES

- [1] "EPS 1300: Probabilistic Safety Assessment of Reactor Unit 3 in the Paluel Nuclear Power Centre (1300 MWe), Overall Report" (May 31, 1990)
- [2] G. Östberg, "Evaluation of a Design for Inconceivable Event Occurrence", *Materials and Design*, Vol. 5 (April/May 1984)
- [3] B.E. Busby, K.S. Canady, P.M. Abraham, "Accident Precursor Program at Duke Power Company".
- [4] A. Dubreuil Chambardel, "Why Markovian Techniques were used in EDF's PSA of Paluel", PSAM, Beverly Hills (February 4-7, 1991).
- [5] L. Magne, M. Balmain, "Comparison of Various Methods Used in PSAs: First Lessons", PSA 93, Clearwater (January 29-25, 1993).
- [6] "Case Study on the Use of PSA Methods: Assessment of Technical Specifications for the Reactor Protection System Instrumentation", IAEA-TECDOC-669.
- [7] A. Dubreuil Chambardel, "ELSA: un Ensemble de Logiciels quantifiant les Séquences Accidentelles", EDF-DER - HT13/4/85 (January 1985).
- [8] N.E. Deeb, J.M. Pabich, T.R. Eisenbart, "Power Plant Electrical System Reliability Evaluation", *Nuclear Plant Journal* (September-October 1992).
- [9] Operating instructions
- [10] J. Dewailly, S. Deriot, A. Dubreuil Chambardel, Ph. François, L. Magne, "Living PSA Issues in France on Pressurized Water Reactors", IAEA TCM on "Use of PSA for Optimizing NPP Operational Limits and Conditions", Barcelona (20-23 September, 1993).

**080 Understanding Organization Factors Through Risk Models**

*Chair: J.H. Gittus, British Nuclear Industry Forum*

An Approach for Incorporation of Organizational Factors into Human Reliability Analysis  
in PRAs

*P. Moieni, D.D. Orvis (Accident Prevention Grp.)*

The Work Process Analysis Model (WPAM): An Integrated Approach to the  
Incorporation of Organizational Performance into Probabilistic Safety Methodology

*K. Davoudian, J-S. Wu, G. Apostolakis (UCLA)*

Risk Assessment - Including the "CHAOS" Factor

*C.T. Kleiner (C.T.K. Enterprises); R.L. Cummings (Interstate Assessment Tech.)*

## AN APPROACH FOR INCORPORATION OF ORGANIZATIONAL FACTORS INTO HUMAN RELIABILITY ANALYSIS IN PRAs<sup>1</sup>

Parviz Moieni and Douglas D.Orvis

Accident Prevention Group  
16980 Via Tazon, Ste. 110  
San Diego, CA 92127

### INTRODUCTION

A systematic approach is developed for incorporation of organizational factors into human reliability estimates to extend the applicability of probabilistic risk assessment (PRA) to safety culture improvement and integrated risk management<sup>1</sup>. The approach is based on use of decision trees, expert judgement, empirical data on human error (if available) and information collected on organizational factors (OFs) in the form of ratings. The proposed method also addresses the dependence between multiple operator actions in an accident scenario due to common organizationally grounded influence factors. This paper presents a methodology for incorporating the common influence of organizational factors into estimates of control room crew reliability in PRA.

### BACKGROUND

Studies of many large scale disasters such as Chernobyl, Challenger, Piper Alpha, Three Mile Island have shown that human error is a key cause of the accidents and, furthermore, organizational and management factors are a strong contributory cause of human errors. Currently, the U.S. Nuclear Regulatory Commission (NRC) and the nuclear industry are considering the potential benefits of increasing the uses of probabilistic risk assessment (PRA) and human reliability analysis (HRA) in risk-based consideration in regulation, inspection and decision making<sup>2</sup>. Recently, the NRC and other organizations have sponsored research in the area of identification, measurement, and assessment of influence of organizational factors on the safety of nuclear power plants (NPP) and other industries<sup>1,3,4</sup>. The NRC research included modeling of OFs in PRA<sup>1,3</sup>.

### APPROACH

In HRA technology, the relative probabilities of human errors among different situations or task contexts are scaled according to a number of performance shaping factors (PSFs). Traditional PSFs for control room crews include the quality of the man-machine interface (MMI) with respect to instruments and controls or the emergency operating procedures (EOPs), and training, in the context of a particular accident scenario.

A logical extension of the PSF concept is to include organizational influences in HRA models as higher-level influences that may concurrently affect several of the "traditional PSFs" as well as introduce other direct influences on personnel performance, such as changes in motivation or attitude. With empirically calibrated PSFs for OFs, the probability of an accident sequence for a given NPP as calculated for one organizational situation can thus be adjusted to account for improved or worsened situation at the same NPP, or for inferring the effects

---

<sup>1</sup> This paper is based on work supported by the U.S. Nuclear Regulatory Commission. Any opinions, findings, and conclusions or recommendations expressed here are those of the authors and do not necessarily reflect the views of the NRC.



of OFs on PRA of a different NPP. The approach consists of six steps.

#### Step I: Develop a Causal Model of the Control Room Crew Reliability

Figure 1 shows a simplified causal model of the control room operating crew reliability. The main three main categories of influence factors (IFs) for crew reliability are: 1) knowledge, skill and abilities (KSA), 2) tools and resources (TR), and 3) motivation and morale (MM). Each of these categories of IFs are mutually influenced to varying degrees by higher level organizational factors through plant departments and programs. KSA represents the background of the operating crews resulting from hiring practices, training program effectiveness, and crew experience. Tools and resources represent the quality of physical and organizational resources available to the crew and includes the quality of control room, quality of procedures and the engineering support of same, availability of other NPP personnel when needed. Motivation and morale represent the effects of organizational climate as they affect crew members likelihood to put KSA and TR to good and proper use.

The demonstration in Figure 1 uses the five groups of organizational factors comprised of 20 organizational dimensions developed by the collaborative efforts of four NRC contractors (BNL, PSU, UCLA and Accident Prevention Group)<sup>3,5</sup>.

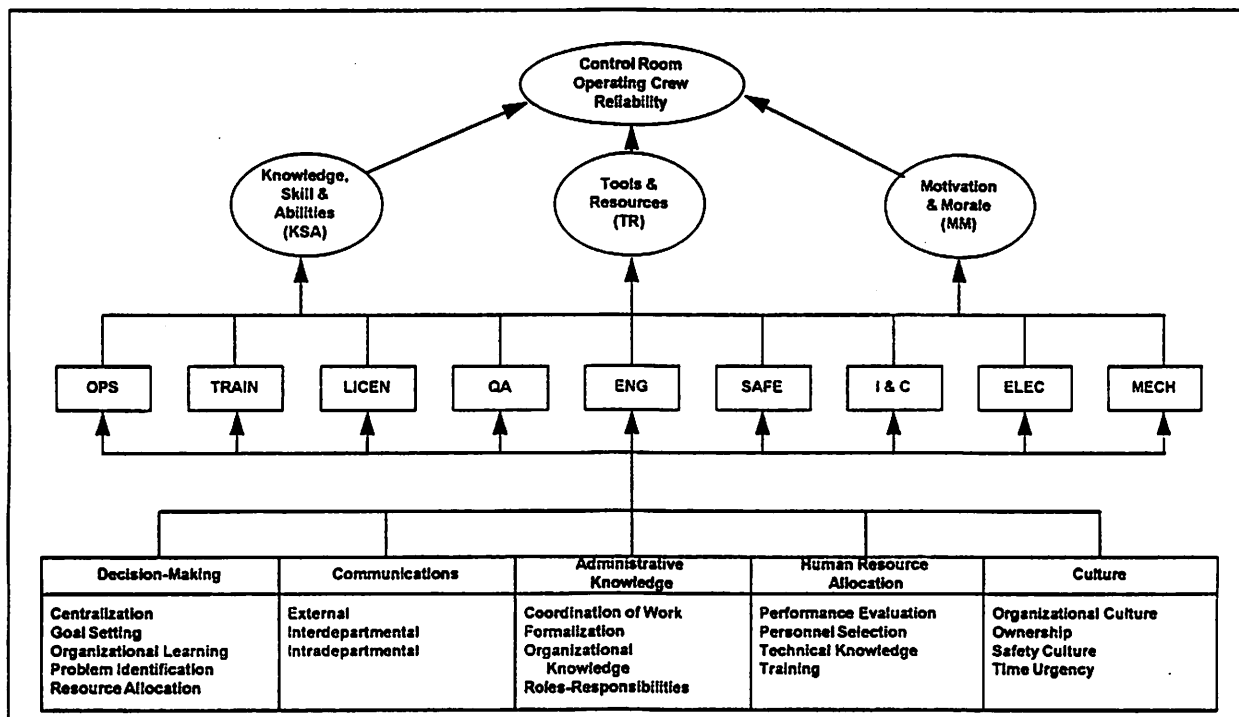


Figure 1. Influence of Organizational Factors Through Departments on Control Room Crew Reliability

#### Step II: Develop a Decision Tree For Control Room Crew Reliability

Figure 2 shows a decision tree for estimation of human error probability (HEP), using the three categories of influence factors, i.e., KSA, TR and MM. Decision tree provides a structured method to integrate the important influence factors that affect the likelihood of human errors and quantify their rates.<sup>1,6</sup> Preferably, empirical plant-specific and/or generic data would be used as anchor points in quantification to complement expert judgment.

In Figure 2, the degrees of influence for various IFs are shown by circled numbers. For example, the degree of influence of KSA on human error probability is assessed to be a factor of 10: the probability of failure of operators to perform the required action when their KSA level is judged to be "poor" is larger by a factor of 10 compared to the case where such factors are judged to be "good". It is noted that the "degree of influence" of a given IF may vary depending on the condition of other IFs. This is allowed to model potential interactions between various IFs. The "conditional error probabilities" derived in Figure 2 are calibrated with the anchor error probability according to the end point scales on the tree. The "conditional error probabilities" in Figure 2 are conditional on the state of the three IFs which derive from the ratings of the OFs for various NPP departments.

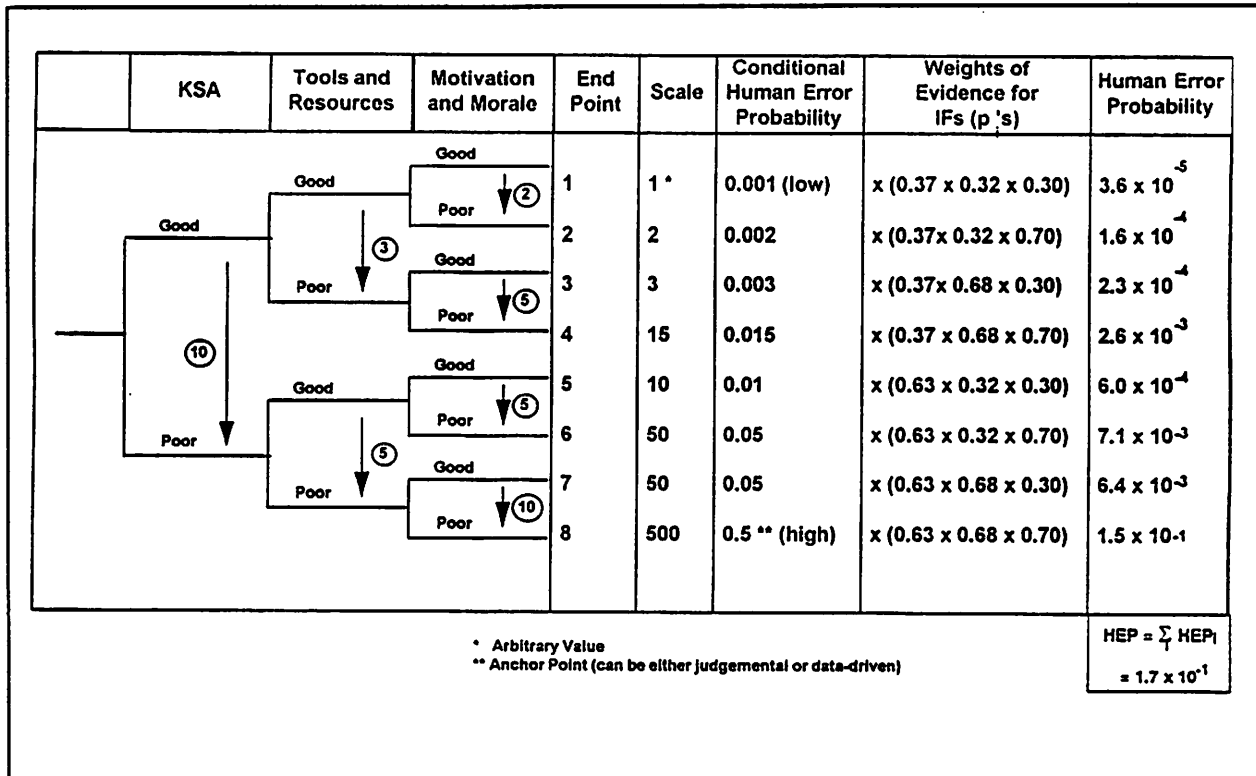


Figure 2. A Decision Tree to Estimate Human Error Probability

### Step III: Determine Ratings for Organizational Factors

Organizational factors are measured, or rated, using various "instruments"; for example, the Behaviorally Anchored Rating Scales (BARS) method<sup>7</sup>. Results of applying BARS and other instruments produce a set of OF ratings on a scale of 1 (lowest or worst score) to 7 (highest or best score) for the proposed 20 organizational dimensions for each NPP department which are aggregated to produce ratings for each of the five OFs. An example of applying such instruments is shown in Table 1 as developed by BNL/PSU for a representative nuclear power plant<sup>3</sup>. The bottom of each column (i.e.,  $R_j$  in Table 1) shows the overall (i.e., average) OF rating for each department.

### Step IV: Calculate Organizationally Grounded Ratings for IFs

Figure 1 diagrams potential causal links of organizational influences on crew reliability but the degree of influence varies among different departments. One may argue that the operations and training departments have the greatest influence on the operating crews' KSA compared to the other departments. Accordingly, the organizational ratings for departments are weighted for their

**Table 1. Organizational Factor Quantification with Respect to Departments for a Plant**

DEPARTMENTS FACTORS	OPS	TRAIN	LICEN	QA	ENG	SAFE	MAINTENANCE		
							I&C	ELEC	MEC H
1. Communication	3	3	2	2	4	3	3	2	2
2. Administrative Knowledge	2	4	4	4	3	3	3	2	2
3. Human Resources Administration	3	4	3	4	4	4	3	3	3
4. Culture	2	3	3	3	2	3	2	2	2
5. Decision Making	2	4	2	2	2	2	1	1	1
Overall Ratings ( $R_i$ )	2.4	3.6	2.8	3	3	3	2.4	2	2

NOTE: Scale = 1 through 7, with 7 being the highest (best) score and 1 being the lowest (worst) score.

degree of influence as follows:

$$R_i = \sum_j W_{ij} \times R_j \quad (1)$$

Where:

$R_j$  = Rating associated with j-th department considering all OFs

$W_{ij}$  = Weighting factor indicating degree of influence of j-th department on i-th human reliability influence factor;

$$0 \leq W_{ij} \leq 1 \text{ and } \sum_j W_{ij} = 1.0$$

$R_i$  = Rating associated with i-th human reliability influence factor (i.e., KSA, TR or MM)

**Table 2. Summary of Assigned Weighting Factors for Various Departments and Overall Ratings of Human Reliability Influence Factors**

WEIGHING FACTORS ( $W_{ij}$ )	OPS	TRAIN	LICEN	QA	ENG	SAFE	MAINTENANCE			$R_i^*$
							I&C	ELE C	MEC H	
KSA	0.3	0.6	0	0	0	0.1	0	0	0	3.2
Tools and Resources	0.1	0.1	0.1	0.1	0.4	0.1	0.1	0	0	2.9
Motivation and Morale	0.6	0.3	0	0	0	0.1	0	0	0	2.8

\* NOTE: Scale = 1 through 7, with 7 being the highest (best) score and 1 being the lowest (worst) score.

Table 2 demonstrates the assigned weighting factors and the calculated ratings for the three influence factors using Equation (1) where the weighting factors  $W_{ij}$  have been directly assigned judgementally. In situations where analysts do not feel comfortable in directly assigning the weighting factors, structured methods

such as Saaty's Analytic Hierarchy Process (AHP) can be used.

#### Step V: Assess Probabilities (or Weights of Evidence) for IFs

The objective of this step is to convert the ratings on human reliability influence factors (i.e.,  $R_i$ ) into probabilities or weights of evidence (i.e.,  $p_i$ ). A simple linear model is suggested here, i.e., as the organizational rating increases, the probability that the quality of a specific influence factor (such as operators' tools and resources) is good also increases. Mathematically:

$$p_i = a + b \times R_i \quad (2)$$

The two extreme ratings may be used to estimate the parameters of the calibration equation (i.e.,  $a$  and  $b$ ). Assuming:

$$\begin{cases} p_i = \text{Pr}(\text{Quality of } i\text{-th influence factor} = \text{good}) = 1 \text{ if } R_i = 7 \\ p_i = \text{Pr}(\text{Quality of } i\text{-th influence factor} = \text{good}) = 0 \text{ if } R_i = 1 \end{cases} \quad (3)$$

Using conditions (3) in equation (2) yields:

$$p_i = \text{Pr}(\text{Quality of } i\text{-th IF} = \text{good}) = -0.17 + 0.17 \times R_i \quad ; i = \text{KSA, TR, MM} \quad (4)$$

Table 3 summarizes the calculated estimates for  $p_i$  using  $R_i$  estimates calculated in Step IV (See Table 2).

Table 3. Summary of Weights of Evidence ( $p_i$ ) for the Three Human Reliability Influence Factors

Influence Factor	Rating ( $R_i$ )	Influence Factor Scale	$p_i = -0.17 + 0.17 \times R_i$
Knowledge, Skill and Abilities (KSA)	3.2	Good	$p_1 = 0.37$
		Poor	$\bar{p}_1 = 0.63$
Tools and Resources (TR)	2.9	Good	$p_2 = 0.32$
		Poor	$\bar{p}_2 = 0.68$
Motivation and Morale (MM)	2.8	Good	$p_3 = 0.30$
		Poor	$\bar{p}_3 = 0.70$

#### Step VI: Incorporate IFs' Weights of Evidence Into Decision Tree

The last step incorporates the information on quality of organizational factors, departments and crew related influence factors into the decision tree to produce unconditional human error probabilities. This step is performed by multiplying the conditional probabilities of the end points in the decision tree (Figure 2) by the joint probabilities of the three influence factors (i.e., the product of  $p_i$ 's) and adding them up. Figure 2 shows the results as "human error probability" or HEP. The estimated HEP is 0.17, based on the organizationally grounded ratings of 3.2, 2.9 and 2.8 (all below average for the example plant) for the influence factors KSA, TR and MM, respectively.

#### ORGANIZATIONALLY-INDUCED DEPENDENCE BETWEEN MULTIPLE OPERATOR ACTIONS

The dependence between multiple operator actions in an accident scenario due to common organizational influence factors may be addressed in the decision tree

framework. This type of dependence between PRA events, in general, has been identified by other researchers<sup>1,8</sup>. To demonstrate the method, consider an ATWS accident sequence with two operator actions (e.g., operator failure to manually scram the reactor when the RPS is failed (HEP<sub>1</sub>) and operator failure to manually initiate emergency boration (HEP<sub>2</sub>)). Steps I through V are carried out for each individual operator action using individual or the same decision tree as appropriate. In Step VI, however, the dependency between events is included in the joint human error probability for the two operator actions (HEP<sub>1,2</sub>) using Equation (5):

$$HEP_{1,2}(R_1, R_2, R_3) = \sum_{c=1}^8 (HEP_{1,c} | KSA, TR, MM) \times (HEP_{2,c} | KSA, TR, MM) \times P_{KSA}(R_1) \times P_{TR}(R_2) \times P_{MM}(R_3) \quad (5)$$

Where  $R_1$ ,  $R_2$ , and  $R_3$  represent the OF ratings associated with the three influence factors and  $(HEP_c | KSA, TR, MM)$  represent the human error probabilities conditional upon various states of the influence factors, as shown in the decision tree in Figure 2. Note that although both of the two operator actions are dependent on the same OFs, they are assumed to be conditionally independent in Equation (5). In other words, there is no direct dependence assumed between the two actions.

For illustration, we assume that results derived in Figure 2 apply to both operator actions and are used in Equation (5); the estimate for  $HEP_{1,2}$  ( $R_1 = 3.2$ ,  $R_2 = 2.9$ ,  $R_3 = 2.8$ ) is  $7.6 \times 10^{-2}$ . By contrast, if one treats the two human actions to be independent (even with consideration of OF influences), the joint HEP is  $HEP_{1,2}(\text{independent}) = HEP_1 \times HEP_2 = 0.17 \times 0.17 = 2.9 \times 10^{-2}$  which underestimates the joint HEP by a factor of about 2.5. The difference between the two treatments becomes more pronounced as the number of operator actions in the sequence of events increases.

#### Acknowledgments

The authors would like to thank their colleagues V.Joksimovich and A.J.Spurgin for their contributions, and acknowledge the support and guidance of the NRC project officers J.Kramer and C.Johnson.

#### REFERENCES

1. D.D. Orvis, P. Moieni, and V. Joksimovich, *Organizational and Management Influences on Safety of Nuclear Power Plants: Use of PRA Techniques in Quantitative and Qualitative Assessments*, Draft NUREG/CR-5752, USNRC (1993).
2. V.Joksimovich, "Where Do We Go From Here in U.S. Nuclear Safety Regulation?", Paper to be Presented at PSAM-II Conference, San Diego, CA (1994).
3. S. Haber and G.Apostolakis, *Review of Organizational Factors Research: Presentation to ACRS*, February 12, 1993, Washington, D.C., (1993).
4. L.J.Bellamy and T.A.W. Geyer, "Techniques for Assessing the Effectiveness of Management", *Proceedings of European Safety and Reliability Research Development Association (ESRRDA) Seminar on Human Factors*, Bournemouth, (1988).
5. R.Jacobs, et al., "Organizational Processes and Nuclear Power Plant Safety", *Proceedings of PSA'93, International Topical Meeting on Probabilistic Safety Assessment*, Clearwater Beach, FL, (1993).
6. P.Moieni, A.J. Spurgin and A. Singh, "Advances in Human Reliability Analysis Methodology - Part I: Frameworks, Models and Data", to appear in *Reliability Engineering and System Safety*, (1993).
7. F.G.Landy and J.L. Farr, *The Measurement of Work Performance*, Academic Press, Inc., New York, (1982).
8. J.S.Wu, G. Apostolakis and D. Okrent, "On the Inclusion of Organization and Management Factors Into Probabilistic Safety Assessments of Nuclear Power Plants", in *Probabilistic Safety Assessment and Management (PSAM)*, Ed. G. Apostolakis, Elsevier, NY, (1991).

## THE WORK PROCESS ANALYSIS MODEL (WPAM): AN INTEGRATED APPROACH TO THE INCORPORATION OF ORGANIZATIONAL PERFORMANCE INTO PROBABILISTIC SAFETY ASSESSMENT METHODOLOGY

Keyvan Davoudian, Jya-Syin Wu, and George Apostolakis\*

School of Engineering and Applied Science  
38-137 Engineering IV  
University of California  
Los Angeles, CA 90024-1597

Tel: (310) 825-1300  
Fax: (310) 206-2302

\*To whom correspondence should be addressed

### INTRODUCTION

Industrial experience and research findings have shown that major concerns regarding the safety of nuclear power plants (NPPs) and other complex industrial systems are not so much about the breakdown of hardware components or isolated operator errors as about the insidious and accumulated failures occurring within the organization and management domains<sup>1</sup>. The state of the art in current PSA methodology is such that *organizational dependencies* between hardware failures, between human errors, and between hardware failures and human errors are not modelled explicitly. Instead, the current methodology is confined mostly to models of isolated human errors and equipment failures<sup>2</sup>. Therefore, models must be developed that focus primarily on capturing the *common-cause* effect of organizational factors on parameters such as equipment failure rates. This, in effect, is analogous to the common-cause failure (CCF) analysis of hardware, where the "basic" failure probabilities are left alone and an additional term (containing the  $\beta$  factor, for example) is introduced to account for the failure of redundant equipment due to a single cause<sup>3</sup>. In capturing the common-cause effect of organizational factors on NPP safety, however, WPAM does more by going beyond conventional CCF analyses and considering organizational common-cause failures of not only similar, but also *dissimilar* systems and/or components. Also, as may be inferred from the common-cause-analysis nature of WPAM, the methodology goes beyond a mere recalculation of independent event-probabilities; it is the "common" effect that is of more interest in this analysis.

### AN OVERVIEW OF THE WORK PROCESS ANALYSIS MODEL (WPAM)

Figure 1 is an illustration of the WPAM philosophy; that is, it demonstrates the ways in which organizational factors are viewed to impact NPP safety. The top portion of the figure contains a simple example of an event tree for a typical accident sequence. As can be seen, the frequency of core damage

( $f_{CD}$ ) is a function of hardware failure rates ( $\lambda$ ), human error probabilities ( $\gamma$ ), etc. The bottom portion of the figure consists of two levels of organizational factors: The top level, represented by the overall culture and its constituents, and the second level, represented by factors contained under decision making, communications, administrative knowledge, and human resource allocation. The link between the top and bottom portions of Figure 1 is achieved by recognizing that any one or more of the organizational factors can influence the quality and efficiency of a given work process. This, in turn, will impact personnel and/or equipment performance, with the effect being manifested in parameters such as  $\lambda$  and  $\gamma$ .

## WORK PROCESSES AT NUCLEAR POWER PLANTS

As its name implies, the Work Process Analysis Model (WPAM) uses nuclear-power-plant work processes as its backbone. A careful examination of these processes shows that, for a given working unit, although the goal may be different from one job assignment to the next, the path to achieving that goal basically follows a standardized pattern. In other words, although each job assignment accomplishes a different goal, all job assignments follow a standardized flow path. For example, in the maintenance department, fixing a valve and fixing a pump are two different job assignments. However, they are both carried out by following the same sequence of steps, i.e., initiating a work request, having the work request reviewed, planning the work, etc.

Clearly, the execution of an assignment from beginning to end (e.g., from initiating a work request to documenting the work) involves a predictable flow path. The term "work process" is henceforth used in referring to this flow path (or process). Formally, a work process is defined as *a standardized sequence of tasks designed within the operational environment of an organization to achieve a specific goal*.

Using work processes, it is the goal of this analysis to identify all possible paths through which human errors due to organizational deficiencies can affect the PSA event tree (refer to Figure 1). In PSA, each basic event in each minimal cut set (MCS) is represented by one or more parameters. In the present study, the dependence that is introduced by organizational factors (OFs) is evaluated by recalculating basic-event probabilities while accounting for the dependencies among these parameters. As such, the parameters (i.e.,  $\lambda$ ,  $\gamma$ , etc.) take center stage in the procedure that has been devised to incorporate the impact of organizational factors into basic-event probabilities. In this procedure, the above-mentioned parameters are referred to as "candidate parameter groups" (CPGs), i.e., groups of parameters that are candidates for re-assessment with regard to the OFs.

The predictable nature of work processes suggests that a systematic analysis can be conducted to identify the desirable characteristics of a given process and to develop performance measures with respect to the strengths and weaknesses in the process. Furthermore, since work processes are closely related to plant performance, it is possible to conduct the analysis in such a way so as to facilitate the integration of organizational factors and PSA methodology. In order to address these issues, the Work Process Analysis Model has been divided into two parts. WPAM-I consists of a mostly qualitative analysis of a given work process, including an assessment of the importance of the role of organizational factors in the overall quality and efficiency of the work process. WPAM-II, on the other hand, consists of a quantitative analysis for each dominant accident sequence, whereby the effect of organizational factors on a work process, and thus, on the candidate parameter groups is measured and then incorporated into PSA results.

## WORK PROCESS ANALYSIS MODEL-I (WPAM-I)

For each work process, WPAM-I proceeds by asking the following basic question: How can the accumulation of organizational failures lead to an unsafe plant condition? In other words, how can unsafe attitudes or unsafe decisions made in the work processes defeat the defenses and barriers of the organization and be translated into noticeable unsafe events of either hardware failures or human errors? In answering these questions, WPAM-I utilizes a three-step procedure to systematically investigate each work process.

This three-step procedure is as follows (for more details, see ref. 1). First, a task analysis is conducted for each work process which focuses on understanding the tasks (e.g., planning, execution, etc.)

that are involved in the work process, the plant personnel involved in each, the actions involved in each task and their failure modes, and the defenses or barriers involved in each task and their failure modes. Second, for each key work process, an "organizational factors matrix" is defined which shows the organizational factors that might impact the safe performance of each task in the work process. This may be accomplished by collecting related procedures/documents on the work process of interest, by conducting interviews with plant personnel, and by collecting information on plant operating experience (e.g., through Licensee Event Reports). Finally, since each task in a given work process can be influenced by more than one organizational factor, it is deemed necessary (for the purposes of prioritizing investigative and/or corrective actions and for use in WPAM-II) to rank the pertinent factors according to their importance to (i.e., their level or degree of influence on) the tasks of the work process under analysis. This last step is accomplished through the use of the Analytic Hierarchy Process (AHP)<sup>4</sup>, a computer interactive tool that has been developed to aid in setting priorities.

The Work Process Analysis Model-I (WPAM-I) along with its products are used as inputs to the formalism of WPAM-II, which presents a mathematical algorithm for the quantification and incorporation of organizational factors into PSA. This is achieved as follows: Recognizing that, in PSA, each basic event in each minimal cut set (MCS) is represented by one or more CPGs, WPAM-II is used to recalculate basic-event probabilities in such a way that each new (organizationally dependent) probability accounts for (either explicitly and/or implicitly) the dependence among the CPGs. In other words, while WPAM-II recognizes that it is the CPGs that are dependent due to the influence of organizational factors, it calculates new probabilities for the events that are modelled by the CPGs as opposed to calculating a new value for each CPG.

## WORK PROCESS ANALYSIS MODEL-II (WPAM-II)

WPAM-II is composed of two basic steps: Minimal-cut-set screening and quantification (the details of these steps can be found in reference 5). The first step reduces the list of MCS for each dominant accident sequence by highlighting only those whose basic events show strong organizational dependence. Each minimal cut set normally contains two or more basic events. The screening process starts by defining a vector for each basic event. The purpose of this vector is to facilitate the assessment of the level of organizational dependence between two basic events. This is achieved by defining four members for each vector, and then rating each set of two basic events based on the commonalities that are introduced through the four vector members. Of course, one of the vector members is the parameter which represents the basic event. This vector is (WP, CPG, WU, ID) where WP: work process; CPG: candidate parameter group; WU: working unit/department; and ID: system/component identification.

Having this revised list, the quantification process then reassesses the MCS frequencies by first using WPAM-I to identify the organizational factors which may affect each candidate parameter group, and then deriving new frequencies for each minimal cut set through the use of an approach similar to that of SLIM<sup>6</sup>.

In general,

$$f_{MCS} = f_{IE} \cdot \prod_{i=1}^n p_i \quad (1)$$

where,

$f_{MCS}$	=	The core damage frequency contributed by a minimal cut set,
$f_{IE}$	=	The initiating event frequency,
$p_i$	=	The probabilities of basic events, allowing for the influence of organizational factors,
$n$	=	The number of basic events in a minimal cut set.



WPAM is focused on modifying MCS frequencies due to organizational dependencies between basic events and, as such, considers changes in absolute basic-event probabilities to be second order effects. This, in effect, means that the first basic event is left alone and SLIM is used to reconsider the conditional probability of the second event given that the first event has occurred, and so on. For example, for a MCS with two basic events,

$$f_{MCS} = f_{IE} \cdot p_1 \cdot p_{2|1} \quad (2)$$

where  $p_1$  and  $p_{2|1}$  are the probabilities of events that are modelled by candidate parameter groups.

In order to determine the value of  $p_{2|1}$ , SLIM proceeds by defining a Success Likelihood Index ( $SLI_{2|1}$ ) as:

$$SLI_{2|1} = \sum_j R_j \cdot W_j \quad (3)$$

where,

- $W_j$  = Normalized importance weight with respect to the  $j$ th dimension (or organizational factor),  
 $R_j$  = Rating of the  $j$ th dimension.

The weights  $W_j$  are obtained by asking experts to "rate" the pertinent organizational factors two at a time (i.e., perform a pairwise comparison) by using the Analytic Hierarchy Process (AHP)<sup>4</sup>. The ratings  $R_j$  are derived, on the other hand, by using measurement instruments such as Behaviorally Anchored Rating Scales (BARS), structured interviews, research surveys, and behavioral checklists<sup>7-10</sup> to rate the performance of a plant on each of the organizational factors that are deemed relevant to plant safety. Normally, a 5-point scale is used, where "1" represents the lowest (worst) score, and "5" represents the highest (best) score.

Each SLI will result in the probability of an event conditional upon the occurrence of its prior event(s). Considering the first two events of a MCS, a SLI will be calculated for the second event using the performance rating for the second event (i.e., no dependence is accounted for in the ratings). This leaves the weight to show the organizational dependence between the two events. In other words, in calculating the SLI for the second event, neither the weight for event #1 nor that for event #2 can be used independently. Instead, a combination of these weights has to be used which will bring out the dependence between the two events. In order to accomplish this task, WPAM-II uses the following expression for the effective weight,  $W_{2|1,j}$ :

$$W_{2|1,j} = \frac{W_{1j} \cdot W_{2j}}{\sum_j W_{1j} \cdot W_{2j}} \quad (4)$$

where the subscript "2|1,j" means "the weight for event #2 given event #1, with respect to the  $j$ th organizational factor."

Having determined  $SLI_{2|1}$ , the conditional probability of the second event,  $p_{2|1}$ , is calculated as:

$$\log ( p_{2|1} ) = a \cdot SLI_{2|1} + b \quad (5)$$

where "a" and "b" are calibration constants (or anchor points) and are determined by

$$\log ( p_2 ) = a \cdot (SLI_{2|1} = 5) + b \quad (6)$$

and

$$\log ( p_u ) = a \cdot (SLI_{211} = 1) + b \quad (7)$$

with

- $p_2$  = The lower anchor point, which is assumed to be equal to the organizationally independent probability of event 2, and
- $p_u$  = The upper anchor point.

Once the minimal-cut-set frequencies in all sequences have been modified, a new core damage frequency (CDF) must be calculated. Since the number of MCS in a typical PSA or IPE can run into the thousands, computational tools are needed for this recalculation. At present, only a preliminary computer code has been developed which does not allow a comprehensive recalculation of all the MCS frequencies and, thus, the CDF. For this reason, in a preliminary sample case, the frequency of only one (dominant) MCS has been recalculated.

The example which was used as the sample case was taken from an IPE and involved the analysis of a MCS contained in one of the station blackout dominant accident sequences leading to core damage. This sequence contains 150 MCS, with a (sequence) frequency of  $6.17 \times 10^{-7}$  per reactor year. For demonstration purposes, only this accident sequence was chosen and, for this sequence, only the top 25 and the bottom 25 MCS were retained for further analysis. Following the procedures detailed above and in references 1 and 5, the application of WPAM to this example showed that the CDF could increase from its initial value of  $1.9 \times 10^{-6}$  to a new value of  $4.2 \times 10^{-6}$  due to the influence of organizational factors.

## RISK MANAGEMENT

Sensitivity analyses were performed on the ratings in order to rank the organizational factors in terms of their effect on plant risk. Once this is done, the results can be used to guide the direction of organizational improvements and the allocation of resources.

The results of the sensitivity analysis are as follows. First, when all of the ratings are raised to a value of "3", the CDF is already reduced to its lowest value (i.e., the IPE CDF). Normally, this would be expected to occur when the ratings are all raised to "4" or "5" (for the case in which the anchor point for the IPE values is set at plant ratings corresponding to 5). However, it must be remembered that the estimates used in this analysis are very coarse. Second, improvements in formalization, training, and coordination of work seem to be the most advantageous in terms of risk reduction. On the other hand, not much would be gained from improvements in interdepartmental communication, for example. Finally, improving both formalization and training together would reduce plant risk significantly.

## SUMMARY AND DISCUSSION

The WPAM methodology is predicated on the observation that the day-to-day operation of nuclear power plants is, in general, governed by work processes. The research on work processes has shown that these processes standardize NPP operations while conforming to the defense-in-depth philosophy. Furthermore, the impact of organizational factors on NPP safety may be captured through the use of work processes (and the personnel, hardware, etc. involved in them) as a bridge between the organizational factors and PSA parameters. WPAM-I, the first part of WPAM, was introduced as the first step of this integration process.

The details of WPAM-II were discussed and, using WPAM-I and its products, the entire Work Process Analysis Model was applied to a sample case in order to both qualitatively describe and quantitatively determine the degree to which organizational factors act as common causes of hardware and/or human failures. Here, it was shown that, based on preliminary estimates, the common-cause effect of organizational factors on basic-event probabilities could cause the overall core damage frequency to double.

Sensitivity analyses were also performed for the ratings and the results were used to demonstrate their utility in the allocation of resources in risk management. For example, for this specific case, it was shown that a simultaneous improvement in both formalization and training would reduce plant risk significantly. On the other hand, improving inter- and intradepartmental communication together would have lower risk-reduction potential.

Several suggestions can be made for future research. First, no uncertainty analysis was performed in this study. It is expected that the uncertainty in the WPAM results will be large because the data for the analysis are largely obtained through expert judgment. Even though what has been proposed and demonstrated in the present study may be considered a good start, it is clear that the performance of an uncertainty analysis is essential to the furtherance of what has been accomplished so far. Second, computational tools are needed which can carry out the procedure in a more comprehensive manner. This, of course, goes hand in hand with the development of rigorous algorithms through which the impact of organizational factors on a single minimal cut set can be translated to the impact on the overall core damage frequency. Finally, an important task for the future involves the extension of this work to a broader range of work processes and even non-work-process related scenarios, i.e., Chernobyl-type accidents.

## REFERENCES

1. K. Davoudian, J. S. Wu, and G. Apostolakis, "Incorporating Organizational Factors into Risk Assessment Through the Analysis of Work Processes," *Reliability Engineering and System Safety*, (in Press).
2. "PRA Procedures Guide," NUREG/CR-2300, U.S. Nuclear Regulatory Commission, Washington, D.C., (1983).
3. A. Mosleh, "Common Cause Failures: An Analysis Methodology and Examples," *Reliability Engineering and System Safety*, 34, 249-292, (1991).
4. T. L. Saaty, *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*, McGraw-Hill International Book Co., New York, (1980).
5. K. Davoudian, J. S. Wu, and G. Apostolakis, "The Work Process Analysis Model (WPAM)," *Reliability Engineering and System Safety*, (in Press).
6. D. E. Embrey, P. C. Humphreys, E. A. Rosa, B. Kirwan, and K. Rea, "SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment," NUREG/CR-3518, U.S. Nuclear Regulatory Commission, Washington, D.C., (1984).
7. R. Jacobs, J. Mathieu, F. Landy, et al., "Organizational Processes and Nuclear Power Plant Safety," in *Proceedings of the Probabilistic Safety Assessment International Topical Meeting*, pp. 211-215, Clearwater Beach, FL, January 26 - 29, 1993.
8. R. Jacobs, J. Mathieu, F. Landy, et al., "Organizational Processes and Nuclear Power Plant Safety--Research Summary" in *Proceedings of the 1992 IEEE Fifth Conference on Human Factors and Power Plants*, pp. 394-398, Monterey, CA, June 7 - 11, 1992.
9. S. B. Haber, D. A. Shurberg, and M. T. Barriere, "Organizational Factors and Performance Reliability," in *Proceedings of the Probabilistic Safety Assessment International Topical Meeting*, pp. 216-219, Clearwater Beach, FL, January 26 - 29, 1993.

10. S. B. Haber, D. A. Shurberg, M. T. Barriere, and R. E. Hall, "The Nuclear Organization and Management Analysis Concept Methodology: Four Years Later," in *Proceedings of the 1992 IEEE Fifth Conference on Human Factors and Power Plants*, pp. 389-393, Monterey, CA., June 7 - 11, 1992.

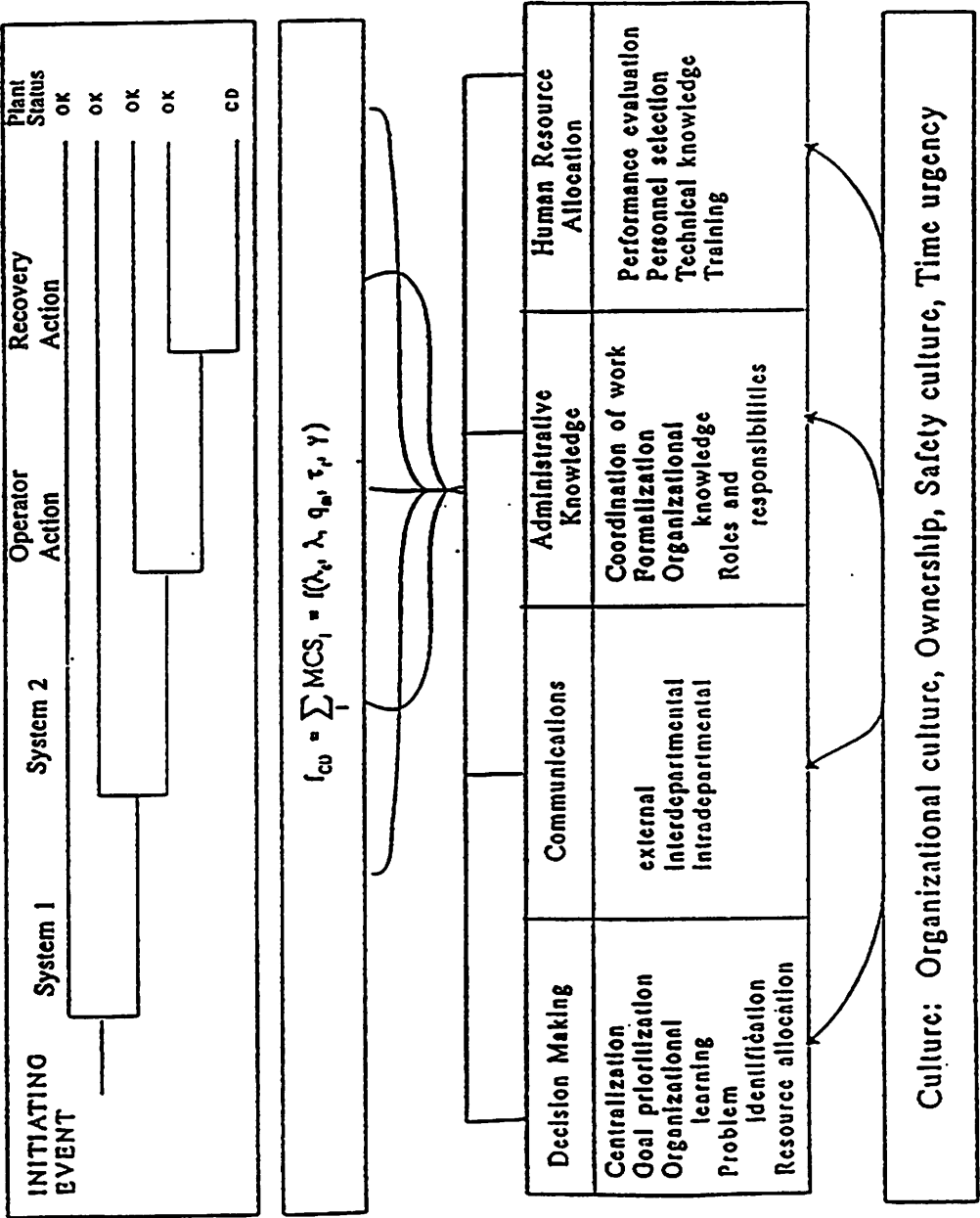


Figure 1. Incorporation of Organizational Impact into PSA

## RISK ASSESSMENT - INCLUDING THE "CHAOS" FACTOR

Charles T. Kleiner<sup>1</sup> and Ralph L. Cummings<sup>2</sup>

<sup>1</sup>C.T.K. Enterprises, Anaheim, CA 92807

<sup>2</sup>Interstate Assessment Technologies,  
San Diego, CA 92126-4431

### INTRODUCTION

There is no doubt that the number and types of risks being encountered by individuals, businesses, governments and the world in general are increasing at an alarming rate. It is also becoming evident that conventional methods for assessing risk and advising people relative to the impact may not be sufficient to avoid catastrophic consequences. This can result from: (1) not reviewing all of the possible choices before making a decision, (2) making the wrong decision or (3) making the right decision too late to change the outcome. This paper discusses CHAOS<sup>1</sup> as it can impact risk assessment. There have been many new concepts for analysing risk such as: Artificial Intelligence [Expert Systems], Fuzzy Logic, Neural Networks and Bayesian Theory<sup>2</sup>.

We propose a simple concept based on a "common sense" approach to risk assessment which avoids the need to calculate probabilities and various cost/avoidance tradeoffs in favor of a Risk Factor vs. Expected Time-of-Occurrence. This concept relies on certain terms that make up a system needed to understand and quantify the nature of the risk and the most controllable parameters. As such, the terms used in describing this method of risk assessment include: (1) Units having certain characteristics, (2) Objectives pertinent to the Units, (3) possible Choices that are available, (4) Decisions made based on the Choices, (5) Action taken by the unit based on the decisions (6) Results occurring due to the action and (7) the Evaluation (was the objective achieved?).

In the next section, we assemble these terms in a systematic way to show how various Units can be processed in a wide range of possible scenarios so that all available choices can be reviewed rapidly and a near-optimum decision can be made. The key element in this process is rapid selection, because certain events can unfold which are not instigated by the Unit in question but by some other independent Unit.

We also introduce CHAOS as an important aspect of risk assessment. The entire concept of risk assessment, including the CHAOS factor, is tied together with the DARTBORD computer software [DARTBORD is an eight character designation].

## DEFINITION OF TERMS

In the introduction, we discussed the items that form the basis for this risk assessment concept. We define the terms and how they are used. Figure 1 shows all of the terms and how they emanate from the UNIT.

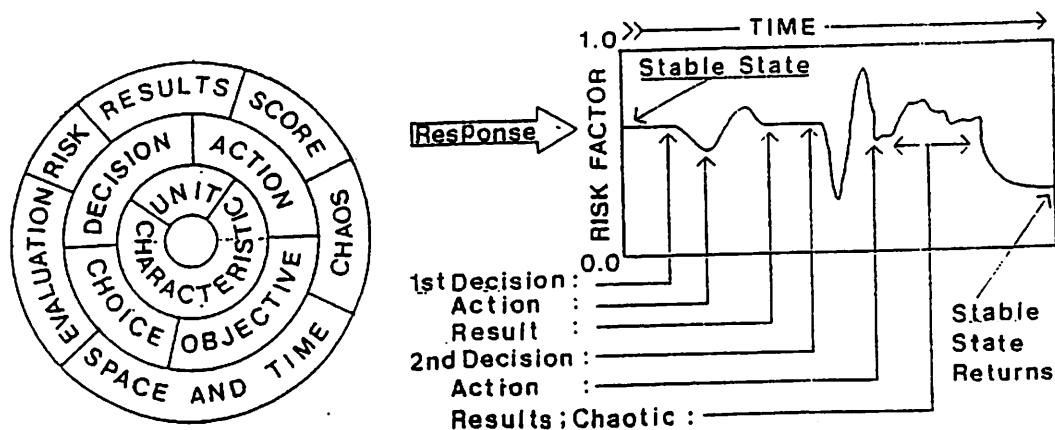


Figure 1. Risk assessment including the effects of CHAOS, is shown as a dartboard with units, objectives, choices, decisions, actions, results and evaluations.

Terms in Figure 1 are defined as follows:

### Unit

This is the prime subject, upon which, all of the terms operate in a direct manner. The UNIT may be inanimate [can't move or function] or animate [capable of moving, making choices, taking action, being acted on, and having various characteristics]. A ROCK would be considered inanimate and a living HUMAN would be considered animate. A ROCK could move or fall as a result of external force but would still be considered inanimate. A HUMAN may not be able to move or make too many choices if confined or impaired but would still be considered animate provided life is present. A ROBOT can be made of inanimate material but would have many (or more) of the characteristics of an animate UNIT. A UNIT can be a very simple system or it can be very complex and consist of many other UNITS operating in some environment. For example, a UNIT may be one Human or an aggregate of all Humans such as the Total Human Population at a given time. It is also necessary to define where this UNIT is located in space and time. In the case of the ROCK, it could have been located miles below the surface of the Earth millions of years ago but is now perched on the edge of some cliff ready to tumble down on a road, thus endangering a HUMAN driving a vehicle at a later time. UNITS, whether animate or inanimate, have characteristics and these characteristics can also change as a function of the UNITS' location in space and time. An individual, community, town, city, county, state, country and World Community can all be characterized as UNITS. Similarly, Power Sources, Agricultural entities, Corporations and other organizations can also be characterized as UNITS. It is clear that the combination of many types of UNITS with a wide set of characteristics can be subordinated/controlled by

other UNITS in a very complex way. This condition can rapidly expand as the complexity and mobility increase as is the present case today. The time available to examine possible Choices and then make an optimum DECISION can continue to decrease. As a result, the likelihood of making a good decision in time to avoid undesirable results also decreases.

### Objective

This is the perceived need of the UNIT. For an animate UNIT, the objective may include: (1) Survival, (2) Territory, (3) Possessions, etc. Over a period of time, the objective may change. Objectives can be defined in very specific ways and are the first steps in establishing the future course of events involving the UNIT and its environment.

### Choice

This is the possible options available to the UNIT when considering how to achieve the Objective. There are risks and opportunities posed by making certain Choices. This includes the introduction of a Risk Index and an Expected Time-of-Occurrence. These two quantities represent the primary concept presented in this paper and are discussed later.

### Decision

For a given Objective, a final Choice is selected which becomes the Decision to take Action. A Decision to take no action is still considered to be a Decision and is often the most frequent one selected [usually because the other Choices available to the UNIT were not preferred].

### Action

This implements the decision. Actions are influenced by the characteristics of the UNIT and its reaction with the environment existing during the time span of the Action. One simple example would involve a UNIT in search of FOOD and WATER. The UNIT's capability in walking and sensing the presence of this objective would be influenced by the terrain, weather and actual location of the Objective.

### Result

This is the outcome of the Action. The UNIT has either: (1) achieved the objective or (2) has fallen short of achieving the Objective. Full achievement would be rated as [1], partial achievement as [?] and total failure to achieve the Objective as [0]. This series of Results compared to the Objectives can be SCORED just as with a dartboard.

### Evaluation

This evaluates the results and establishes a SCORE which could be used by the same or other UNITS in achieving specific OBJECTIVES. This also includes an Evaluation of the Risk taken at each specific Space and Time.



This completes the serial activities shown in Figure 1. The next step involves methods for (1) making Choices and (2) using previous Evaluations to improve selection of the best Choice during the time-frame needed to achieve the Objective.

## LINEAR vs NON-LINEAR SYSTEMS

An important ingredient for making the best Decision from a group of Choices involves understanding how various possible Actions might turn out. Most decision-making processes rely on fairly simple linear behaviour. In practice, most systems display linear and non-linear behaviour. A Linear system is generally characterized by being: (1) repeatable, (2) predictable and (3) controllable. A Non-Linear system is often characterized by being: (1) nonperiodic, (2) erratic, (3) unpredictable and (4) uncontrollable. CHAOS can result when a controllable and understandable system response rapidly transforms to an uncontrollable behaviour. To understand Choices and then make the best possible decision, the UNIT must understand what kind of system behaviour is possible. The following descriptions define: (1) Linear system behaviour and (2) Non-Linear system behaviour.

### Linear Behaviour

This is an Action that could be repeated many times from the same location in space and time with identical results. In general, the result of a Choice and the same Action would produce the same RESULT. Because everything is well understood and predictable, the RESULT can be controlled.

### Non-linear Behaviour

In this case, given the same location in space and time, the same Action maybe not be repeatable, predictable or controllable. As a result, a Choice, subsequent Action and Result would not be the same no matter how many times it was repeated. Because everything is not understood and predictable, the Result can be uncontrolled. These definitions help describe the nature of CHAOS and its relation to risk.

## THE CONCEPT of CHAOS and ENTROPY

Chaos Theory is often related to Entropy. Many modern Physicists regard Entropy as an index of how far the passage from an ordered to a disordered state has progressed. It may also be noted, that Entropy is really a statement of what is most probable rather than what must be. With the immense number of molecules composing bodies large enough to be tested, the odds are overwhelmingly in favor of the passage of heat energy from faster to slower aggregation. As a result, the CHAOS or randomness of molecular motions is intensified; that is, the total entropy is increased. In order to apply this concept to Risk Assessment, it needs to be included in the Choice, Decision and Action components described in the previous sections. Figure 1 also illustrates how this is incorporated. In order to initialize the CHAOS factor, it is necessary to start with Steady-State in which there is no

CHAOS present. This may not be realistic, but it is the only way to provide a precise means for performing the analysis. The next step is to introduce possible disturbances to the system with the exact location and time yet to be determined. When and where the disturbances are entered will cause the "system" to respond differently. The response can be normal and controlled or it can become unstable. It will be assumed that instability is an undesireable reaction and therefore needs to be prevented. Also the onset of instability may not be evident in its early stages. There may be some random or statistical variations that exist as part of the Steady-State conditions that mask the early warning signals for instability. Because of the apparent link between CHAOS and ENTROPY, it is intuitively obvious that energy in some form must be introduced to maintain stability. If enough controlled energy is properly introduced to the system, then stability is maintained. The most important thing to remember is: That the energy required to maintain stability be introduced IN TIME to prevent instability. This can be difficult if the system is not well understood and the "background noise" masks the key parameters signalling the onset of instability. If instability is present but not immediately detected, then when the key parameters show variations or values that are interpreted as leading to instability, an onset of "panic" may begin. In general, we assume that the initial "panic" preceeds CHAOS. In fact the onset of "panic" will be defined as the "precursor" to CHAOS. It will also be assumed that the UNIT [regardless of size or complexity] will be biased toward stability and self-preservation and therefore, will want to prevent "panic" and avoid CHAOS. To do this, the UNIT has to: (1) recognize the onset of instability and (2) know what parameters will restore control. We now arrive at the need for a RISK FACTOR and an EXPECTED-TIME-OF-OCCURRENCE. These are easy to define:

#### RISK FACTOR

A Risk Factor of 1 means that there is a 100% certainty that "panic" and subsequent CHAOS will occur. A Risk Factor of 0 means that there is 100% certainty that "panic" and subsequent CHAOS will not occur. Therefore, the RISK FACTOR can only have a value between 0 and 1.

#### TIME OF OCCURRENCE

This is the time elapsed between the locations in space and time prior to the actual occurrence of "panic" and CHAOS. If there has been no analysis, sensing or mitigating action, then only some EVALUATOR will take data as the ACTION takes place. The exact date for the occurrence of a Richter 8+ on the San Andreas Faults is hard to predict but the maximum time of occurrence can be estimated at 30 years. In Figure 1 the TIME-OF-OCCURRENCE is measured from the time the initial Decision was made through the time Action took place and ends when the final Result is recorded. If the UNIT survives the Action and achieves the Objective in spite of Chaotic conditions, the Risk Factor may be less. Conversely, the Risk Factor may increase if the Objective is not reached.

## DARTBORD, A NEW TOOL FOR RISK ASSESSMENT

We have developed a new computer program [DARTBORD] that will run on the more advance PC's which implements the concepts shown in Figure 1. This software is still in the early development stage, but shows great promise for solving simple or complex Risk Assessment tasks. We currently use it to aid the assessment of Economic and Environmental clean-up tasks and other similar projects. The following applications illustrate how the program is used: (1) UNIT SEARCH FOR FOOD AND WATER: In this simple case, a primitive biped is faced with the need to find water and food (in this case a stream with fish). The biped is the UNIT and the OBJECTIVE is the stream containing food. The UNIT has certain characteristics (can walk at a certain speed, can live without food for one week but only three days without water and must rest or sleep six hours per day). The UNIT must make some DECISIONS from a set of CHOICES. The location of the OBJECTIVE is not known to the UNIT. DARTBORD solves this problem by using the characteristics of the UNIT and randomly places the OBJECTIVE at various near or far locations and SIMULATES the UNIT's search until an optimum strategy emerges. (2) POPULATION GROWTH: In this case, the UNIT is the entire human population at a given point in time on the land mass of the planet Earth. In this case, the OBJECTIVE is to predict the future population using constant population growth rates for the linear case and dependent population growth rates for the nonlinear case. And finally, (3) GLOBAL SECURITY- Nuclear Explosives/Reactors: In this instance, the UNIT is an advanced technology nation subject to potential Terrorist attack using some type of Nuclear Explosive Targeted at several unknown OBJECTIVES. DARTBORD simulates the effect of various preventative means needed to thwart such attacks using Attack/Defend OBJECTIVES.

### SUMMARY

This paper shows that the most important aspect in making a risk assessment is the selection of key parameters. Also, critical timing and a clear understanding of Choices are required before making a Decision to take Action. One of the most important concepts introduced by this paper is the need to take into account the possibility of CHAOS. In order to partially automate this risk assessment technique, we have developed a computer program called DARTBORD to assist in the performance of the analysis.

### REFERENCES

1. James Gleick, "CHAOS Making a New Science" Published by Viking Penguin Inc., 40 west 23rd Street, New York, New York 10010, U.S.A. (1988)
2. Martz, H. F. and Waller, R. A. "Bayesian Reliability Analysis" Published by John Wiley & Sons, New York, NY 10158 (1982)

## **081 DOE Safety Studies**

*Chair: R.E. Hall, BNL*

**An SAR Issue for the Savannah River Reactors Resolved with PRA Methods**  
*S.V. Topp (Westinghouse Savannah Rvr.)*

**Evaluation of Replacement Tritium Facility (RTF) Compliance with DOE Safety Goals  
Using Probabilistic Consequence Assessment Methodology (U)**  
*K.R. O'Kula, J.M. East, M.L. Moore (Westinghouse Savannah Rvr.)*

**Fault Tree Analysis on the F&H Canyon Exhaust Systems at the Savannah River Site**  
*J.M. Low, K. Marshall (Westinghouse Savannah Rvr.)*

## **AN SAR ISSUE FOR THE SAVANNAH RIVER REACTORS RESOLVED WITH PRA METHODS**

Stephen V. Topp

Westinghouse Savannah River Technology Center  
Aiken, South Carolina

### **INTRODUCTION**

A Level 1 Probabilistic Risk Assessment (PRA) was completed in July, 1990, and revised and updated in January, 1993, for the Department of Energy production reactors at the Savannah River Site in Aiken, S. C. The PRA has since been used several times to guide risk management decisions, as well as to quantify absolute risk and to help in understanding system interactions. This paper describes one of the risk management applications where PRA analysis determined that a reactor subcriticality issue being considered for inclusion in the Safety Analysis Report (SAR) is low enough in expected frequency that it can be excluded.

### **DISCUSSION**

Chapter 15.4.4.2 of the SAR, "Other Reactivity Additions During Shutdown", covers transients than might happen after about thirty seconds following nuclear shutdown. The following sequence of events was being considered for inclusion in that chapter:

- (1) Reactor scrams from any cause.
- (2) Reactor is restarted near the peak of the xenon transient (after about 3 hours and before about 24 hours).
- (3) A second scram occurs within the 21 hour window after critical when reactor is at power but before xenon burns out. This scram must be caused by primary cooling water motor trip from power loss.
- (4) A total of four or more rods from the control and/or safety complement fail to enter.
- (5) The operating crew fails to get all but three or fewer of the missing rods into the core within four hours.
- (6) There is a failure to restore power and start the large primary cooling water motors

within four hours.

- (7) If the large cooling water motors have been successfully started, then the operating crew fails to actuate the Supplementary Safety System (SSS). This system injects gadolinium nitrate into the moderator and would keep the reactor subcritical after xenon decay, even with some rods missing, but requires the large motors to ensure mixing.

The event tree given in Figure 1 shows this scenario schematically. The upper branch at each node represents the answer "yes" to the associated event. The origin of the initiator frequency and the conditional probabilities at each node are discussed briefly below.

Dependencies among the failure events was considered, and it was concluded that the electro-mechanical events are independent. Past experience with scrams has indicated no tendency for coupled scrams to occur, for example. The human errors in events 5 and 7 could be dependent, because the same crew could be involved in both actions. The failure probability for event 7 was taken to be fairly large to account for this dependency.

**Event 1--ANY SCRAM** This is the expected number of unscheduled scrams per year that would be followed closely by restart, derived using Savannah River experience over an 18 year period.

**Event 2--RESTART PEAK XENON** The conditional probability that, given a scram, the reactor would be restarted during the time that xenon would have built up enough to have the potential for a significant reactivity transient upon decay, estimated using experience with Savannah River administrative controls.

**Event 3--AREA POWER SCRAM** The conditional probability that the reactor scrams a second time, from loss of electric power, within the 21 hour window that xenon effects could be important relative to rod worth. Derived from Savannah River experience with loss of electric power.

**Event 4--FOUR RODS FAIL** This is dominated by a fault tree analysis of failure of rod reversal to respond to transients.

**Event 5--FAIL TO INSERT** The conditional probability that the operating crew will not insert the failed rods within four hours, derived using a THERP Human Reliability Analysis.

**Event 6--FAIL TO RESTORE** This is the probability that power will not be restored within four hours of the scram in Event 3, derived using Savannah River Experience.

**Event 7--SSS** The probability that the operating crew would fail to activate the gadolinium nitrate Supplementary Safety System, derived using a THERP Human Reliability Analysis.

The sum of sequence frequencies for failure is  $2.1 \text{ E-}10$ . The consequence of failure is a violation of Technical Specifications. For criticality to actually occur, this reactor charge would also have had to been created and operated at power with the margin of control far out of specifications--itself a low probability event.

The success criterion used at Savannah River for elimination of scenarios from detailed treatment in the SAR is an occurrence frequency of about  $\text{E-}06$  per reactor-year, depending upon judgments about the uncertainty in individual event frequencies that make up the total. The scenario described is far enough below this criterion and is made up of events characterized by some confidence in failure probabilities, so that it was dropped from further consideration for inclusion in the SAR.

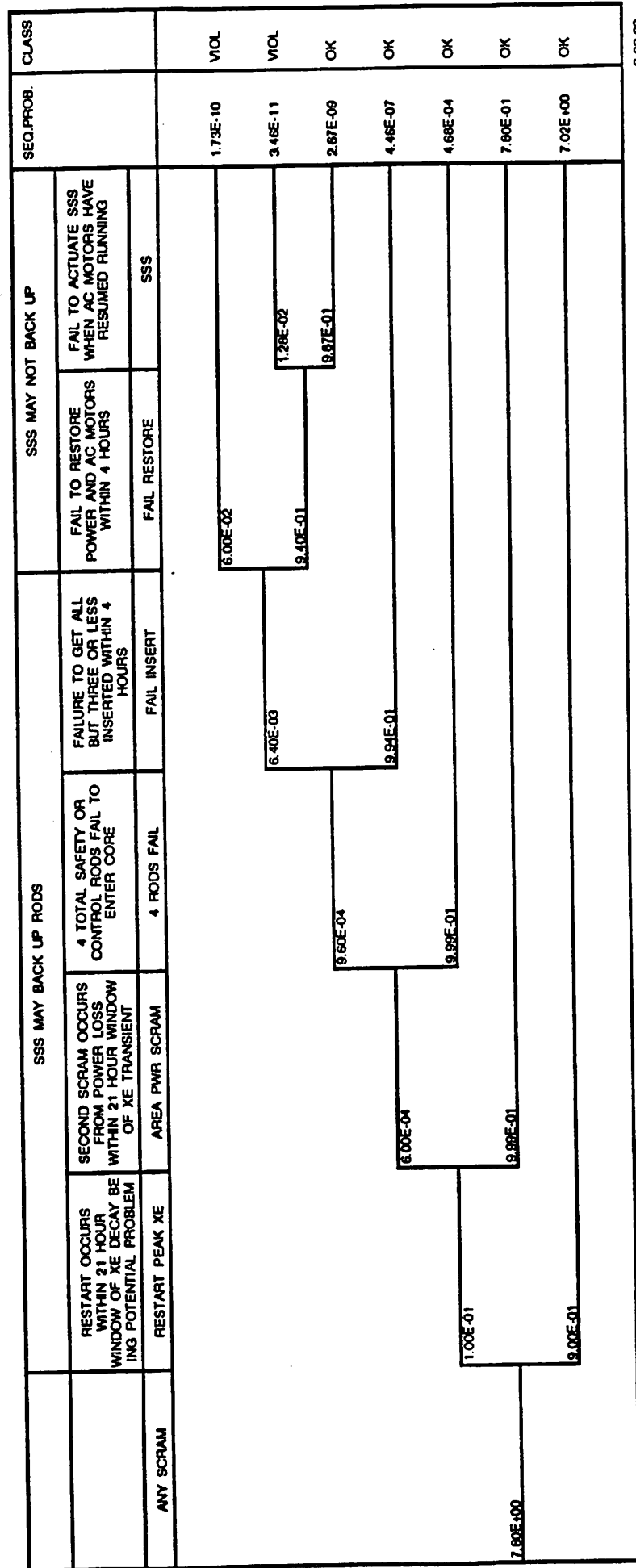


Figure 1. Event tree for Savannah River SAR issue.

# **EVALUATION OF REPLACEMENT TRITIUM FACILITY (RTF) COMPLIANCE WITH DOE SAFETY GOALS USING PROBABILISTIC CONSEQUENCE ASSESSMENT METHODOLOGY (U)**

Kevin R. O'Kula, Jacqueline M. East, and Marlene L. Moore

Process Safety Technology Section  
Savannah River Technology Center  
Westinghouse Savannah River Company  
1991 South Centennial Avenue  
Aiken, SC 29803-7657

## **INTRODUCTION**

The Savannah River Site (SRS), operated by the Westinghouse Savannah River Company (WSRC) for the U. S. Department of Energy (DOE), is a major center for the processing of nuclear materials for national defense, deep-space exploration, and medical treatment applications in the United States. As an integral part of the DOE's effort to modernize facilities, implement improved handling and processing technology, and reduce operational risk to the general public and onsite workers, tritium processing at SRS was moved from the Consolidated Tritium Facility to the Replacement Tritium Facility (RTF) in 1993.

To ensure that operation of new DOE facilities such as RTF present minimum involuntary and voluntary risks to the neighboring public and workers, indices of risk have been established to serve as target levels or safety goals of performance for assessing nuclear safety. These goals are discussed from a historical perspective in the initial part of this paper. Secondly, methodologies to quantify risk indices are briefly described. Lastly, accident, abnormal event, and normal operation source terms from RTF are evaluated for consequence assessment purposes relative to the safety targets.

## **RISK INDICES**

The U. S. Nuclear Regulatory Commission (NRC) adopted safety goals in 1986 to broadly define a tolerable level of radiological risk that is imposed on the public as a result of nuclear plant operation.<sup>1</sup> A basis for incremental risk goals indicates the individual mortality risk of prompt fatality in the United States is about  $5 \times 10^{-4}$  per year for all accidental causes of death.<sup>2</sup> If an increased incremental risk of 0.1% is tolerated, an increase in an average individual risk of accidental death by an increment of  $5 \times 10^{-7}$  per year results. The goal is applicable to the average individual residing within one mile of the plant site boundary.

Similarly, approximately nineteen persons per 10,000 population die annually in the United States as a result of cancer, or about  $2 \times 10^{-3}$  per year. Thus a delayed fatality risk safety goal of 0.1% would limit the increase to an individual's annual risk of cancer-related



death to an increment of no more than  $2 \times 10^{-6}$  per year. The goal is applied to the average individual residing within ten miles of the plant site boundary. In practice, comprehensive risk analyses such as probabilistic safety assessments (PSAs) are used to quantify risks for comparison to the goals.<sup>3</sup>

Current DOE facility safety guidance is based on Secretary of Energy Notice 35-91 (SEN-35-91), issued September 9, 1991.<sup>4</sup> The goals embody the same safety philosophy to limit the risks of fatality associated with DOE's nuclear operations as that endorsed by the NRC to limit risk for commercial reactor operation. The DOE Safety Goals are

**Acute:** The risk to an average individual in the vicinity of a DOE nuclear facility for prompt fatalities that might result from accidents should not exceed one-tenth of one percent (0.1%) of the sum of prompt fatalities resulting from other accidents to which members of the population are generally exposed. For evaluation purposes, individuals are assumed to be located within one mile of the site boundary. [ $5 \times 10^{-7}$  per year]

**Latent:** The risk to the population in the area of a DOE nuclear facility for cancer fatalities that might result from operations should not exceed one-tenth of one percent (0.1%) of the sum of all cancer fatality risks resulting from all other causes. For evaluation purposes, individuals are assumed to be located within ten miles of the site boundary. [ $2 \times 10^{-6}$  per year]

DOE personnel, managing and operating contractors, and subcontractor workers employed on a DOE reservation are typically assigned to a specific facility. A facility is defined as a building and related structures, their functional systems and equipment, and other fixed systems and equipment installed therein, under common process safety management.<sup>5</sup> Workers assigned to a facility, i.e., facility workers, are to be differentiated from co-located workers. The two groups of onsite workers are defined as follows:<sup>5</sup>

**Facility worker** - Any worker whose day-to-day activities are controlled by process safety management programs and a common emergency response plan associated with a facility or facility area.

**Co-located worker** - A worker in a fixed population outside the day-to-day process safety management controls of a given facility area. In practice, this fixed population is normally the workers at an independent facility area located some distance from the reference facility area.

A draft safety goal policy was developed for Department of Energy nuclear facilities in 1989 by the DOE Office of Environment, Safety, and Health (DOE/EH).<sup>6</sup> In this policy statement, onsite worker individual risk increments are 0.01 and 0.001 of the U.S. occupational fatality and general public cancer fatality rates, respectively. The quantitative goals of  $(.01) \times (1 \times 10^{-4}) = 1 \times 10^{-6}$  and  $(0.001) \times (2 \times 10^{-3}) = 2 \times 10^{-6}$  per facility-year of operation result, as limiting onsite worker risks due to acute and latent fatality, respectively. The acute guideline worker population refers to the zone from the facility boundary or access control perimeter (security fence) to one mile beyond. The latent guideline applies from the facility control perimeter for a distance of ten miles beyond.

## METHODOLOGIES FOR QUANTIFYING RISKS

Two methodologies are used in this study for individual risk evaluation and for SEN-35-91 and DOE/EH compliance determination. A brief description follows.

Consequence assessment to estimate individual risk from facility operation for comparison against DOE safety goals is performed with software developed to support PSAs. The primary tool for this purpose is the MACCS code.<sup>7-9</sup> Parallel effort has been expended to develop assessment capability for accidental radioactive releases from fusion reactors, resulting in FUSCRAC3.<sup>10,11</sup>

Both MACCS and FUSCRAC3 allow probabilistic sampling of site-characteristic meteorology, calculation of airborne plume transport and deposition, organ dose incurred via short-term (acute) and long-term (chronic) pathways, and assessment of health effects. Acute dose conversion data have been implemented in MACCS for inhalation and skin absorption of tritium and for long-term uptake of tritium-contaminated water. FUSCRAC3 also accounts for long-term population dose from incorporation of tritium in the food chain through plant and meat ingestion. In FUSCRAC3, it is assumed that tritium is in equilibrium with non-radioactive isotopes of hydrogen.<sup>12</sup>

Both codes predict acute and latent fatality consequences in a conditional complementary cumulative distribution function (CCDF) format, or, the probability that a certain level of consequence will be equaled or exceeded for the postulated source term. Variability in the level of consequence stems from the relative likelihood of meteorological conditions in the

area of the nuclear facility. The overall facility CCDF for a measure of consequence is formed by weighting conditional CCDFs from a set of source terms by the respective set of source term frequencies and summing in an appropriate manner.

Population bases for the RTF safety goal compliance are input to these codes in a polar coordinate system for the prompt and latent individual risk goals, respectively. The offsite prompt risk area extends from the SRS boundary to one mile away in each of sixteen compass sectors, while the latent risk area extends from the site boundary to ten miles away in each direction. The RTF facility is the coordinate system origin, and average public vehicular traffic is included.

Onsite prompt risk area extends from the RTF inner control perimeter boundary to one mile away in each of sixteen compass sectors, while the latent risk area extends from the inner control perimeter to ten miles away in each direction. No credit is taken for evacuation or sheltering in the baseline calculations.

### RTF Source Terms and Dose Pathway Assumptions

For the determination of individual prompt and latent fatality risks, source terms were developed from postulated beyond-design basis, design basis, and abnormal events, as well as for normal operation. Beyond-design basis events consider multiple failures and are developed from standard fault/event tree logic models. Design basis event, abnormal event, and normal operation source terms and their respective frequencies are based on the Safety Analysis Report governing RTF operation.

Tritium initially released from RTF in postulated accident conditions will be a mix of tritiated oxide ( $T_2O$ , HTO) and elemental tritium (HT,  $T_2$ ). In the plume passage phase of a given release, the dose to receptors is based on the tritium oxide component alone. The elemental component is ignored because of toxicity differences (Ref. DOE 5400.5, *Radiation Protection of the Public and the Environment*). However, ex-plant environmental conditions over long periods of time may convert the released elemental tritium to the tritium oxide form. In this analysis, results are based on the tritium oxide specified in the source term alone.

Health effects models are incorporated in both MACCS and FUSCRAC3 computer codes to interpret the dose accumulated in the early- and long-term phases after an hypothetical facility accident. The models account for dose rate effects, an important consideration for realistic prediction of adverse consequences expected in the emergency and long-term phases following a radioactive release. Two time frames are used: acute - start of release to seven days after, and chronic - seven days to five years afterward in the MACCS calculations, and seven days to fifty years afterward in the FUSCRAC3 calculations. Both codes use fifty-year dose conversion factors in the chronic phase portion of the modeling.

The offsite general public risk calculations include acute (inhalation and skin absorption uptake) and long-term, or chronic uptake (inhalation, skin absorption, food ingestion and water consumption). Inhalation of resuspended tritium and the ingestion of contaminated water is included. An early dose period assesses early exposure, calculating a fifty-year dose commitment from inhalation during plume passage. Ingestion dose during the chronic period is a fifty-year dose commitment from ingestion of contaminated food for fifty years subsequent to the accident. Offsite calculations are performed with MACCS and FUSCRAC3 for each source term, frequency-weighted and summed at the mean consequence level.

Onsite worker risk determination includes the acute period (plume passage) only, and is calculated with MACCS. Inhalation and skin absorption pathways are included, and seven-day acute inhalation dose conversion factors are used. MACCS calculates latent fatality cases from direct exposure (direct inhalation and resuspension inhalation) to the resident population in the ten-mile zone surrounding the SRS boundary. A risk factor of 8% latent fatality per person-sievert of effective dose equivalent, or EDE ( $8 \times 10^{-4}$  per person-rem) is applied.<sup>13</sup>

The component of latent fatality from long-term ingestion of contaminated food is determined with the FUSCRAC3 code. The food-chain model accounts for transport of tritium oxide away from the nuclear facility, incorporation of the tritium into soil and foodstuffs, and subsequent uptake by animals and humans. The food-related dose is incurred over fifty years and is reported as whole-body population dose. A dose reduction factor of two is applied to modify the acute dose rate effect for long-term, chronic calculations.<sup>13</sup>

## RESULTS

The individual prompt fatality risk within one mile of the site boundary is zero for all accident scenarios, at all levels of consequence. It is determined that the amount of tritium oxide released must be about  $1.9 \times 10^9$  Ci, or an amount significantly larger than that released in the largest source term.

The individual latent fatality risk within ten miles of the site boundary was evaluated as  $8.7 \times 10^{-10}$  per individual per facility-year, or more than three orders of magnitude below the safety goal of  $2 \times 10^{-6}$  per facility-year when postulated accident conditions and normal operation releases are frequency-weighted and summed. Table 1 lists the components to individual risk for RTF operation, indicating normal operation contributes nearly 80% of the individual risk. The contributing CCDFs and the total summed CCDF are shown in Figure 1. The risk estimates for the offsite general public could be reduced with prudent countermeasures, specifically evacuation or sheltering measures during plume passage and interdiction of foodstuffs to minimize tritium uptake through ingestion pathways in the long-term phase.

Environmental conditions will eventually convert most of the elemental tritium released to tritium oxide. A sensitivity study was performed to evaluate overall individual risk assuming normal, beyond-DBE, and DBE releases are converted to tritium oxide before human uptake. In this case, the overall risk increased from  $8.7 \times 10^{-10}$  to  $4.1 \times 10^{-8}$ .

### Individual Risks to Onsite Workers

The individual prompt fatality risk within one mile of the RTF facility is zero for all scenarios, at the mean level of consequence. A "threshold" level of tritium,  $1.5 \times 10^8$  Ci, is not available in any of the RTF source terms that would lead to acute fatalities at a 0.5 mile source-to-receptor distance.

The individual latent fatality risk within ten miles of RTF is  $3.0 \times 10^{-10}$  per individual per facility-year, almost four orders of magnitude below the safety goal of  $2 \times 10^{-6}$  per facility-year. Components to the overall risk are listed in Table 1. It is observed that normal operation contributes about 63% of the individual risk. Figure 2 represents the component CCDFs and the total CCDF for the onsite co-located workers. Onsite co-located risk is lower relative to the safety goal than the offsite general public, principally due to food ingestion of tritium being considered for offsite populations but not for onsite workers.

**Table 1. Individual Risks (per facility-year) from RTF Operation.**

	Offsite (w/o evacuation)	Onsite (w/o evacuation)	Co-Located (w/ evacuation)	Facility Worker (w/ evacuation)
<b>Individual Latent Fatality Risk</b>				
Beyond Design Basis	1.08E-10	7.78E-11	2.44E-11	1.15E-8
Design Basis Events	6.30E-11	3.41E-11	1.09E-11	1.70E-9
Abnormal Events	3.79E-12	2.04E-11	6.58E-13	1.01E-10
Normal Operation	6.99E-10	1.90E-10	—	—
Total	8.74E-10	3.04E-10	3.60E-11	1.33E-8
Goal	2.00E-6	2.00E-6	2.00E-6	
<b>Individual Acute Fatality Risk</b>				
Total	0	0	0	4.06E-10

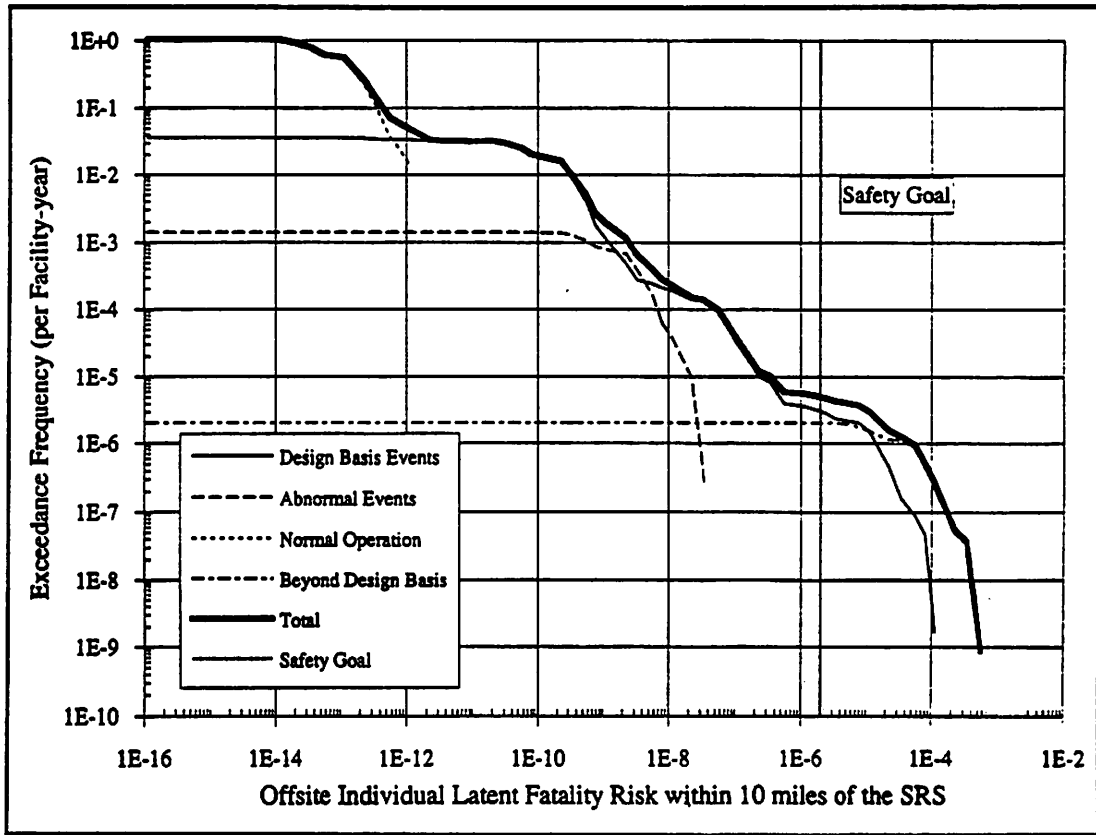


Figure 1. CCDFs for Individual Risk to General Public

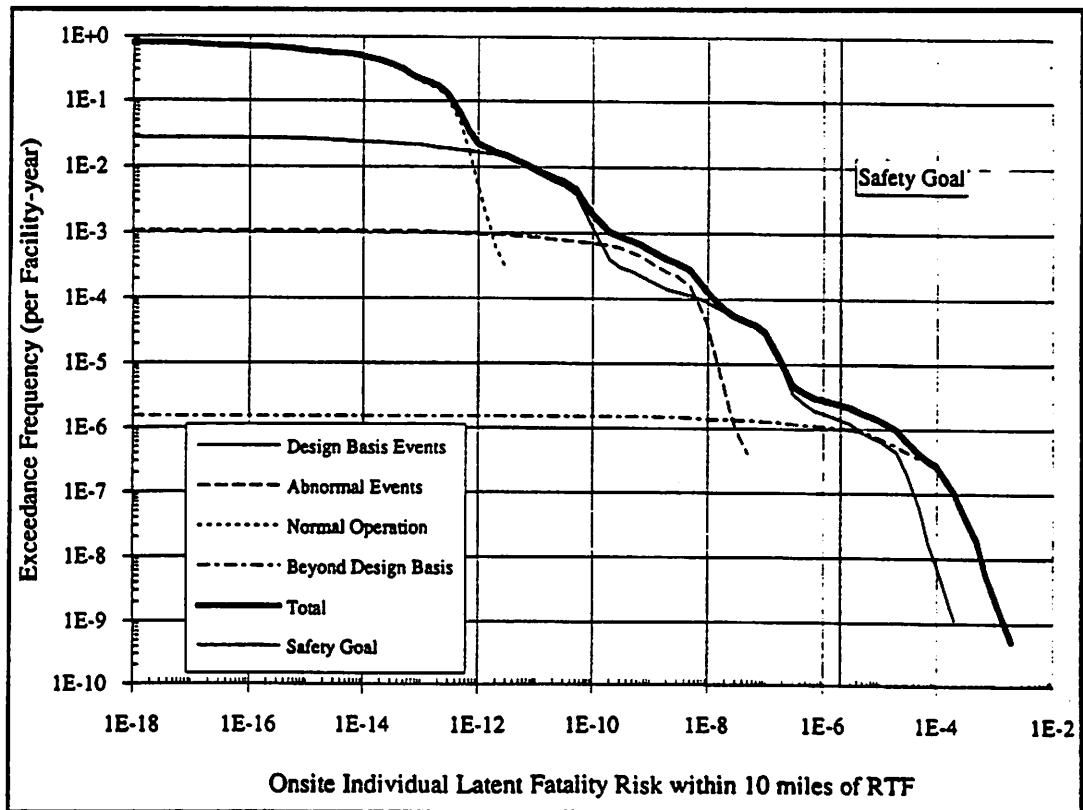


Figure 2. CCDFs for Individual Risk to Onsite Co-located Workers

The individual worker risk analysis, as described earlier, accounts for the effects of the initial plume passage alone. Long-term effects arising from incorporation of tritium into the environment are not included. It is less likely that released elemental tritium will be converted to the oxide form during the plume passage phase of the release to effect onsite populations.

Baseline co-located worker risk calculations above were made without crediting emergency management programs. A sensitivity study was conducted, implementing a limited evacuation model. Workers evacuate at 3.8 m/s starting at 0.5 hour after the beginning of the release. During the waiting period, workers are engaged in normal activity. Evacuees are subject to the effects of the plume passage until they reach a distance of five miles from RTF. Table 1 results suggest evacuation is effective in reducing onsite latent fatality risk.

A final assessment was performed, modeling evacuation of the RTF work force. In this case, the RTF personnel are stationary for one hour, at the primary rally point. The personnel are considered to be standing outside with no protection from the passing plume. Once the hour has expired, these personnel travel to the SRS boundary at 0.9 m/s. Table 1 lists the results for the RTF facility workers. The acute risk is far below the most limiting of the quantitative goals ( $5 \times 10^{-7}$ ). The latent risk estimate is a factor of 150 below the safety guideline value of  $2 \times 10^{-6}$  individual fatality per facility-year.

FUSCRAC3 and MACCS are probabilistic consequence models, implying a given calculation implicitly contains many model, data, and parameter uncertainties. Hamby has evaluated parameter and model uncertainty recently with respect to atmospheric release of tritium oxide.<sup>14</sup> A factor of four was observed from median to 95th percentile values. It is estimated the current estimates have an order of magnitude of uncertainty.

Current probabilistic consequence analysis of postulated accidents involving tritium at Savannah River are now being revised with the Karlsruhe code, UFOTRI.<sup>15</sup> This code offers more realistic modeling options and can assess elemental and oxide releases.

## SUMMARY

Operational risk of the Replacement Tritium Facility (RTF) at the Savannah River Site due to normal operation and from a spectrum of postulated accident conditions was quantified for comparison against acute and latent fatality safety guidelines for the general public and onsite workers. The SEN-35-91 safety goal value of  $2 \times 10^{-6}$  per individual per year is met by more than three orders of magnitude. Ingestion of contaminated foodstuffs dominates the chronic dose incurred by the general public, and in general, this effect causes general public risk to be larger than that of co-located workers. However, interdiction would greatly reduce the overall societal impacts estimated in this study.

The individual risks for co-located workers within ten miles of RTF is smaller by nearly four orders of magnitude than a draft DOE goal of  $2 \times 10^{-6}$  per individual per year. Evacuation and sheltering countermeasures would be effective in reducing these very small risks. This analysis concludes that RTF risks posed are well within quantitative guidelines established by the Department of Energy for increased incremental risk.

## ACKNOWLEDGMENT

This report was prepared in connection with work done under Contract No. DE-AC09-89SR18035 with the U. S. Department of Energy.

## REFERENCES

1. "Safety Goals for the Operation of Nuclear Power Plants," Policy Statement, Federal Register, Vol. 51, No. 149, August 4, 1986, pp. 28044-28049.
2. "Safety Goals for Nuclear Power Plant Operation," U. S. Nuclear Regulatory Commission Report NUREG-0880, Rev. 1 (For Comment), May 1983.
3. "Reactor Risk Reference Document," U.S. Nuclear Regulatory Commission, Washington, D. C. NUREG-1150 (1991).
4. Secretary of Energy Notice SEN-35-91, "Nuclear Safety Policy," U. S. Department of Energy (September 9, 1991).

5. DOE Office of Defense Programs (DOE/DP) Draft Standard DOE-DP-STD-3005-93, *Definition and Criteria For Accident Analysis* (1993).
6. U. S. Department of Energy Office of Environment, Safety, and Health "DOE Nuclear Safety Policy," Draft DOE Notice 5480.PP (May, 1989) .
7. D. I. Chanin, J. L. Sprung, L. T. Ritchie, and H-N Jow. "MELCOR Accident Consequence Code System (MACCS), Volume 1. User's Guide." NUREG/CR-4691, SAND86-1562, Sandia National Laboratory, Albuquerque, NM 87185 (February 1990).
8. H-N Jow, J. L. Sprung, J. A. Rollistin, L. T. Ritchie, and D. I. Chanin. "MELCOR Accident Consequence Code System (MACCS), Volume 2. Model Description." NUREG/CR-4691, SAND86-1562, Sandia National Laboratory, Albuquerque, NM 87185 (February 1990).
9. J. A. Rollistin, D. I. Chanin, and H-N Jow. "MELCOR Accident Consequence Code System (MACCS), Volume 3. Programmer's Reference Manual." NUREG/CR-4691, SAND86-1562, Sandia National Laboratory, Albuquerque, NM 87185 (February 1990).
10. S. J. Brereton and S. J. Piet, "Modifications to FUSCRAC2 In Creating FUSCRAC3," Idaho National Engineering Laboratory, SJB-33-88 (December 16, 1988).
11. S. J. Brereton et al., "Offsite Dose Calculations For Hypothetical Fusion Facility," IAEA Workshop on Fusion Reactor Safety, Jackson, WY (April, 1989).
12. S. J. Piet, V. J. Gilberti and M. S. Kazimi, "FUSECRAC: Modifications of CRAC for Fusion Application," M.I.T. Plasma Fusion Center, PFC/RR-82-20 (DOE UC-20 C, D, E) (June 1982).
13. National Research Council, Committee on the Biological Effects of Ionizing Radiation. 1990. Health Effects of Exposure to Low Levels of Ionizing Radiation (BEIR V). Washington D. C. National Academy of Sciences, National Academy Press (421 pp.).
14. D. M. Hamby, A Probabilistic Estimation of Atmospheric Tritium Dose, *Health Phys.* 65:33 (1993).
15. W. Raskob, "UFOTRI: Program for Assessing the Offsite Consequences from Accidental Tritium Releases," KfK-4605, Kernforschungszentrum Karlsruhe (1990).

## **FAULT TREE ANALYSIS ON THE F&H CANYON EXHAUST SYSTEMS AT THE SAVANNAH RIVER SITE**

**J. Mike Low and Kathryn Marshall**

Regulatory Programs  
Nuclear Materials Processing Division  
Westinghouse Savannah River Company  
Aiken, SC 29808

### **INTRODUCTION**

The Canyon Exhaust System (CES) for the F&H Canyon Chemical Separations Facilities are considered safety class items (SCIs). SCIs are defined in DOE Order 6430.1A as systems, components, and structures, including portions of process systems, whose failure could adversely affect the environment or safety and health of the public. As such, any modification to SCIs must be carefully reviewed for impact to safety. During the last year, the Savannah River Technology Center of WSRC has been requested to perform two major evaluations on the Canyon Exhaust Systems. These evaluations include 1) an Upgrade to Canyon Exhaust System (UCES) Project for both F&H Areas and 2) a Backfit Analysis for a standby diesel generator in F-Area. The purpose of the first evaluation was to evaluate the impact of cost reduction options on the UCES reliability. The purpose of the second analysis was to provide justification for not upgrading an existing standby diesel generator to meet current safety class standards.

### **DISCUSSION**

#### **Existing System Description**

In each canyon exhaust system, exhaust air leaves the canyon through an underground tunnel. This tunnel leads to an underground sand filter. The exhaust air is pulled through the sand filter by four fans in both Buildings 292- F&H. Three of these units are normally in operation and the remaining unit is in stand-by. The stand-by unit comes on if the vacuum in the exhaust tunnel drops below a preset level. The filtered exhaust air is then discharged to either the Building 291- F or 291-H exhaust stack. Normal power for fans 2 and 3 is provided to the Savannah River Site by South Carolina Electric and Gas. Normal power for fans 1 and 4 is provided by dedicated diesel generators. Standby power is provided to fans 2 and 3 from a 600 kW diesel generator in Building 292- F&H. Figure 1 provides a schematic of the existing exhaust system.

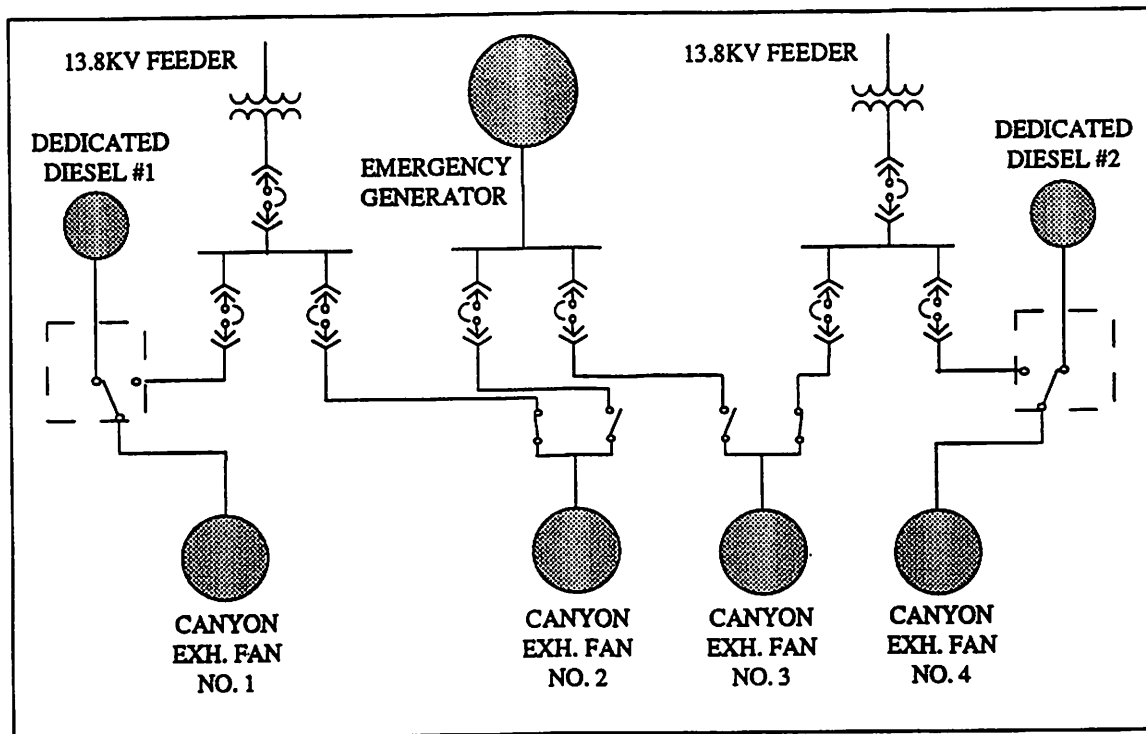


Figure 1. Schematic of the existing canyon exhaust system. Fans 1 and 4 are normally powered by dedicated diesels, and fans 2 and 3 are run on utility power. Emergency power is supplied by the emergency generator.

### Fault Tree Modeling

This work was performed using fault tree analysis techniques and the Computer Aided Fault Tree Analysis (CAFTA) Program. Fault tree analysis provides a structured method for evaluation of failure modes and sequences in a system, through the use of a logic model describing system operation. System failure modes are identified by a deductive reasoning process. This process uses process and operations information to formulate possible failure scenarios leading to the occurrence of an undesired event, called the top event in the fault tree. Credible failure modes are logically incorporated into the fault tree for qualitative and quantitative evaluation. System failure requires the occurrence of initiating and enabling events, and these constitute the basic elements of the fault tree model. An initiating event must occur in order to begin the failure sequence. Enabling events are those which allow the failure sequence to continue to the top event.

For these analyses, some of the operating systems, such as fans 1, 2, and 4, are considered operating redundant systems. These systems are treated as initiator/enablers because any individual fan failure can initiate or enable the top event. For example, one scenario could be failure of fan 1 with fans 2, 3, and 4 in their failed state. A similar scenario could be failure of fan 2 with fans 1, 3, and 4 in their failed state. The CAFTA cutset editor, "CSRAM", allows the fans to be treated as initiator/enablers and adequately quantifies these scenarios.

The fault tree logic for this work was developed by reviewing existing fault tree models (Durant and Perkins, 1983). The existing fault tree was revised to reflect current system design and to include additional design details. The top event for the analysis was identified as "Exhaust System Failure". Exhaust system failure was defined as the failure or loss of all four exhaust fans. Initiating events for the fault tree included 1) stack collapse by earthquake, 2) stack collapse by tornado, 3) exhaust tunnel collapse, and 4) mechanical or electrical failures that cause an operating fan to fail. The first three initiating events listed are considered to be single event failure modes, i.e. the occurrence of any one of these events could cause failure of the entire exhaust system. The fourth set of initiating events includes loss of utility power, loss of a transformer, tie-breaker fails to open, fan bearing failure, etc.

Enabling events for the fault tree include those basic events that would cause a second, third, and fourth fan to be in a failed state. These events are similar to the fourth



set of initiating events. The difference is that initiating events are reported in terms of frequency (rate of failure) and enabling events are reported in terms of probability (unavailability, unreliability, and/or undependability). Therefore, enabling events report the probability that a fan will be in a failed state (having already failed to start or failed to continue running).

### Case 1 - Upgrade to the Canyon Exhaust System (UCES)

The canyon exhaust systems in both F&H Areas are over 30 years old. NMPD Engineering has proposed new canyon exhaust systems for both F&H Areas. The total project cost to upgrade the exhaust systems in both areas was estimated to be \$177 million. The UCES consisted of four new exhaust fans, new electrical switchgear, two new diesel generators, and a new exhaust stack. As in the existing exhaust system, the UCES assumed three operating fans and one stand-by fan. The stand-by fan would come on if the vacuum in the exhaust tunnel dropped below a preset level. The filtered exhaust air would be discharged through a new stack. Normal power for all four fans would be provided to the Savannah River Site by South Carolina Electric and Gas. Emergency power would be provided to the fans using the two diesel generators. Figure 2 provides a schematic of the UCES.

This evaluation compared the failure frequency of an existing canyon exhaust system to the proposed exhaust system and two cost reduction options. The first option was deletion of the decontamination and decommissioning (D&D) activities. D&D activities included removal of the existing fan building and stack. Collapse of the fan building would not be expected to impact the proposed activities. However, collapse of the stack onto the new exhaust system could have significant impact. Elimination of this work would reduce the UCES project costs by \$29 million. The second option was deletion of the safety class requirements in DOE Order 6430.1A. These requirements included single failure criterion and redundancy and equipment environment consideration; i.e. design basis accidents. Elimination of this work would reduce the UCES project costs by \$19 million.

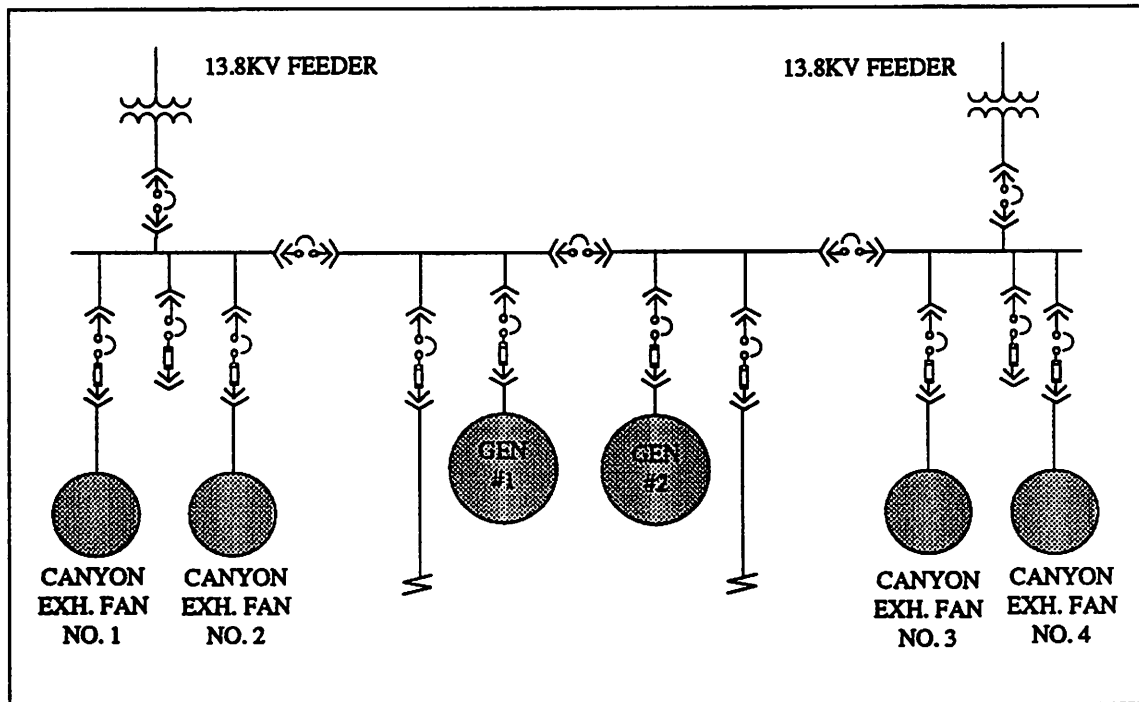


Figure 2. Schematic of the proposed upgrade to the canyon exhaust system. Normal power is supplied to the fans by the utility feeders, and standby power is supplied by the two diesel generators.

Fault trees were prepared to model the proposed UCES and the two options. This evaluation did not consider beyond design basis accidents. The results of the fault trees are presented in Table 1. The results indicate that the proposed exhaust system would

improve system reliability by a factor of about 100; i.e. the system failure rate would decrease from once every 42 years to once every 4200 years. Even if the system were not designed to meet safety class design requirements, there would be an improvement of a factor of 8.3; i.e. the failure rate would decrease from once every 42 years to once every 350 years. This decrease is due to the fact that design requirements have become more stringent. Finally, the results indicate that D&D activities could be deleted from the project with no impact to safety.

**Table 1. Results of UCES fault tree modeling.**

Description	Failure Rate
Failure rate of the existing exhaust system	2.9E-06/hr
Failure rate of the proposed exhaust system	2.7E-08/hr
Failure rate of option 1; deletion of D&D activities	2.7E-08/hr
Failure rate of option 2; deletion of safety class design requirements	3.2E-07/hr

### **Case 2 - Backfit for Diesel Generator**

The diesel generators that provide both normal and standby power to the canyon exhaust systems are over 30 years old. Completion of the Upgrade to the Canyon Exhaust System (UCES) Project is a multi-year task. Between now and the time that the project is installed and operating, NMPD Engineering is charged with the responsibility of keeping the existing canyon exhaust system operating within the safety envelope specified in the Authorization Basis. This may require the short term replacement of some of the existing components.

Recently, the diesel generator that provided standby power to the F-Canyon Exhaust System failed. SRTC was requested to evaluate three diesel generator alternatives for the F-Canyon Exhaust System. These options were; 1) repair of the failed diesel generator, 2) replacement of the failed diesel generator with a new safety class diesel generator, or 3) replacement of the failed diesel generator with a non-safety class diesel generator. The cost and schedule of the three options are summarized in Table 2.

**Table 2. Cost and schedule for diesel generator options.**

Option	Cost (\$\$)	Schedule
Repair of the failed diesel generator	\$500,000	8-9 Months
Replacement of the failed diesel generator with a new safety class diesel generator	\$675,000	12-14 Months
Replacement of the failed diesel generator with a non-safety class diesel generator	Under \$200,000	Immediate

As previously stated, the top event in the F-Canyon Ventilation Fault Tree is "Exhaust System Failure". Exhaust system failure is defined as the failure or loss of all four exhaust fans. The failure scenarios for the fault tree are 1) failure of the stack liner and pluggage of the exhaust path due to a 0.04 g earthquake, 2) failure of the exhaust system switchgear due to a 0.08 g earthquake, 3) failure of the stack and pluggage of the exhaust path due to a tornado, 4) failure of the exhaust tunnel due to structural collapse,

and 5) mechanical and/or electrical failures. The failure rates for these scenarios are summarized in Table 3.

**Table 3.** Failure scenarios and frequencies for the canyon exhaust system.

Description	Failure Rate
Failure of the stack liner and pluggage of the exhaust path due to a 0.04 g earthquake	2.6E-06/hr
Failure of the exhaust system switchgear due to a 0.08 g earthquake	2.3E-07/hr
Failure of the stack and pluggage of these exhaust path due to a tornado	5.0E-08/hr
Failure of the exhaust tunnel due to structural collapse	5.0E-08/hr
Mechanical and/or electrical failure of canyon exhaust system (all four fans fail)	2.0E-09/hr
No significant air flow through the canyon exhaust system	2.9E-06/hr

The fault tree analysis indicates no significant difference between the three diesel generator options. The predicted rate of failure of the canyon exhaust system does not change because the fault tree is dominated by failures due to natural phenomena. This analysis allowed NMPD Engineering to select the most cost/time effective option. Using fault tree analysis, NPSR was able to demonstrate that "backfit" of the diesel generator to meet new safety class requirements did not make good sense (cents).

## CONCLUSIONS

As described above, fault tree analysis can be an effective means of documenting justification for or against proposed changes to a system. The results of the analysis quantify the change in system reliability due to design modifications. The calculated reliability can then be combined with cost estimates to determine if the design modifications are worthwhile.

Upgrades to existing systems classified NS should be evaluated using a cost benefit analysis to determine if the proposed upgrades from the original design requirements to the new NS design requirements are warranted. This cost benefit analysis should be documented and kept as part of the project file.

## REFERENCES

- Browne, E.V., Low, J.M., and Lux, C.R., 1992, "Fault Tree Analysis of Project S-4404, Upgrade Canyon Exhaust Systems (U)," WSRC-TR-92-306.
- Durant, W.S., and Perkins, W.C., 1983, "Systems Analysis - 200 Area Savannah River Plant, H-Canyon Operations," DPSTSY-200-1H.
- Marshall, K.M., and Browne, E.V., 1992, "Fault Tree Analysis of Standby Diesel Generator Alternatives for the F-Canyon Ventilation System (U)," WSRC-TR-93-099.

## **082 Fires, Floods, and Spatial Interactions**

*Chair: R. Oehlberg, EPRI*

**Fermi Internal Flood Analysis Using a Component-Based Frequency Calculation Approach**  
*J.C. Lin, Y.M. Hou (PLG); J.V. Ramirez, E.M. Page (Detroit Edison)*

**Advances in the Methodology for the Analysis of Location-Dependent Hazards for Probabilistic Risk Assessment (PRA)**  
*J.K. Liming, L.A. Bennett (ERIN Eng. & Res.)*

**Location Transformation for Identification and Screening of Internal Fire and Flood Scenarios**  
*T.A. Thatcher, J.L. Jones (INEL); S.A. Eide (LATA)*

**EPRI Fire Events Database**  
*K. Bateman, M. Marteeny, B. Najafi, B. Parkinson (SAIC); R. Oehlberg (EPRI)*

## **FERMI INTERNAL FLOOD ANALYSIS USING A COMPONENT-BASED FREQUENCY CALCULATION APPROACH**

James C. Lin,<sup>1</sup> Yung-Ming Hou<sup>1</sup>  
Jorge V. Ramirez,<sup>2</sup> Earl M. Page<sup>2</sup>

<sup>1</sup>PLG, Inc.  
4590 MacArthur Boulevard, Suite 400  
Newport Beach, CA 92660-2027

<sup>2</sup>Detroit Edison Company  
Fermi 2 Nuclear Plant  
6400 North Dixie Highway  
Newport, MI 48166

### **INTRODUCTION**

An analysis to identify potential accident sequences involving internal floods at Fermi Unit 2 was completed to fulfill the individual plant examination requirements.<sup>1</sup> Floods can be significant core damage scenarios if they cause an initiating event and a common mode failure of critical systems.

### **APPROACH**

Four types of flooding hazard are evaluated in this analysis: water submergence, water spray, steam environment, and steam jet. The basic approach was a conservative screening analysis that first established potential flood sources and safety equipment locations. Flood scenarios were identified in terms of the source and type of flooding, the extent of propagation to adjacent locations, and the equipment impacted. The frequencies of these scenarios were then determined. Important scenarios were combined with independent failures in the overall risk screening model to obtain the estimated contribution to the core damage frequency. A more detailed analysis was performed to reduce conservatism, as required when the preliminary results appeared to be significant.

## POTENTIAL FLOOD SOURCES AND LOCATION OF MITIGATION EQUIPMENT

To identify potential internal flooding sources and the safety impact of floods, the plant layout was reviewed, and a plant walkdown was performed. The potential flood sources are documented in a table that lists the flooding locations, propagation paths, nature of the paths (hatch opening, drains, door, etc.), flood sources (i.e., system/equipment), and the flooding hazard types. An example page of this table is shown in Table 1. In addition, a component location table was developed to include components that could potentially be damaged by the various flooding hazards. This table contains the following information: component designator, component description, component type, component location, component elevation, top event in which the component is modeled, and susceptibility of the component to the flooding hazards. An example page of the component location table is given in Table 2.

Table 1. An example page of hazard source and propagation path table.

Source Location		Propagation		Source Systems	Hazard Type			
ID	Description	Path	to	(Equipment)	SM	SP	SE	SJ
A1	RB TORUS Area	Door	A2	RHR (pipes, valves)	X	X		
		Door	A3	CSS (pipes, valves)	X	X		
		Door	A4	HPCI (pipes, valves)	X	X		
		Door	A5	RCIC (pipes, valves)	X	X		
				FPCC (pipes, valves)		X		
				RWCU (pipes, valves)	X	X		
				RBFP (pipes, fire hose, sprinklers)	X	X		
				TORUS (pipes)	X	X		
				EECW (pipes, valves)		X		
				TWMS (pipes, valves)	X	X		
				CND (pipe)	X	X		
A2	RB SBSM SW Corner Room	Door	A1	RHR (pipes, valves, pumps)	X	X		
		Stairway#	A6					
		HVAC#	A1	RBFP (pipes, fire hose)	X	X		
		(Note 1)		TORUS (pipes)	X	X		
				EECW (pipes, valves)		X		
A3	RB SBSM NW Corner Room	Door	A1	RHR (pipes, valves, pumps)	X	X		
		Stairway#	A7					
		HVAC#	A1	RBFP (pipes, fire hose)	X	X		
				TORUS (pipes)	X	X		
				CND (pipe)	X	X		
				RBHVAC (pipe, valve)			X	
				EECW (pipes, valves)		X		
A4	RB SBSM SE Corner Room	Door	A1	CSS (pipes, valves)	X	X		
		Door	B1	pumps)				
		Stairway#	A8	CST (pipes)	X	X		
		Penetrat.	B1	TORUS (pipes)	X	X		
		HVAC#	A1	RBFP (pipes, fire hose)	X	X		
				RBHVAC (pipes, tank, valves, pumps)		X	X	
				HPCI (pipe-steam)			X	X
				EECW (pipes, valves)		X		
				RBCCW (pipes, valves)	X	X		

### Notes:

1. The hazard propagation path with "#" indicates that the path is for the propagation of the steam-related hazards only.
2. Floods propagating through the equipment and floor drains are considered only for those enclosed locations in the reactor building and the auxiliary building within which the flood hazards are likely to be confined.

Table 2. An example page of equipment/component location table.

Component Identification	Type	Loc	Elev	Top Event(s)	Susceptibility				DESCRIPTION
					SM	SP	SE	SJ	
N30F158B	E/V	T3L11	643	TT	X	X	X	X	TT SVA 4B TROTTLE VALVE 2
N30F158C	E/V	T3L11	643	TT	X	X	X	X	TT SVA 4C TROTTLE VALVE 3
N30F158D	E/V	T3L11	643	TT	X	X	X	X	TT SVA 4D TROTTLE VALVE 4
N30F159A	E/V	T3L11	643	TT	X	X	X	X	TT SVB 4A TROTTLE VALVE 1
N30F159B	E/V	T3L11	643	TT	X	X	X	X	TT SVB 4B TROTTLE VALVE 2
N30F159C	E/V	T3L11	643	TT	X	X	X	X	TT SVB 4C TROTTLE VALVE 3
N30F159D	E/V	T3L11	643	TT	X	X	X	X	TT SVB 4D TROTTLE VALVE 4
N2100F403	AOV	T3P5	664	FL	X	X	X	X	AOV STARTUP LCV
N2101B002	SHTR	T3P5	643	FW	*				STEAM HEATER SOUTH 6S
R1600S012A	MCC	T3S	641	B2	X		X		MCC 72R-2A
R1600S023A	MCC	T3S	641	B2	X		X		MCC 72L-3D
P4300B001	HX	T3S	643	TB	*				TBCCW HEAT EXH 1
P4300B002	HX	T3S	643	TB	*				TBCCW HEAT EXH 2
P4300C001	MDP	T3S	643	TB	X	X	X	X	TBCCW SYSTEM PUMP NORTH
P4300C002	MDP	T3S	643	TB	X	X	X	X	TBCCW SYSTEM PUMP CENTER
P4300C003	MDP	T3S	643	TB	X	X	X	X	TBCCW SYSTEM PUMP SOUTH
P43F405	AOV	T3S	647	TB	X	X	X	X	TBCCW RETURN TO HX FCV AOV
N2001C018	MDP	TBN7	579	CN	X	X	X	X	CONDENSER PUMP "S"
N2001C019	MDP	TBN7	579	CN	X	X	X	X	CONDENSER PUMP "C"
N2001C020	MDP	TBN7	579	CN	X	X	X	X	CONDENSER PUMP "N"
N1100F059A	HOV	TM23	628	MC	X		X		EAST TURB BYPASS HOV
N1100F059B	HOV	TM23	628	MC	X		X		WEST TURB BYPASS HOV

Notes for susceptibility:  
 \* - source of hazard  
 x - component affected by hazard

## FLOOD DATA AND FREQUENCY

The primary source of data includes internal flood data in U.S. nuclear power plants. The industry experience was reviewed to determine the frequencies of floods in different parts of a nuclear plant.

The approach to the calculation of flood frequency can be based on the flooding cause (such as floods due to human errors or hardware failures), the system from which the flood water comes (e.g., circulating water system, service water system, etc.), the equipment from which the floods originate, or the location at which the flooding occurs. Each of these approaches would lead to a different event categorization scheme.

An investigation of the root causes of internal floods in the nuclear plants identifies the following: human error, procedure inadequacy, design deficiency, hardware failure, and manufacturing flaw.

Since a flood can be induced by one cause or by a combination of the preceding causes, the approach used to analyze the flood frequency must be able to represent the effects of these causes. In most of the previous studies, plant location has most often been used as the lowest element at which the frequency is evaluated. This is because (1) each location containing flood source equipment from which a flood may originate can reflect all types of flooding causes and (2) floods initiated from different source equipment in a location produce essentially the same worst case scenario. A plant location can be defined to be as small as an enclosed pump room in which only one or two systems are involved, or as large as a plant building that encompasses numerous systems. Based on the industry flood event data, it is not difficult to derive the flood frequency for a plant building or a large plant area. However, due to plant-to-plant variabilities in design and equipment

arrangement, the flood frequency for a small plant location cannot be easily determined from the flood event data without making grossly simplifying assumptions.

The approach adopted in the Fermi internal flood analysis is a hybrid of both building locations and source components. This approach starts with a total building flood frequency and apportions it, based on the fraction of the flood source equipment inventory. To obtain the source equipment fractions for the frequency apportionment, information on the plant-specific equipment inventory is necessary. This inventory information is collected only for those equipment that are considered to be flood source related.

In the events reviewed, floods in the auxiliary/reactor building usually involved failures of valve gaskets, maintenance errors, pump leaks, or failures of small connections to the pipes. Only one pipe break (at a welded joint) occurred. This observation suggests partitioning the building flood frequency according to the major equipment type that failed or was mispositioned (or its associated components failed or mispositioned), thus producing the flood. The following five categories were used in this analysis in the classification of auxiliary/reactor building floods: pump, valve, heat exchanger, tank, and piping.

It is noted that the equipment boundary of the flood source equipment types listed in the preceding is defined in a broader sense than what is commonly used. For example, a pump includes the instrument taps, the seal water lines, the casing vent line and vent valves, the lube oil cooler, etc. With these broader definitions, all of the flood events can be attributed to one of these flood source categories, regardless of the root causes.

Some flood events reported involve water sprays onto plant equipment without significant water accumulation on the floor. Typically, in a nuclear plant, equipment and floor drains are provided to collect system leakage and prevent uncontrolled radioactive releases. Sump pumps are installed to transfer the water collected in the equipment and floor drain sumps to the radwaste process systems. The sump pump is normally rated at 50 gpm with an automatic startup on a high sump water level signal. It is thus assumed in this analysis that a flood incident with a spill rate of less than 50 gpm would only result in the spray impact; i.e., no water submergence is assumed.

Based on the relative fraction of flooding events grouped into the five major equipment categories, the auxiliary/reactor building flooding frequencies were subdivided into the five major equipment categories. Then, based on the relative density of equipment of each category in each building location, the flooding frequency for each equipment category is further partitioned into each building location. The total flooding frequency in each building location is obtained by summing the frequencies for the five equipment categories. Table 3 illustrates the water submergence frequency in each source location of the auxiliary/reactor building. The frequency of floods in the residual heat removal (RHR) complex pumproom was also estimated using this method.

Compared to the reactor or auxiliary building, the equipment housed in the turbine building is much less risk significant. Furthermore, many large openings exist in the turbine building to allow the flood water to flow freely to the lowest level; i.e., the basement. Therefore, the frequency of water submergence in the turbine building was not divided into the individual rooms in the building. However, the frequency of water spray in the turbine building and the frequencies of water spray and submergence in the general service water pumphouse were apportioned to the various locations based on the relative density of flood sources.

## FLOOD SCENARIOS

The flood scenarios are developed as follows:

1. Examine the flood sources in the hazard source table to determine the sources that could produce significant impacts on important plant equipment.



2. Examine the drainage system and the information in the hazard source table to see which flood connection paths exist between various locations that might propagate during the course of the flood.
3. Produce a list of the floods and the impact of the floods found in Steps 1 and 2. This list includes the impact on the system in which pipe or tank breaks occur due to the loss of water, and the impact on the systems exposed to the flood. In Fermi analysis, this list is documented in the flood initiator impact table. It contains the flood initiator name, areas that would potentially be affected, and the top events that could potentially be impacted by the initiator.

Table 3. Reactor and auxiliary building submergence frequency.

SUBMERGENCE FREQUENCY CALCULATION:						
REACTOR BLDG AND AUX BLDG FLOOD (SM) FREQ. = 0.0151						
NUMBER OF EVENTS						
PIPING	=	4				
VALVE	=	6				
PUMP	=	2				
TANK	=	2				
HEAT EXCHANGER	=	3				
TOTAL	=	17				
ROOM ID	FREQ (TOT)	PIPING F (PIPE)	VALVE F (VALVE)	PUMP F (PUMP)	TANK F (TANK)	HX F (HX)
A1	1.47E-03	40 3.57E-04	177 1.11E-03	0 0.00E+00	0 0.00E+00	0 0.00E+00
A12N	2.12E-04	16 1.43E-04	11 6.89E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
A12S	3.36E-04	25 2.23E-04	18 1.13E-04	0 0.00E+00	0 0.00E+00	0 0.00E+00
A13	1.70E-04	4 3.57E-05	9 5.64E-05	0 0.00E+00	0 0.00E+00	0.5 7.84E-05
A16	2.14E-04	12 1.07E-04	17 1.06E-04	0 0.00E+00	0 0.00E+00	0 0.00E+00
A17NC	5.45E-05	4 3.57E-05	3 1.88E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
A17NE	7.86E-05	6 5.36E-05	4 2.51E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
A17S	5.72E-04	20 1.79E-04	12 7.52E-05	0 0.00E+00	1 1.61E-04	1 1.57E-04
A17W	5.67E-04	18 1.61E-04	14 8.77E-05	0 0.00E+00	1 1.61E-04	1 1.57E-04
A18N	2.84E-04	5 4.46E-05	29 1.82E-04	1 5.73E-05	0 0.00E+00	0 0.00E+00
A18S	1.90E-04	5 4.46E-05	14 8.77E-05	1 5.73E-05	0 0.00E+00	0 0.00E+00
A19	1.06E-03	8 7.14E-05	33 2.07E-04	0 0.00E+00	0 0.00E+00	5 7.84E-04
A2	5.38E-04	15 1.34E-04	28 1.75E-04	4 2.29E-04	0 0.00E+00	0 0.00E+00
A20	3.91E-04	2 1.79E-05	8 5.01E-05	0 0.00E+00	2 3.23E-04	0 0.00E+00
A21	2.15E-05	1 8.93E-06	2 1.25E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
A22N	2.62E-04	10 8.93E-05	15 9.39E-05	0 0.00E+00	0 0.00E+00	0.5 7.84E-05
A22S	3.24E-04	10 8.93E-05	25 1.57E-04	0 0.00E+00	0 0.00E+00	0.5 7.84E-05
A24	6.08E-05	4 3.57E-05	4 2.51E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
A28	4.96E-04	2 1.79E-05	8 5.01E-05	2 1.15E-04	0 0.00E+00	2 3.13E-04
A3	5.07E-04	15 1.34E-04	23 1.44E-04	4 2.29E-04	0 0.00E+00	0 0.00E+00
A34	1.00E-03	25 2.23E-04	14 8.77E-05	1 5.73E-05	2 3.23E-04	2 3.13E-04
A4	6.09E-04	18 1.61E-04	35 2.19E-04	4 2.29E-04	0 0.00E+00	0 0.00E+00
A41	5.09E-04	10 8.93E-05	67 4.20E-04	0 0.00E+00	0 0.00E+00	0 0.00E+00
A43	4.99E-04	12 1.07E-04	11 6.89E-05	0 0.00E+00	2 3.23E-04	0 0.00E+00
A5	1.25E-03	22 1.96E-04	98 6.14E-04	5 2.87E-04	0 0.00E+00	1 1.57E-04
A6	2.15E-05	1 8.93E-06	2 1.25E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
A7	2.77E-05	1 8.93E-06	3 1.88E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
A8	4.65E-05	1 8.93E-06	6 3.76E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
A9	4.65E-05	1 8.93E-06	6 3.76E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
R1A19	1.70E-04	4 3.57E-05	9 5.64E-05	0 0.00E+00	0 0.00E+00	0.5 7.84E-05
R1B12	1.08E-04	3 2.68E-05	13 8.14E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
R4A16	6.88E-05	7 6.25E-05	1 6.26E-06	0 0.00E+00	0 0.00E+00	0 0.00E+00
R4E11	3.38E-04	1 8.93E-06	1 6.26E-06	0 0.00E+00	2 3.23E-04	0 0.00E+00
A3G10	2.77E-05	1 8.93E-06	3 1.88E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
B1	9.13E-04	17 1.52E-04	60 3.76E-04	4 2.29E-04	0 0.00E+00	1 1.57E-04
B11	2.15E-05	1 8.93E-06	2 1.25E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
B14	8.93E-06	1 8.93E-06	0 0.00E+00	0 0.00E+00	0 0.00E+00	0 0.00E+00
B19	8.93E-06	1 8.93E-06	0 0.00E+00	0 0.00E+00	0 0.00E+00	0 0.00E+00
B2	2.61E-04	8 7.14E-05	12 7.52E-05	2 1.15E-04	0 0.00E+00	0 0.00E+00
B20	8.93E-06	1 8.93E-06	0 0.00E+00	0 0.00E+00	0 0.00E+00	0 0.00E+00
B24	3.04E-05	2 1.79E-05	2 1.25E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
B27	1.52E-05	1 8.93E-06	1 6.26E-06	0 0.00E+00	0 0.00E+00	0 0.00E+00
B27A	3.66E-05	2 1.79E-05	3 1.88E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
B28N	0.00E+00	0 0.00E+00	0 0.00E+00	0 0.00E+00	0 0.00E+00	0 0.00E+00
B28S	0.00E+00	0 0.00E+00	0 0.00E+00	0 0.00E+00	0 0.00E+00	0 0.00E+00
B29	2.15E-05	1 8.93E-06	2 1.25E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
B3	7.69E-05	3 2.68E-05	8 5.01E-05	0 0.00E+00	0 0.00E+00	0 0.00E+00
B6	8.93E-06	1 8.93E-06	0 0.00E+00	0 0.00E+00	0 0.00E+00	0 0.00E+00
B9	1.15E-03	30 2.68E-04	38 2.38E-04	3 1.72E-04	1 1.61E-04	2 3.13E-04
TOTAL	1.51E-02	398 3.55E-05	851 5.33E-03	31 1.78E-03	11 1.78E-03	17 2.66E-03

## DESIGN CONSIDERATIONS FOR INTERNAL FLOODING

Due to the open design and layout of the Fermi Unit 2 plant, significant immersion of components could only take place in the sub-basement of the reactor/auxiliary building and the basement of the turbine building. Open floor plans and extensive penetrations through the floor on each level of these buildings would prevent immersion on the upper levels. Spray can only be a significant problem for areas with unprotected electrical cabinets and components near normally operating systems with large, high pressure sources. Major sources of steam in the reactor building include the high energy lines and the building heating system. The only major steam source in the auxiliary building is the building heating steam. Since the building heating system contains only low energy steam, the low steam pressure is not expected to result in a steam environment or steam jet severe enough to cause equipment damage.

## RESULTS

Internal flooding at Fermi Unit 2 has been evaluated to be a low risk compared to core damage from other contributors. The total contribution to core damage due to internal flood scenarios is about 3% of all contributors. All flood scenarios were estimated to be less than  $1 \times 10^{-8}$  events per year except for the following three scenarios:

- Rupture of condensate or RHR system equipment in north reactor water cleanup pumproom on the second floor of the reactor building results in flooding in the southwest and northwest corner rooms in the reactor building sub-basement. Due to water submergence, the RHR system is failed. Low pressure coolant injection, torus cooling, and shutdown cooling modes of RHR operation become unavailable. In addition, long-term operation of the high pressure coolant injection/reactor core isolation cooling and core spray systems would be prevented by the gradual heatup of the suppression pool. If all other vessel injection systems (i.e., feedwater, standby feedwater, and condensate along with vessel depressurization) or heat removal systems (i.e., main condenser and torus vent) are also lost because of failures unrelated to the flooding, core damage would occur.
- Rupture of the circulating water system or the condensate system equipment in the turbine building results in a large amount of flood water accumulating in the turbine building basement. Due to the extremely large water inventory and the high water flow rates in these systems, the impact of this scenario is failure of the balance-of-plant AC power, condensate system, and standby feedwater system by the flood water. Consequently, vessel injection by the feedwater system and decay heat removal by the main condenser also become unavailable. If all other vessel injection systems or core heat removal systems were also lost due to failures not associated with flooding, core damage would occur.
- Rupture of RHR or condensate equipment in the general area of the third floor of the reactor building results in flooding of the southwest and northwest corner rooms in the reactor building sub-basement. The impact of this scenario is similar to the first scenario.

## REFERENCE

1. J. C. Lin, et al., "Fermi 2 Internal Flood Analysis," PLG-0849 (1992).

**ADVANCES IN THE METHODOLOGY FOR  
THE ANALYSIS OF LOCATION-DEPENDENT HAZARDS  
FOR PROBABILISTIC RISK ASSESSMENT (PRA)**

**James K. Liming and Lawrence A. Bennett**

**ERIN Engineering and Research, Inc.  
2175 N. California Blvd., Suite 625  
Walnut Creek, CA 94596-3574  
(510) 943-7077; FAX (510) 943-7087**

**INTRODUCTION**

Location-dependent hazards to the successful operation of complex engineered facilities include fire, flood, earthquakes, tornadoes, severe weather, and other natural phenomena known as external hazards. They also include fire, flood, explosion, chemical attack, biological attack, toxic environments, sabotage, and other "internal" hazards directly associated with the people and equipment that make up the process(es) of the facility of interest. These hazards are location-dependent because they can originate in one or a small set of areas, zones, or rooms of a process facility, affect one or more systems associated with the facility, and then propagate to other areas of the facility thus causing multiple dependent failures in process systems. Risks associated with these hazards include health risk to the general public, health risk to the facility operators, risk of mission failure, and financial risk to facility owners and stockholders, among others. While the concept of analysis of these location-dependent hazards within a probabilistic risk assessment (PRA) of complex engineered facilities is not new, several advances in the analysis of these hazards have been made over the past two to three years as a result of the performance of location-dependent hazard analysis mandated by regulatory requirements such as:

- The U.S. Nuclear Regulatory Commission (NRC) requirement to perform an analysis of internal flooding in nuclear power plant individual plant examinations (IPEs).
- The NRC requirement to perform earthquake, fire, severe storm, and other location-dependent hazards in nuclear power plant individual plant examinations for external events (IPEEEs).

- The upcoming Environmental Protection Agency (EPA) requirements for all facilities manufacturing, distributing, or handling certain hazardous or toxic materials to develop risk management plans.

The purpose of this paper is to present the current state of the art in location-dependent hazard analysis methodology and specifically describe several recent advancements in this technology.

## OVERVIEW OF LOCATION-DEPENDENT PRA METHODS

Historically, location-dependent PRA has been applied at varying levels of detail and at different levels of indenture in facilities, based, at least in part, on the desired scope of the analysis determined by those funding the PRA work. The basic process of location dependent PRA includes defining a three-dimensional zone designating system for the facility of interest, locating hazard sources, locating hazard-susceptible "target" components of important process systems, defining hazard propagation scenarios, and quantifying the risk associated with each scenario. In practice, engineering judgement has been applied at many stages of this process, particularly in hazard source location, target component location, and hazard propagation analysis. A comprehensive analysis of the impact of location-dependent hazards on overall facility risk includes the following general tasks:

- Preliminary hazard scenario development
- Facility walkdown
- Initial hazard scenario frequency screening
- Refinement of analysis bases and assumptions
- Detailed hazard scenario risk quantification

The final two steps are often performed iteratively until each scenario is determined to be below a pre-established screening frequency or until the scenario frequency is as low as is reasonably achievable by removing or revising conservatisms in the analysis. A flow chart illustrating a typical hazard scenario screening and quantification process is presented in Figure 1.

## ADVANCES IN LOCATION-DEPENDENT PRA

Analysts performing PRAs for large complex facilities generally develop detailed logic models (fault trees and event trees) to characterize the risk associated with independent internal failures of specific facility components. These models define the facility risk minimal cut sets, sets of one or more basic human errors and/or component failures that are both necessary and sufficient to cause a defined consequence. The impact of dependent events (i.e., common cause failures and location-dependent hazards) is often "added in" or assessed with the knowledge of the composition of the independent basic event minimal cut sets. For example, in a nuclear power plant PRA of core damage frequency, it may be determined in the "independent basic event risk model" that the set of failures including an initiating event I (such as a reactor trip), and failures of pump A, motor-operated valve B, pressure transmitter C, and human action D form a minimal cut set (IABCD) that defines one possible core damage scenario. For this example, let us assume that these

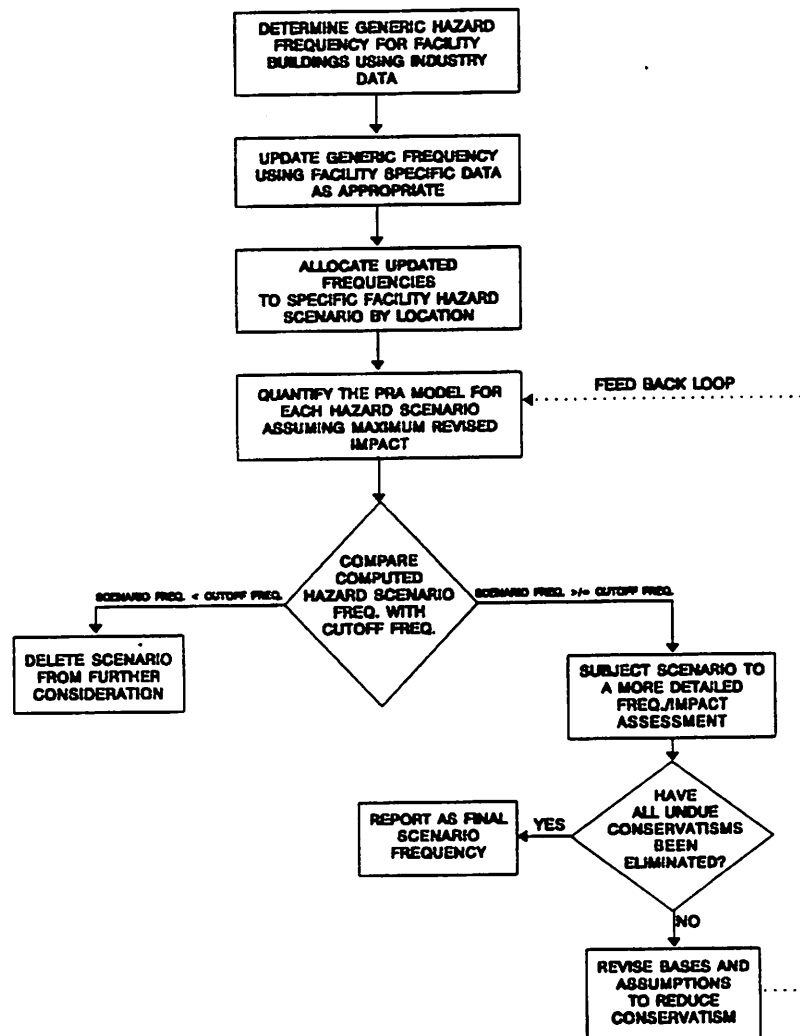


Figure 1. Hazard Scenario Frequency Screening and Quantification Process

events are associated with diverse systems or equipment. Independently, each of these five events may have a relatively low failure rate or unavailability upon demand (i.e.,  $\leq 10^{-3}$  per year or  $\leq 10^{-3}$  per demand) thus yielding a very low cut set frequency of less than  $10^{-15}$  per year. In practice, current fault tree codes, such as FTAP, that are used in popular risk assessment software may be set up to truncate cut sets at or even above  $10^{-12}$  per year. This would mean that our example cut set IABCD would be truncated. This is acceptable in the independent plant model because other, generally lower-order, higher frequency cut sets dominate the overall risk. However, this may not be the case for many location-dependent hazard scenarios. For example, a simple fire or flood scenario may cause a plant transient initiating event and also, consequently, fail or disable all four additional components in our example cut set at the hazard scenario initiating event frequency which could be about  $10^{-4}$  to  $10^{-3}$  events per year. This example illustrates why it is important to, if practical, load location-dependent hazard scenario basic event impacts into the "front-end" of the risk model rather than trying to post-process existing cut sets through a "back-end" analysis. A check calculation performed during a recent nuclear power plant individual plant examination (IPE) indicated that the error introduced by performing traditional "back-end" analysis versus

"front-end" analysis can be significant (greater than 10% of the calculated core damage frequency). Of course, if all cut sets of the independent logic model are developed (i.e., no truncation was performed), then back-end analysis of location-dependent hazards can be effectively and efficiently accomplished. However, to analyze complex facility logic models, it is generally necessary to apply a truncation process to avoid overflowing arrays in current versions of risk applications software and to avoid excessive personal computer time.

When applying front-end location-dependent hazard analysis using current software, it is often necessary to apply two types of logic model runs. In the first type of run, called a TRUE run, the components and other model basic events deemed to be failed by the location-dependent hazard scenario of interest are set equal to a logical true (guaranteed failure) in the model run input file. In the second type of run, called a ONES run, these basic events are set equal to one (1.0) in the input file. There are advantages and disadvantages to each type of run. The TRUE run yields a mathematically correct consequence frequency, and ultimately must be performed to yield accurate risk quantification results. Also, TRUE runs reduce logic model complexity up front in the analysis, thereby promoting faster run times for cut set generation and quantification. However, the TRUE run does not conserve the hazard-affected basic event identification in the logic model cut sets. Therefore, if, as is usually the case, recovery analysis must be performed, another method must be used to generate cut sets. The ONES run conserves the hazard-affected basic event identification in the cut sets, but yields a significantly overstated consequence frequency in the risk quantification. This occurs because there are many "parallel" logic paths from the initiating event to a defined consequence (i.e., reactor core damage) in location-dependent hazards scenarios. Using current PRA software, both types of runs must be applied to yield accurate risk quantification results.

If a screening process is applied in location-dependent PRA which has several defined hazards scenarios, it is advisable to review all scenarios for repeated patterns of identical basis event impact. Defining these patterns and performing recovery analysis for cut sets generated by these patterns can significantly reduce the total time and effort involved in location-dependent hazards PRA. For example, in a flood analysis, the flood liquid (usually water) generally propagates through floor drains, doorways, and stairwells down to the lowest elevation zones in the facility of interest. Thus, for most flood scenarios where the flood starts in a specific room of a specific building in the facility, there is usually a specific set of zones into which the flood liquid propagates and collects. Performing successful recovery analysis for flooding in this specific set of zones which appears in the propagation paths of many of the flood scenarios identified in the location-dependent PRA, can yield successful recovery of all of those scenarios.

The most thorough and accurate location-dependent PRAs include a careful review of process support systems such as electric power, component cooling water, service water, service air, and heating, ventilation, and air conditioning (HVAC) systems. The impact of location-dependent hazards on these systems can cause cascading or dependent failures that result in risk-significant consequences at process facilities. Electric power and associated control and instrumentation wiring are often the most challenging systems to analyze in a location-dependent PRA because their associated cable routing is complex and pervasive throughout many zones of the facility of interest. However, recent experience has shown that many facilities now have computerized configuration management systems that can be effectively employed to develop effective cross-reference lists of hazard-susceptible equipment (including important electric cables) in specific facility rooms or zones. Effective use of these

computerized configuration management systems can greatly streamline the process of developing a comprehensive set of hazard scenarios and associated impacts for the facility of interest.

Other tools and techniques applied by the authors in recent location-dependent hazards PRAs have proved to be very effective in streamlining the analysis process. While the size restriction on this paper prohibit a full explanation of each of these tools, they include or deal with the following topics:

- Review of the hazard scenarios in order to ensure the correct transient response is modeled. In other words, if a turbine trip transient is to be used as the assumed initiator, perform a review to ensure that hazard induced failures do not result in other consequential events such as a total loss of feedwater or a loss of coolant accident (LOCA).
- The importance of clearly stated, realistic analysis bases and assumptions. It is advisable to develop a list of generic bases and assumptions for effective hazard screening analysis.
- The linking of hazard-caused process equipment failure and human action failure basic events to hazard scenarios and specific facility zones through effective data base management techniques.
- The importance of including hazard-independent failures in location-dependent hazards risk models versus the conventional approach of focusing only on hazard-dependent direct paths to failure.
- Methods for efficiently "pre-processing" hazard-dependent dynamic human action and recovery action successes and failures prior to risk model quantification.
- Hazard propagation analysis using time-dependent arguments and models.

Application of these tools and techniques can improve the quality and reduce the manpower associated with location-dependent PRA.

## CONCLUSION

For accurate location-dependent PRA risk quantification, it is important to understand the difference between front-end and back-end logic model quantification, and the advantages and disadvantages of each approach. While back-end quantification is much less manpower and computer run time intensive, it can yield significantly erroneous results unless it can be assured that all cut sets are generated and retained in the original independent event logic model analysis. This is generally not the case for PRA of large complex facilities analyzed using current versions of popular risk management software, which must apply a truncation routine to avoid overflowing arrays and/or causing excessive computer run time. Tools and techniques for addressing this issue and other important issues associated with location-dependent PRA have been developed and are being effectively applied in today's risk analyses.

## ACKNOWLEDGMENTS

The authors would like to thank the engineering, operations, and maintenance departments (and particularly the risk assessment staffs) of the following organizations for their valuable input into the development and refinement of the technical tools and techniques discussed in this paper: Entergy Operations, Inc. (both the Arkansas Nuclear One and Waterford Unit 3 staffs) and TU Electric.

## REFERENCES

- Gaertner, J. P., et. al., "Arkansas Nuclear One Unit 2 Internal Flood Screening Study," prepared for Entergy Operations, Inc., May 1992.
- Iden, D. C., J. K. Liming, and R. Suarez, "Waterford 3 Steam Electric Station Individual Plant Examination Internal Flood Analysis," prepared for Entergy Operations, Inc., October 1991.
- Iden, D. C. and J. K. Liming, "Comanche Peak SES IPE Internal Flood Risk Analysis," prepared for TU Electric, October 1981.
- Liming, J. K., J. H. Ambrose, J. M. Nolan, "ANO 1 & 2 Response to INPO SOER 85-5 Internal Flooding for Power Plant Buildings," 92-R-0024-01, prepared for Entergy Operations, Inc., February 1993.
- Pickard, Lowe and Garrick, Inc., "Muehleburg Probabilistic Risk Assessment Internal Fire and Flood Analysis," prepared for Bernische Kraftwerke AG, July 1990.
- Pickard, Lowe and Garrick, Inc., "Three Mile Island Unit 1 Probabilistic Risk Assessment Internal Fire and Flood Analysis," PLG-0525, prepared for GPU Nuclear, November 1987.
- Pickard, Lowe and Garrick, Inc., "Diablo Canyon Probabilistic Risk Assessment Internal Fire and Flood Analysis," prepared for Pacific Gas & Electric Company, December 1986.
- Pickard, Lowe and Garrick, Inc., "Beznau Probabilistic Risk Assessment Internal Fire and Flood Analysis," prepared for Nordostschweizerische Kraftwerke AG, August 1986.



## **LOCATION TRANSFORMATION FOR IDENTIFICATION AND SCREENING OF INTERNAL FIRE AND FLOOD SCENARIOS<sup>a</sup>**

**T. A. Thatcher<sup>1</sup>, S. A. Eide<sup>2</sup>, and J. L. Jones<sup>1</sup>**

<b>Idaho National Engineering Laboratory</b>	<b>Los Alamos Technical Associates, Inc.</b>
<b>P. O. Box 1625</b>	<b>P. O. Box 51688</b>
<b>Idaho Falls, ID 83415</b>	<b>Idaho Falls, ID 83405-1688</b>

### **INTRODUCTION**

The Advanced Test Reactor (ATR) probabilistic risk assessment (PRA) included a comprehensive internal fire and flood analysis. Identification and screening of fire and flood scenarios involved a location transformation or vital area analysis<sup>1</sup>. Highlights of the project include the following:

- Development of transformation equations to model the locations of equipment corresponding to basic events in system fault trees associated with the internal fire and flood event tree
- Accident sequence cutset evaluation completely on a personal computer (PC), with truncation of cutsets containing more than two vital areas or combinations of component random failures with a combined probability of 1.0E-8
- Automated elimination of non-physical cutsets for internal fire analysis and for internal flooding analysis
- Screening quantification of all internal fire and flood scenarios, with special screening values for initiators and human errors

---

<sup>a</sup>Work supported by the U.S. Department of Energy, Assistant Secretary for Nuclear Energy, under DOE Idaho Field Office Contract No. DE-AC07-76ID01570.

- Comparison of vital areas identified by location transformation with areas identified by only detailed walkdowns
- Efficient and detailed screening process resulting in a logical and traceable scenario identification and screening that includes the contribution of random events

The ATR is a Department of Energy 250-MW<sub>thermal</sub> test reactor located at the Idaho National Engineering Laboratory. The ATR has numerous systems related to safe reactor shutdown and emergency core cooling. Parts of these systems are located in different buildings and within various rooms and compartments. Different systems share the same area, and some equipment support more than one system. Thus, the complexity of the systems and the arrangement of equipment invited the use of a systematic and thorough approach to determine the most important areas of the facility in terms of fuel damage risk. Complexity was also posed by the nature of fire and flood events possible at ATR. A fire event can spread to more than one room, and fire suppression activities can cause additional damage in various areas. A flooding event can propagate across and/or down through the facility, causing damage to equipment located far from the source of the flood. In order to aid the identification of scenarios and to efficiently screen them, the location transformation approach was used.

## **METHODOLOGY**

The internal fire and flood analysis for ATR involved the following steps:

1. Designate zones (rooms or parts of large rooms) within the buildings containing equipment important to safety
2. Develop a general event tree to cover both fire and flood scenarios
3. Identify the locations or zones for all of the basic events in the system fault trees that could be impacted by a fire or flooding event.
4. Perform a location transformation analysis to obtain sequence cutsets involving damage to equipment within a zone or zones and the additional random events (not related to the fire or flood event) that must occur in order to lead to fuel damage
5. Create flood- and fire-specific sequence cutsets by eliminating cutsets containing combinations of zones that cannot all be affected by a single fire or flood event
6. Quantify and screen fire and flood scenarios by using screening initiator frequencies, propagation (from zone to zone) probabilities, and human error probabilities

7. Perform refined analyses for fire and flood scenarios that survived the screening process.

The location transformation methodology affected all of the steps except step 7. However, the methodology mainly impacts steps 4, 5, and 6. All of the steps are summarized below.

In step 1, zones within the ATR were identified mainly to agree with fire zones. In some cases, a zone was subdivided because of the separation of equipment important to safety. The resultant zones made sense for both fire and flood analyses.

Step 2 involved the development of a single event tree for both the fire and flooding analyses. This single event tree could then be used for all of the internal fire and flood scenarios identified. The event tree was simplified without introducing significant conservatisms, and it included only those systems that would have equipment and cable locations traced. The system fault trees applicable to the event tree had already been developed as part of the overall ATR PRA.

Step 3 involved identifying the locations of equipment modeled in the event tree and corresponding fault trees in terms of the zones specified in step 1. In addition to locations of components, locations were also identified for human actions and for dependent failures. Only the equipment or cables susceptible to damage from a flood or fire event with regard to the basic event failure mode were traced in detail. Ground rules were developed that provided guidance for determining equipment susceptibility, correspondence between passive component faults not modeled explicitly and existing basic events in the fault tree, and treatment of common cause events.

In step 4, the system fault trees were modified to include information on component zones and the accident sequence cutsets were determined. This step is the heart of the location transformation methodology. Basic events within the fault trees were transformed into corresponding zones and (the same) basic events using fault tree OR-gate logic. For example, if the original basic event for pump failure was named "PUMPA", and the pump was located in zone "ZONE1", the transformation equation would be as shown below:

$$\text{PUMPA} = \text{PUMPAX} + / \text{ZONE1}$$

The zone "ZONE1" was complemented to allow truncation on the number on zones in the cutset using the SETS code. Additionally, to include cable faults that were not modeled in the original fault trees, if the pump was located in zone 1, and the power supply and actuation cables were located in zones 3 and 4, and cable fault would disable the pump, OR-gate logic can be used to create the transformation equation shown below:

$$\text{PUMPA} = \text{PUMPAX} + / \text{ZONE1} + / \text{ZONE3} + / \text{ZONE4}$$

While the "replaced" random event (PUMPAX) must be combined with the zone or zones using OR-gate logic, zones can be logically combined with any combination of OR-gate or AND-gate operators.

The resultant system fault trees were then combined to determine sequence cutsets, using the fault tree linking process. System successes were accounted for by deleting cutsets that could not occur given successes in the sequence in question. (This process was performed using only the random events in the cutsets; such a process was deemed not appropriate for the zones.) Sequence cutsets were truncated if they contained more than two zones or a cutset probability of less than  $1.0\text{E-}8$ . Human error rates of 1.0 were assumed for this step. The entire process was performed using a personal computer (PC) version of the SETS code.<sup>1</sup>

For step 5, given the generalized accident sequence cutsets for the event tree sequences leading to fuel damage, the results were made flood- or fire-specific by deleting cutsets that contained combinations of zones that could not be affected by a single fire or flood event. The unwanted zone combinations were treated, in essence, like an event tree success branch. Combinations of events that are successful cannot occur in the failure cutsets.

Step 6 involved a comprehensive screening quantification of all event tree sequences for each potential fire or flood scenario. This quantification was performed using screening values for initiator frequencies, propagation probabilities, and human errors. Also, this screening process assumes that all equipment or human actions within a zone fail given the fire or flood. The plant response to the fire or flood initiator was also evaluated because the timing of some events may not be bounded by previous analyses.

Finally, step 7 involved a refined analysis of fire and flood scenarios that were not screened in step 6. Such refined analyses estimate the actual contribution of fires and floods to the overall ATR fuel damage frequency. The refined analysis included refined initiator frequencies, refined estimates of the extent of damage caused by the initiator, and detailed evaluation of important operator actions.

## RESULTS

Adding the location transformation approach to the ATR PRA internal fire and flood analyses resulted in approximately three weeks extra effort. However, the results (identification of scenarios and screening quantification) from such an approach were well worth the effort. A much more comprehensive set of scenarios resulted from the methodology than would have resulted from just walkdowns. Also, the resultant sequence cutsets clearly indicate both the areas involved and the complete set of random component failures involved (including support systems such as electrical, cooling, actuation, and others). Finally, the methodology is logical and reproducible.

## REFERENCES

1. D. W. Stack and Mildred S. Hill, "A SETS User's Manual for Vital Area Analysis", NUREG/CR-3134, April 1984.
2. Halliburton NUS Environmental Corporation, SETS/386, September 25, 1989.

## EPRI FIRE EVENTS DATABASE

Dr. Richard N. Oehlberg<sup>1</sup>, Marna Marteeny<sup>2</sup>, Karen Bateman<sup>2</sup>, Bijan Najafi<sup>2</sup>, and William Parkinson<sup>2</sup>

<sup>1</sup>Electric Power Research Institute  
3412 Hillview Avenue  
Palo Alto, CA 94303

<sup>2</sup>Science Applications International Corp.  
5150 El Camino Real, Suite B-31  
Los Altos, CA 94022

## INTRODUCTION

Following the NRC request that utilities perform Individual Plant Examinations (IPEs) of their nuclear power plants<sup>1,2</sup> and anticipating NRC's further request for fire risk analyses<sup>3,4</sup>, EPRI initiated a coordinated research program to develop fire risk tools to assist utilities. A primary objective of the program was to provide an appropriate methodology that would enable licensees to efficiently identify potential fire-related vulnerabilities. The Fire-Induced Vulnerability Evaluation (FIVE) methodology<sup>5</sup> provide this capability. Perceiving that undue conservatism may exist in some past Fire Probabilistic Risk Assessments (FPRAs), EPRI also developed methods and data that improve the realism of FPRAs.

The realism of FPRA or FIVE depends in large part upon the quality and completeness of its data sources. Fire initiation frequency and automatic suppression reliability can both be obtained from fire event data. Insights gained from the events data may be useful in resolving other fire risk issues, e.g., manual suppression effectiveness.

Many of the fire risk assessments<sup>6-17</sup> were limited by the availability of fire events data. The earliest effort to gather fire events data resulted in the "HTGR" fire database<sup>18</sup>. This database contained roughly 60 events, 18 of which reported duration. Some FPRAs<sup>6-11</sup> developed their own databases of fire ignition sources, resulting in some duplicated efforts and different results.

In 1983, EPRI published the Nuclear Power Plant Fire Loss Database, EPRI NP-3179<sup>19</sup>. This database contained 116 fires that occurred between February 1965 and February 1982. Events were included only for plants in pre-operational testing<sup>\*</sup> or commercial operation. This database contained 19 fields that described the plant, the fire ignition source, any damage caused by the fire, and the fire suppression activities. Inclusion details of fire suppression activities made this database more complete than prior databases. Fifty-seven of the 116 fire events reported fire duration. More than half of these 57 events

---

\* Pre-operational testing has been defined as the period of time between the date of issue of a *nuclear reactor operating license* to the date the reactor was formally connected to a commercial power grid. This definition of the pre-operational testing period has been redefined in the fire event data base as the date of issue of a *reactor low power operating license* to the date the reactor was formally connected to a commercial power grid.

occurred before the Browns Ferry fire (March 22, 1975), and all of them occurred before 1978. (For the events occurring from 1978 to February 1982, the EPRI database did not report duration). While this database included a larger number of fire events and a larger number of fire events with reported fire duration, most of the events (and all the events with reported duration) were pre-Appendix R<sup>20</sup> (that is, pre-1980 time period). Furthermore, 20 of the 57 reported events that included fire duration occurred during the pre-operational testing phase of plant operation.

In 1986, NRC published NUREG/CR-4586<sup>21</sup>, often referred to as the "Wheelis Database" in recognition of its author. This database contained 354 reported fire events representing nuclear power plant experience during construction, pre-operational testing, and commercial operation from February 1965 through June 1985. Wheelis reported approximately 300 fire events through February 1982 versus the 116 in the EPRI database. However, 113 of the additional events occurred during construction, a phase EPRI considered inappropriate for use in operating nuclear power plant fire risk assessments. The Wheelis Database contained 31 fields, 15 of which were not contained in the EPRI database. Of those, nine were used to identify the plant. This database was structured for easy use with a personal computer.

Unfortunately, as with the early EPRI database<sup>19</sup>, a number of fields are often empty. In particular, only 83 of the 354 events reported fire durations, 15 of which occurred during construction. A large fraction of Wheelis' other 68 fire events with durations were also reported in the EPRI database, which was a principal reference for NUREG/CR-4586. These events were the principal data source for the 69 events in the Fire Risk Scoping Study's manual suppression database<sup>22</sup> and the manual suppression probabilities in the recent NUREG-1150 fire risk assessments of Surry and Peach Bottom<sup>23,24</sup>. The Wheelis database was also the principal source for NUREG-1150's ignition frequencies. Consequently, much of the manual suppression basis for these NUREG-1150 studies is derived from the pre-Appendix R experience originally tabulated in the EPRI database.

Despite the usefulness of the Wheelis database, a number of motivations for an improved database remained. Between June 1985 and December 1988 there were approximately 340 reactor-years of nuclear plant operating experience. This time period represents nearly 40 percent of the total contained in Wheelis and an even larger fraction of the post-Appendix R experience. A new survey of fire events data would increase the fraction of the database representing current operating practices, thereby making the Individual Plant Examination for External Events (IPEEE)<sup>3,4</sup> searches for fire vulnerabilities more contemporary.

One further motivation existed for improving the quality and completeness of fire events data. In the Wheelis database, many of the fields contained incomplete information. General improvements in event reporting practices by utilities suggested that more recent descriptions of fire events would be more complete, especially regarding suppression.

In response to the above considerations, it was decided to build a new fire events database by updating the Wheelis database to include the years through 1988. This update was performed by reviewing Daily Plant Status Reports (DPSRs) from 1985 through 1988<sup>25</sup>. The resulting database was verified and augmented by incorporating new information from other sources including a recent unpublished database from an EPRI project<sup>26</sup>, the Nuclear Power Experience (NPE) database<sup>27</sup>, and selected fire PRAs<sup>9,11,23,24</sup>. Other less obvious sources were also used<sup>29,30,31</sup>. Lastly, EPRI sent a questionnaire to utilities requesting them to fill in incomplete fields for previously reported events, as well as to identify any additional notable events. This paper describes the EPRI Nuclear Power Plant Fire Events Database (FEDB) that came out of that effort<sup>32</sup>.

## DESCRIPTION OF THE FIRE EVENTS DATABASE (FEDB)

FEDB contains 753 fire events that occurred in PWRs and BWRs between February 1965 and December 1988. The reactor low-power operating license date for each plant was the principal screening criterion used to identify events for inclusion in the database. Use of the license date assured that a consistent period would be adopted for data collection and interpretation. A similar approach was used by EPRI in its USI A-44 station blackout database activities.

The FEDB package consists of main database files and a small dBase program, which is used to calculate reactor operating experience in days and years. As with the Wheelis Database, FEDB was created using the computer code, dBase III+, however FEDB may be queried through later versions of dBase or other database management systems such as Q+E, part of the Excel 3.0 for Windows spreadsheet package.

The EPRI FEDB contains 753 fire events with 35 fields that describe distinct attributes of each fire. Table 1 shows the names, types, widths, and descriptions of each field. It contains a substantial database of fire durations and suppression times. Nearly two-thirds of the events (478) reported fire durations, and one-half (374) reported suppression times.

The EPRI FEDB contains information for each US nuclear power plant including those plants that are built, under construction, or were at one time planned for construction. Information such as reactor type, plant and utility name, capacity, date of operating license issuance, date of reactor decommissioning, date of initial criticality, and date of commercial operation are also contained in the FEDB<sup>28</sup>. One file can be used to calculate reactor operating experience to relative to user select event characterizations. Reactor operating experience can be easily calculated for BWRs, PWRs, or both. Beginning and ending dates may be varied for different applications. Currently, the beginning and ending dates are set to February 1, 1965 and December 31, 1988 respectively. Table 2 shows the reactor operating experience in years for BWRs and PWRs, both individually and combined, for the current database contents.

**Table 1. Fire Data Base Structure**

Field	Field Name	Type	Width	Description†
1	INCIDENTNO	Character	5	The number assigned to each fire incident chronologically.
2	STATE_TOWN	Character	35	The state and town in which the plant is located.
3	PLANT_UNIT	Character	30	The plant name and unit number where the fire occurred.
4	CAPACITY	Character	10	The reactor output, expressed in net megawatts (electric).
5	UTILITYPRN	Character	60	The principal utility that operates the plant.
6	REACTORTYP	Character	8	The type of reactor.
7	REACTORSUP	Character	35	The nuclear reactor supplier.
8	OL_ISSUED	Character	10	The issuance date of a reactor low power operating license.
9	INITIALCRT	Character	10	The date the nuclear reactor first went critical.
10	COMMEROPER	Character	10	The date the reactor was formally connected to a commercial power grid.
11	DATE	Date	8	The date of the fire.
12	TIME	Character	10	The time the fire occurred.
13	LOCATION	Character	40	The location of the fire.
14	LOC_TAB12	Character	40	The location assigned in the binning process.
15	DURATION	Character	10	The duration of the fire.
16	DUR_FLAG	Numeric	2	A number from 1 to 6 that corresponds to the time that a fire burned.
17	MODE_OPER	Character	40	The plant status at the time of the fire.
18	CAUSE_FIRE	Character	67	The cause of the fire.
19	TYPE_FIRE	Character	20	The type of fire that occurred in reference to NEPA/NFPA standards.
20	EXTINGUISH	Character	67	The persons, systems, or methods used to extinguish the fire.
21	DETC_MEANS	Character	67	The method by which the fire was initially detected.
22	SUPP_TIME	Character	10	The time taken to extinguish the fire once suppression personnel or equipment responded.
23	SUP_FLAG	Numeric	2	A number from 1 to 6 that corresponds to the time it took to suppress the fire.
24	AGENT_USED	Character	67	The extinguishing agents used to suppress the fire.
25	EQUIP_USED	Character	67	The equipment used to extinguish the fire.
26	INITCOMPN	Character	40	The equipment or item that initiated the fire.
27	INIT_TAB12	Character	40	The ignition source assigned in the binning process.
28	INITCOMBUS	Character	40	The substance that initiated the fire.
29	COMPEFFECT	Character	120	The equipment items affected by the fire.
30	POWERDEGRA	Character	10	The percentage power degradation of the reactor unit that resulted from the fire.
31	FORCEDOUTG	Character	10	The number of days of outage caused by the fire.
32	DIRECTLOSS	Character	15	The dollar value loss incurred because of the fire.
33	REFERENCE	Character	50	The source material in which the fire incident was documented.
34	EXT_SYS_F	Character	2	Did the extinguishing system fail?
35	UTL_UPD	Character	50	Utility response.

† For lists of the possible field entries, see Table A-1, Utility Questionnaire, in Appendix A of NSAC 178L<sup>32</sup>, except where otherwise noted.

**Table 2. U.S. Nuclear Reactor Operating Experience**

Plant Type	Reactor Years
PWR	785.67
BWR	478.59
Total	1264.27

**USING THE FIRE EVENTS DATABASE (FEDB)**

FEDB was created to supply EPRI member utilities with a generic data source to support fire protection engineers and fire risk analysts. For example, a fire risk analyst can calculate fire frequencies for specific locations and ignition sources using the fire events database. Each fire event has been assigned to one of a number of bins (see the LOC\_TAB12 and INIT\_TAB12 fields in Table 3) to calculate fire frequencies used by the FIVE methodology. Additionally, each bin characterizes the plant location and fire ignition source. A fire protection engineer might be interested in how fires in nuclear plants are detected and suppressed. The database shows that the overwhelming majority of fires are detected by plant personnel. Additionally, the database indicates that if a fire is detected by "Control Room Observation", it is suppressed approximately twice as fast as other fires.

**FIRE IGNITION FREQUENCY MODEL**

The FIVE methodology uses fire ignition source bins to develop estimates of plant-specific fire zone ignition frequencies. Each bin can also be used to characterize ignition locations and energetics. Each bin represents a set of operating experience events and every reported fire is assigned to a bin. The reactor operating years (the denominator for calculating frequency) was calculated from the commercial operating license issuance date through 1988, excluding HTGR experience. Total reactor years were evaluated for each area, e.g., PWR Auxiliary Building, Battery Room or Radwaste Area.

**FIRE IGNITION FREQUENCY METHOD**

A fire ignition frequency method was developed that better recognizes plant to plant and fire area to fire area differences. It achieves this by identifying a set of components which are likely to cause fires, but whose location(s) often varies among plants. Battery chargers and RPS MG sets are examples of these components. In some plants, these ignition sources are located in important locations such as cable spreading rooms.

Some of these "plant-wide" ignition sources are unlikely to be in safety related areas, but may be in an important building, e.g., elevator motors. In older approaches, these fires would be "apportioned" to important areas based on the amount of combustibles present when, in reality, it was impossible such an ignition source could be present in a fire area containing safe shutdown equipment.

The EPRI method also uses more locations for determining electrical cabinet and pump fire frequencies. This increased number should also improve the accuracy of the ignition frequency. The database and the resulting method clears up the confusion regarding assigning fires to a reactor building. PWR reactor buildings are often primary containment and BWR reactor buildings are often secondary containment. Locating fires by the location "reactor building" can be misleading. The EPRI approach bins fires by "BWR reactor building" and by containment.

Finally, the method apportions the number of fires by the number of units at a site as well as the number of buildings. Past approaches have assumed that each "typical" location in every plant contained the same number of ignition sources regardless of whether there was more than one unit or one location. But the amount of equipment in a location varies from plant to plant. A dual unit site may have two units worth of electrical buses in single 4160V and 480V switchgear rooms, while a single unit site may have one unit's worth equipment in four rooms.



The EPRI method currently uses the assumption that the amount of equipment is equal among units. While this assumption is not perfect, it is believed to be better than that previously used. This assumption is believed to be most accurate for safety related equipment, whose total numbers are controlled more by regulation. Safety related equipment ignition sources are most likely to be in places containing safety related power and control circuits. A summary of the method is presented in Table 3.

Table 3. Fire Ignition Sources And Plant Location

Plant Location	Fire Ignition Source	Ignition Source Weighing Factor Method
Auxiliary Building (PWR)	Electrical cabinets	B
	Pumps	B
Reactor Building (BWR)	Electrical cabinets	B
	Pumps	B
Diesel Generator Room	Diesel generators	A
	Electrical cabinets	A
Switchgear Room	Electrical cabinets	A
Battery Room	Batteries	A
Control Room	Electrical cabinets	A
Cable Spreading Room	Electrical cabinets	A
Intake Structure	Electrical cabinets	A
	Fire Pumps	A
	Others	A
Turbine Building	T/G Excitor	B
	T/G Oil	B
	T/G H Hydrogen	B
	Electrical cabinets	B
	Other pumps	B
	Main feedwater pumps	A
	Boiler	B
Radwaste Area	Miscellaneous components	A
Transformer Yard	Yard transformers (propagating to Turbine Building)	A
	Yard transformers (LOSP)	A
	Yard transformers (Others)	F
Plant-Wide Components	Fire protection panels	F
	RPS MG sets	F
	Non-qualified cable run	E
	Junction box/splice in non-qualified cable	E
	Junction box with qualified cable	E
	Transformers	F
	Battery Chargers	F
	Off-gas/H <sub>2</sub> Recombiner (BWR)	G
	Hydrogen Tanks	G
	Misc. Hydrogen Fires	C
	Gas Turbines	G
	Air Compressors	F
	Ventilation Subsystems	F
	Elevator motors	F
	Dryers	F
	Transients	D
	Cable fires caused by welding	C
	Transient fires caused by welding & cutting	C

### TABLE 3 NOTES : IGNITION SOURCE WEIGHTING FACTOR METHOD

Zone specific ignition sources should be verified with a walkdown. Values can be estimated using methods other than direct counting, including engineering judgment. Based on experience, estimated values within about 25% can be used.

- A No ignition source weighting factor is necessary.
- B Obtain the ignition source weighting factor by dividing the number of ignition sources in the fire compartment by the number in the selected location.
- C Obtain the ignition source weighting factor by calculating the inverse of the number of compartments in the locations. Exclude any areas contained in locations other than in this table.
- D Obtain the ignition source weighting factor by summing the factors for ignition sources which are allowed in the zone and dividing by the number of zones in the locations in this table. For example, if cigarette smoking is prohibited do not include the cigarette smoking factor in the calculation. The factors are:
 

• Cigarette Smoking	2
• Extension Cord	4
• Heater	3
• Candle	1
• Overheating	2
• Hot pipe	1

Overheating addresses errors while heating potential combustibles, e.g., battery terminal grease.
- E Obtain the ignition source weighting factor by dividing the weight (or BTUs) of cable insulation in area by the total weight (or BTUs) of cable insulation in Appendix R fire areas, not including fire areas in either the radwaste area or the containment. Cable insulation weights (or BTUs) are provided in Appendix R combustible loading. (Junction boxes and splices are assumed to be distributed in proportion to the amount of cable.)
- F Obtain the ignition source weighting factor by dividing the number of ignition sources in the fire area by the total number in all the locations in this table.
- G Obtain the ignition source weighting factor by dividing the number of ignition sources in the fire area by the total number in all plant locations, including locations that were not specified in this table.

### FIRE EVENTS DATA SYNOPSIS

NSAC-178L<sup>32</sup> contains a synopsis of the fire events experience which is organized by the fire ignition source bins used in the above-mentioned method. The synopsis identifies a number of potential conservatisms in the fire ignition frequencies which are determined by including every event in the database. The report states the number of fires which have occurred early in plant life, e.g., before the first year of commercial operation is complete. During this "infancy" or "burn in" period an increased fire frequency is seen for many fire types. Control room fires are a notable example.

The report also identifies when a potential exists for so-called recurring fires, that is, fires occurring over a short time period due to the same cause. The root cause may not be applicable to the plant in question, or it may be identified and repaired at other plants due to knowledge gained from the first plant's experience. Consequently, it is conservative to count such recurring fires for a generic calculation. Indeed, the control room ignition frequency used in the NUREG-1150 fire analyses<sup>23,24</sup> is based on three fires instead of four because a recurring fire condition was identified. This condition, along with others, is identified in this report.

Finally, the report identifies self-extinguishing fires and fires suppressed solely by de-energizing the ignition source. These fires are conservatively counted in the fire ignition source frequency, but identified in the report for the user to consider them more realistically in an evaluation of vulnerabilities. The synopsis in NSAC-178L<sup>32</sup> also describes interesting or unique fire events and trends or root causes where they could be identified from the source information.

Another focus of the synopsis is the suppression and detection means used for the fire events and the associated suppression times and fire durations. The number of fires suppressed by different means and the range of fire durations are noted for each ignition bin. The evidence from the database indicates that the difficulty in suppressing fires is related to the ignition source involved. Further, the longest duration fires occur in components less likely to be located in areas containing safe shutdown equipment and, therefore, less likely to be significant in a severe accident fire risk assessment (e.g., the turbine generator, charcoal filters, station transformers, hydrogen storage tanks, etc.).

## EXAMPLE FIRE BIN SYNOPSIS

### Control Room Fires

Twelve electrical cabinet fires occurred. Two of the fires occurred between issuance of the operating license and the date of commercial operation. One fire occurred in the first year of commercial operation. These three fires indicate a probable "infancy period".

The ignition frequency model is based on panel fires. The single kitchen fire is counted as a panel fire for ease of implementation. The fire ignition frequency is  $9.5E-3$  per reactor year. Because no control room fires were considered in plant-wide component bins, this frequency is directly comparable to other data sources.

The sources of electrical cabinet fires are distributed evenly among plant types except for two fires occurring at a single plant over a few days. These two fires have been classified as recurring fires by SNL in the NUREG-1150 fire PRAs. We endorse this conclusion. Seven fires occurred at BWRs, and five fires occurred at PWRs.

Each fire was manually suppressed. The means for suppression were as follows:

- 1 de-energized
- 5 portable extinguishers
- 1 none (fire went out of its own accord)
- 5 unknown

Fire duration times ranged from 30 seconds to five minutes for six of the events. No time period was reported for the others; however, one was reported to have been "quickly extinguished", one was characterized as "relatively small", and the two other event descriptions did not imply a fire of significant severity.

## SELECTED IMPORTANT INSIGHTS

In the FEDB, three control room fires occurred before the end of the first year of commercial operation, indicating an "infancy period" is probable for control room electrical cabinet fires. Also, two of the fires are considered recurring fires. Traditionally, and in the NUREG-1150 studies, these fires may be counted as a single event. Finally, one of the fires was a kitchen fire. It is not representative for electrical cabinet fire scenarios. Consequently, five of the twelve control room fires, nearly one half, could be inapplicable to a generic control room fire frequency calculation for commercial operation, irrespective of considering the severity and length of the fire. If these fires are omitted, the fire frequency for a single unit site is roughly twice the frequency predicted in NUREG/CR-4840<sup>35</sup> and used in the NUREG-1150 studies. As the attempt to capture as complete a fire experience as possible progressed, it is noted that the frequency of fires increased and fire severity decreased. This is generally because less severe fires may not have been considered in earlier fire event databases.

The NUREG-1150 fire risk studies of Peach Bottom<sup>24</sup> and Surry<sup>23</sup> indicate that the control room is one of the dominant locations for core-damage frequency due to fires. The principal cause of NUREG-1150's control room core-damage frequency was the need to

evacuate the control room and shutdown the plant from the remote shutdown panel. NUREG-1150 used a frequency of control room fires of  $4.4 \times 10^{-3}$  /year. Sandia guessed that one in ten fires would result in enough smoke to cause evacuation of the control room, resulting in a frequency of serious fires of  $4.4 \times 10^{-4}$  /year. The EPRI fire event database has 12 control room fires, all of which were relatively minor. If the next control room fire results in enough smoke to cause evacuation of the control room, then a Chebyshev upper bound 95% confidence limit using the EPRI database would be one in thirteen rather than one in ten guessed by Sandia. Neither this estimate nor the Sandia estimate can be technically justified. Sandia was at a serious disadvantage in having extremely sparse data, but recognized that not every fire is a serious fire. This experience is one demonstration of the need to continue to update the EPRI database, since the Chebyshev upper bound 95% confidence limit is also based on sparse data, and is not technically satisfactory. Thus, the conditional probability of a serious fire, given a control room cabinet fire, is less than the 0.077 Chebyshev upper bound 95% confidence limit rather than the Sandia guessed 0.1. Further data is expected to continue to lower this number, though to what degree cannot be predicted.

More importantly, in the seven control room fire events that reported fire event duration information, all seven fire durations and suppression times indicated that control room suppression would occur quickly as a function of time. EPRI has published a human reliability model<sup>33</sup> for predicting the time and probability of actions performed in the control room based on observed times to perform them. A companion study<sup>34</sup> applied this model and the FEDB data to control room electrical cabinet fires. That study found that the probability of suppressing an electrical cabinet fire before smoke obscured the control boards was roughly a factor of thirty lower than Sandia's guess of one in ten. The EPRI Fire PRA Requantification Studies<sup>34</sup> determined that the probability of obscuring the main control board was  $4.5 \times 10^{-5}$  /yr. for a single unit plant.

The FEDB experience does indicate that some smoke can enter the control room from fires in other ignition source areas. Smoke was smelled in the control room in three ventilation system fires. However, based on the event descriptions in the database, these fires did not appear to result in a significant amount of smoke accumulation in the control room. The suppression times reported for two of the three events indicated only minor fires, i.e., only one and two minutes.

Containment fire experience is also worth noting. Most containment fires appear to be inapplicable to an IPEEE. The fires did not occur at power and the trend in fire frequency has been markedly down. Twenty two of the thirty five fires occurred during shutdown or pre-operational testing. Fourteen of the thirty five fires were reactor coolant pumps fires. Twelve of these occurred in 1980 or earlier. The remaining two occurred at the same plant within two years, an indication of a potential recurring fire condition. The reduction in RCP fires is probably due to design and operating changes taken to reduce the frequency of these fires, including and especially lube oil control measures.

Lastly, the information in FEDB provides the basis for sanity checks of fire propagation and damage predictions using analytical codes. The uncertainty in the COMPBRN code<sup>36</sup>, the principal tool used in past FPRAs, has been noted in the Fire Risk Scoping Study<sup>22</sup> and in the EPRI Fire Risk Requantification Studies<sup>34</sup>. One example insight that could be drawn from the database include the number and types of fire ignition sources causing damage to other equipment.

A review of the electrical cabinet fires in the database indicated that it is unlikely that an electrical cabinet fire would damage other equipment. Of the more than one hundred such fires, only one might have caused damage based on the event description and the source information. In that event, the additional buses lost appear more likely to be as a consequence of the electrical failure rather than the fire itself.

## SUMMARY

The FEDB has proven a useful source of information for a fire risk and other analysis. The ignition frequency method is identical with the method used in FIVE<sup>5</sup> and EPRI's Fire PSA Method<sup>37</sup>. The event experience for deluge and pre-action systems is the primary source of reliability information for these systems. No other source was found to be as complete in a review of public domain information for suppression system reliability<sup>32</sup>.

Reviews of the event experience for selected ignition sources or for specific issues can provide valuable insights and sanity checks. Fire risk analysts and fire protection engineers can use the information contained in the FEDB to focus more quickly on the dominant causes of fire risk and, having done so, perform a more realistic analysis as well. The EPRI Fire Events Database is the most complete fire events database available for nuclear power plants known to the authors.

Future uses of the database include: (a) performance based regulation, (b) improved (less bounding) fire risk studies, (c) cost-effective fire protection programs, (d) fire brigade training guidance, and (e) insurance and fire detection/suppression system optimization.

EPRI has formed the EPRI Fire Data Exchange (EFDE), whose goals include (a) updating the FEDB annually based on member contributed information, U.S. Nuclear Regulatory Commission Licensee Event Reports, and other public sources; (b) accumulating data for utility nuclear and non-nuclear facilities; and (c) analyzing the data for insights and historical trends. The EPRI Fire Data Exchange (EFDE) will consider eventual expansion to cover detection and suppression system operational and testing data, and data to allow members to better focus their fire protection resources to be as cost effective as possible, while ensuring safety of personnel and property. Advice to EPRI on the future technical direction will be provided by an EFDE Steering Committee, which will consist of Exchange member representatives.

## REFERENCES

1. U.S. Nuclear Regulatory Commission, Individual Plant Examination for Severe Accident Vulnerabilities - 10CFR50.54(f), Washington, D.C.: November 23, 1988. Generic Letter No. 88-20.
2. U.S. Nuclear Regulatory Commission, Individual Plant Examination: Submittal Guidance, Final Report, Washington, D.C.: Government Printing Office, August 1989. NUREG-1335.
3. U.S. Nuclear Regulatory Commission, Individual Plant Examination of External Events for Severe Accident Vulnerabilities, 10CFR50.54(f), Washington, D.C.: June 28, 1991. Generic Letter 88-20, Supplement 4.
4. U.S. Nuclear Regulatory Commission, Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, Washington, D.C.: Government Printing Office, June 1991. NUREG-1407.
5. Fire-Induced Vulnerability Evaluation (FIVE) Methodology Plant Screening Guide, Professional Loss Control, Palo Alto, CA: Electric Power Research Institute, April 1992. EPRI TR-100370.
6. Brunswick Steam Electric Plant Probabilistic Fire Analysis, EI Services, Kent, Washington, December 1987.
7. Indian Point Probabilistic Safety Study, Section 7, Power Authority of the State of New York and Consolidated Edison Company of New York, Inc., March 1982.
8. Severe Accident Risk Assessment - Limerick Generating Station, Chapter 4, Main Report, Philadelphia Electric Company, Report #4161, April 1983.
9. Seabrook Station Probabilistic Safety Assessment, Section 9.4, Public Service Company of New Hampshire and Yankee Atomic Electric Company, December 1983.
10. Oconee PRA - A Probabilistic Risk Assessment of Oconee Unit 3, Section 9.3, Palo Alto, CA: Electric Power Research Institute, Nuclear Safety Analysis Center, June 1984. NSAC-60.

11. Major Common-Cause Initiating Events Study - Shoreham Nuclear Power Station, NUS Corporation, February 1985. NUS-4617
12. W.R. Crammond, D.M. Ericson, Jr., and G.A. Sanders, Shutdown Decay Heat Removal Analysis of a Westinghouse 2-Loop Pressurized Water Reactor - Case Study, Washington, D.C.: Government Printing Office, March 1987. NUREG/CR-4458. Sandia National Laboratories, SAND86-2496.
13. W.R. Crammond, D.M. Ericson, Jr., and G.A. Sanders, Shutdown Decay Heat Removal Analysis of a Babcock and Wilcox Pressurized Water Reactor - Case Study, Washington, D.C.: Government Printing Office, NUREG/CR-4713, March 1987. Sandia National Laboratories, SAND86-1832.
14. W.R. Crammond, D.M. Ericson, Jr., and G.A. Sanders, Shutdown Decay Heat Removal Analysis of a Combustion Engineering 2-Loop Pressurized Water Reactor - Case Study, Washington, D.C.: Government Printing Office, August 1987. NUREG/CR-4710. Sandia National Laboratories, SAND86-1797.
15. W.R. Crammond, D.M. Ericson, Jr., and G.A. Sanders, Shutdown Decay Heat Removal Analysis of a General Electric BWR3/Mark 1 - Case Study, Washington, D.C.: Government Printing Office, March 1987. NUREG/CR-4448. Sandia National Laboratories, SAND85-2373.
16. W.R. Crammond, D.M. Ericson, Jr., and G.A. Sanders, Shutdown Decay Heat Removal Analysis of a General Electric BWR4/Mark 1 - Case Study, Washington, D.C.: Government Printing Office, August 1987. NUREG/CR-4767. Sandia National Laboratories, SAND86-2419
17. W.R. Crammond, D.M. Ericson, Jr., and G.A. Sanders, Shutdown Decay Heat Removal Analysis of a Westinghouse 3-Loop Pressurized Water Reactor - Case Study, Washington, D.C.: Government Printing Office, March 1987. NUREG/CR-4762. Sandia National Laboratories, SAND 86-2377.
18. A Methodology for Risk Assessment of Major Fires and Its Application to an HTGR Plant, K. Fleming, W.J. Houghton, and F.P. Scaletta, San Diego, CA: General Atomic Company, 1979. GA-A15402
19. Nuclear Power Plant Fire Loss Data, K.W. Dungan and M.S. Lorenz, Palo Alto, CA: Electric Power Research Institute, July 1983. EPRI NP-3179
20. Auxiliary Power and Control Code of Federal Regulations 10-CFR Part 50. Appendix R-Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979, Federal Register, Volume 45, Number 105, May 29, 1980.
21. W.T. Wheelis, User's Guide for a Personal-Computer-Based Nuclear Power Plant Fire Data Base, Washington, D.C.: Government Printing Office, August 1986. NUREG/CR-4586. Sandia National Laboratories, SAND86-0300.
22. J.A. Lambright, S.P. Nowlen, V.F. Nicolette, and M.P. Bohn, Fire Risk Scoping Study: Current Perception of Unaddressed Fire Risk Issues, Washington, D.C.: Government Printing Office, December 1988. NUREG/CR-5088. Sandia National Laboratories, Albuquerque, NM, SAND88-0177.
23. M.P. Bohn, J.A. Lambright, S.L. Daniel, J.J. Johnson, M.K. Ravindra, P.O. Hasimoto, M.J. Mraz, W.H. Tong, Analysis of Core Damage Frequency: Surry Power Station. Unit 1 External Events, Washington, D.C.: Government Printing Office, December 1990. NUREG/CR-4550, Vol. 3, Rev. 1, Part 3. Sandia National Laboratories, Albuquerque, NM, SAND86-2084.

24. J.A. Lambright, M.P. Bohn, S.L. Daniel, J.J. Johnson, M.K. Ravindra, P.O. Hasimoto, M.J. Mraz, W.H. Tong, D.A. Brosseau, Analysis of Core Damage Frequency: Peach Bottom, Unit 2 External Events, Washington, D.C.: Government Printing Office, December 1990. NUREG/CR-4550, Vol.4, Rev. 1, Part 3. Sandia National Laboratories, Albuquerque, NM, SAND86-2084.
25. Daily Plant Status Reports (DPSR). A computer listing of reports from 1985 through 1988 containing the keyword "fire" obtained from N. Dietrich, NSAC, 1989.
26. R. Kingsley House, President, Intermountain Technologies, Inc., memo to William Parkinson, SAIC, transmitting summary report data compiled for Dr. J.P. Sursock for EPRI project RP 2639-1, 1989.
27. Nuclear Power Experience, Stoller Power, Inc., December 1984.
28. "World List of Nuclear Power Plants," Nuclear News, August 1989, No. 10.
29. Loss of Offsite Power at U.S. Nuclear Power Plants - All Years Through 1989, H. Wyckoff, Palo Alto, CA: Electric Power Research Institute, April, 1990. NSAC-147.
30. M. Kaminski, A listing of fire events occurring during 1987 and 1988 obtained from J. Haugh (NSAC), 1989.
31. U.S. Nuclear Regulatory Commission, Information Notice 88-64, Reporting Fire in Nuclear Process Systems at Nuclear Power Plants, Washington, D.C.: August 18, 1988.
32. Fire Events Database for U.S. Nuclear Power Plants, W. Parkinson, G. Solorzano, B. Najafi, M. Marteeny, K. Bateman, Palo Alto, CA: Electric Power Research Institute, January 1993. EPRI NSAC-178L, Revision 1.
33. HRA Approach Using Measurements for IPE, A.J. Spurgin, P. Moieni, G.W. Parry, B.O.Y. Lydell, Palo Alto, CA: Electric Power Research Institute, December 1989. EPRI NP-6560L.
34. Fire PRA Requantification Studies, W. Parkinson, K. Bateman, D. Christensen, M. Marteeny, B. Najafi, Palo Alto, CA: Electric Power Research Institute, March 1993. EPRI NSAC-181.
35. Procedures for the External Event Core Damage Frequency Analyses for NUREG-1150, Sandia National Laboratories, Washington, D.C.: U.S. Nuclear Regulatory Commission, November 1990. NUREG/CR-4840.
36. COMPBRN III-E: An Interactive Computer Code for Fire Risk Analysis, V. Ho, S. Chien, G. Apostolakis of UCLA, Palo Alto, CA: Electric Power Research Institute, May 1991. EPRI NP-7282.
37. Fire PRA Methodology, W. Parkinson, B. Najafi, et. al., Palo Alto, CA: Electric Power Research Institute, (to be published 1994).

**083 Environmental Restoration Decision Support System**

*Chair: D. Rice, LLNL*

**Application of Decision Support Systems to Environmental Restoration Processes**

*D.W. Rice, J. Ziagos (LLNL); D. Bell (UCLA)*

**The SEDSS - A Risk Assessment Based Decision Support Tool**

*R. Knowlton Jr., E. Webb (SNL)*

**Environmental Decision Support Systems**

*J. Coleman (USEPA); J. Franco, W. Wee (U. Cincinnati)*



## APPLICATION OF DECISION SUPPORT SYSTEMS TO ENVIRONMENTAL RESTORATION PROCESSES

David W. Rice, Jr.,<sup>1</sup> David Bell,<sup>2</sup> and John Ziagos<sup>1</sup>

<sup>1</sup>Lawrence Livermore National Laboratory  
P.O. Box 808, MS L-619, Livermore, CA 94550  
(510) 423-5059 FAX (510) 422-9203

<sup>2</sup>UCLA  
Los Angeles, CA

### INTRODUCTION

The reduction of public health risk due to potential exposure of environmental contaminants is the prime reason for environmental restoration (ER) remedial actions. The potential cost of nationwide ER is enormous. Therefore, there is a great need to (1) identify the types and levels of effort that are appropriate to reducing both the public health risk and the uncertainty associated with the risk and (2) increase the benefit/cost ratio of the ER effort to prevent unnecessary expense. Environmental Decision Support Systems (EDSSs) provide a means to meet these needs.

Decision makers dealing with environmental issues often are required to integrate enormous amounts of data of very different types. Important information may be buried in vast amounts of unproductive data. Photos, maps, technical articles, newspaper clippings, modeling results, tabular chemical data, sensor data, etc., must be integrated with decision making tools, such as budget estimations, risk evaluations, and decision analysis. The flood of data available may lead to "analysis paralysis."

High performance networks will contribute to the data flood that could inundate ER decision makers but will also provide needed tools to find solutions to ER problems. Currently, the High Performance Computing Act provides for the creation, by 1996, of a National Research and Education Network (NREN), which will run at least 1 million bits a second, and will connect millions of Federal, academic, business, and other users. This effort will vastly expand the capability of the present Internet, which was created over 20 years ago.

Decisions are often made during ER activities or the enactment of laws without using the available data or performing rudimentary cost-benefit analyses. Since much of the data is located in distributed data bases and the retrieval, visualization, and interpretation of the data are slow and inefficient, the information is not used. This is because the decisions are often time-urgent and the needed analysis is computationally complicated and requires long lead times.

New network and software technologies are encouraging the development of a new class of computer software systems to support decision making processes. Decision Support Systems (DSSs) link sophisticated graphical user interfaces, data sources, and computational and modeling tools into an integrated system to make decisions and solve time-urgent problems.<sup>1</sup>

## ELEMENTS OF DECISION SUPPORT SYSTEMS

Conventional software can be characterized as dealing with repetitive, highly structured problems in an automated fashion. Procedures where there is a well-defined series of information processing steps, such as payroll and inventory, are suited for conventional software approaches. DSSs, on the other hand, are aimed at the less well-structured, underspecified problems that managers dealing with environmental issues typically face.<sup>2,3</sup> An Environmental DSS (EDSS) will allow ER decision makers to examine and approach nonroutine, nonrepetitive problems that do not have an established approach that are typical to the ER process.<sup>4</sup>

At the heart of DSSs is application management software that links distributed DSS tools. The problems in realizing the full potential of distributed DSSs are the software and connection issues that must be resolved. A wide variety of commercial, public domain, and "home grown" computational tools are available as elements to DSSs. The "glue" to link applications and allow casual users to access these applications and to pass data between them is a critical element of EDSSs. These application managers (the glue) need further development.

## APPLICATIONS OF ENVIRONMENTAL DECISION SUPPORT SYSTEMS

A hypothetical cost-versus-cleanup model loosely based on the environmental cleanup experience at Lawrence Livermore National Laboratory (LLNL) illustrates the potential applications of EDSSs to the ER process. The model assumes a contaminant plume of volatile organic compounds in ground water that is remediated over the course of 50 years, using pump and treat technologies. The overall effort for a single ER project is often divided into the following two phases: uncertainty reduction and engineering processes (Figure 1a).

The major reduction in contaminant risk uncertainty comes a few years prior to start of cleanup. During this phase, characterization of the spatial distribution of contaminants, relative to the hydrogeochemical characteristics controlling fate and transport, is performed. The cost of uncertainty reduction is small compared to the eventual costs of the engineering processes phase of remediation.

The fastest cleanup occurs during the engineering processes phase and spans the 5- to 15-year period following the uncertainty reduction or characterization phase. Typically, during pump and treat remediation, 50% of the total costs are spent to clean up the last few percentages of contamination. Once the engineering processes phase has removed the major mass of contamination, the period of natural processes or enhanced natural processes should begin (Figure 1b). During this final phase of remediation, additional pumping to remove mass is not cost effective, and natural processes, either biotic or abiotic, should be relied upon to reach cleanup goals. In the illustrated example, about half the total cost of the cleanup can be saved by choosing a natural processes phase when mass removal is no longer cost effective.

During cleanup, an EDSS would be used by ER decision makers to evaluate the impact of collected data on the uncertainty of critical decision-making parameters, evaluate various remedial alternatives, implement optimized remedial designs, continuously perform cost/benefit analysis, and gain acceptance of remedial decisions from multiple stakeholders.

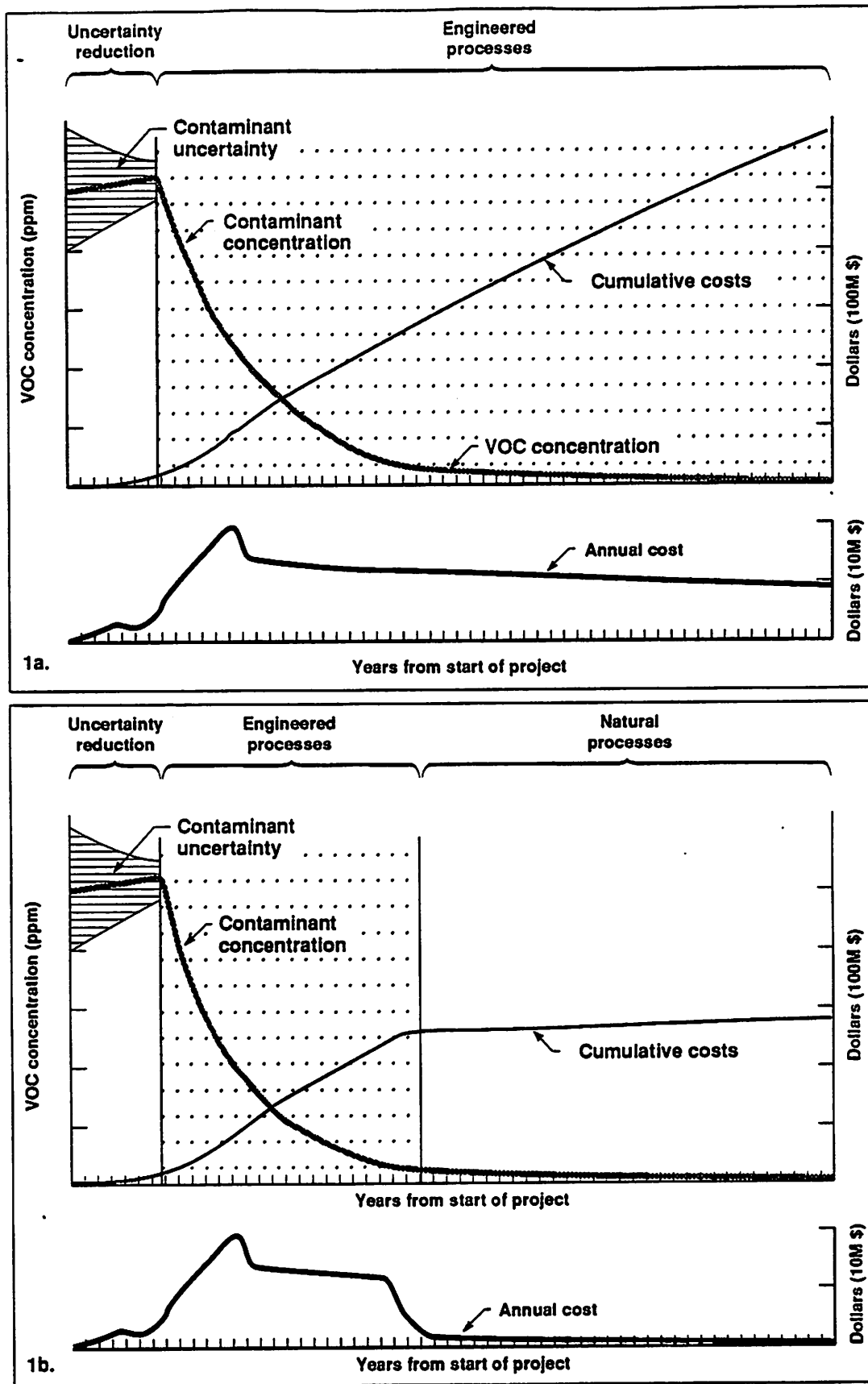


Figure 1. Hypothetical cost vs cleanup curves.

a. Base case: total pumping time is 50 years; stop pumping at 5 ppb.

b. Alternative approach: total pumping time is 17 years; stop pumping at 200 ppb.

During the observational approach to characterization, data quality objectives are established to know "when enough is enough" during characterization.<sup>5</sup> When the collection of additional data begins to have a marginal impact on uncertainty reduction or the remedial decisions at hand, further collection of data is unwarranted. EDSS proved a means to rapidly and repeatedly statistically evaluate the impact on risk uncertainty that additional data provide. EDSSs are used to site borehole locations, develop sampling plans, and visualize the impact that data may have on conceptual models of the site.

Another important use of EDSSs is to allow decision makers to balance the costs of further characterization against the reduced engineering costs during cleanup design and construction that more characterization information may provide. Significant ER cost reductions may be realized because unnecessary characterization would be reduced and the characterization performed would be focused on parameters critical to risk evaluation, remedial design and construction, and the natural processes to be relied upon during the final phase of the project.<sup>6</sup> EDSSs allow the timely calculation of risk uncertainty so that when the uncertainty has been reduced below a reasonable level, the ER managers can either change techniques or reduce the level of activity. Critical contaminant transport parameters used during risk assessment are identified, and an EDSS feedback system is developed that continually evaluates the uncertainty associated with these parameters. Figure 2 illustrates the structure of an EDSS being prepared by LLNL to implement optimized pump and treat ground water remediation.

During the implementation of pump and treat remedial alternatives, significant cost savings can be realized if engineering processes are stopped when they are no longer cost effective and natural processes are relied upon. An EDSS would help balance the cost of operating the cleanup system against any public health benefit of continued operation during the extended years of contaminant mass removal.

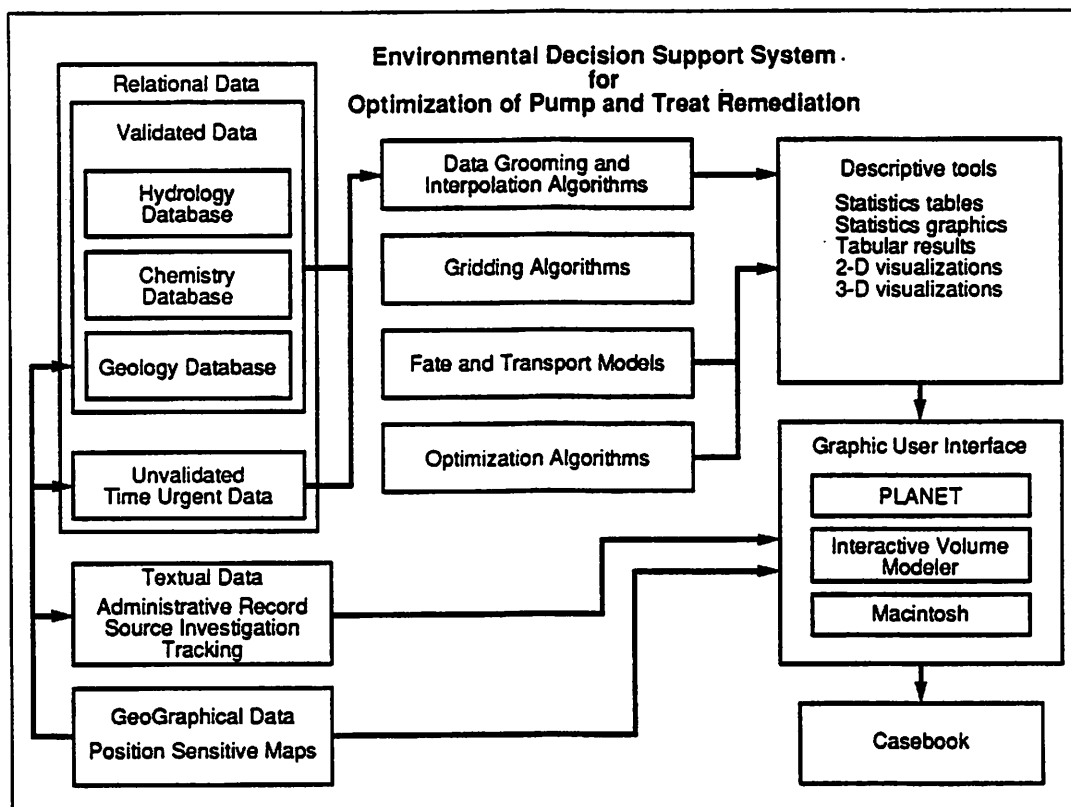


Figure 2.

As ER enters each of the three cleanup phases, critical issues change for each of the multiple stakeholders participating in the decisions. In general, there are three general categories of stakeholders. Those stakeholders whose primary issues center about reducing the actual risk due to potential contaminant exposure, those stakeholders primarily concerned with a perceived risk of potential exposure,<sup>7</sup> and those stakeholders primarily concerned with the amount of money expended during the reduction of potential risk. Each of these three general groups is also concerned to some lesser degree with the issues important to the other two groups. It is important to understand the utility of decisions to each stakeholders group and the outcome that each group expects from the ER effort. This knowledge should be used to gather and communicate information to gain acceptance for cleanup decisions that will increase the benefit/cost ratio of the ER effort and prevent unnecessary expense.

The EDSS graphic user interface is a critical component in the communication of predictive modeling results. The use of graphic EDSS tools to explore "what-if" scenarios, communicate conceptual models, contaminant distributions, modeling predictions, and involve multiple stakeholders in remedial alternative selections is critical to ER decision making processes. A user-centered design strategy can be employed that permits stakeholders to participate from day one, facilitates the identification of stakeholder issues, and gains acceptance of selected remedial alternatives.

The hypothetical model indicates that the decision to stop pumping and allow natural processes to complete the remediation is one of the most cost effective decisions possible during the remedial process. This decision involves the participation from regulatory, budgetary, and community stakeholders. The decision will be based to a large degree on the acceptance of the predictive contaminant fate and transport modeling performed to evaluate potential exposure risk and to implement a remedial design.<sup>8</sup>

EDSSs facilitate the communication of conceptual models and visualization of "what if" scenarios.<sup>9</sup> Typically, a greater amount of a managed risk is tolerated compared to a risk perceived as unmanaged. If the modeling is viewed as being unrepresentative or inaccurate, then stringent cleanup targets will typically be imposed. If cleanup managers understand early in the remedial process the criteria that are critical to gain acceptance of the predictive modeling, then money spent to gather data to validate models and meet stakeholder acceptance criteria will lead to higher allowed cleanup levels and greater cost savings. EDSSs used in this manner have been shown to gain acceptance of remedial alternatives that saved over \$100 million at one site.

## SUMMARY

Even when optimized, ER methods take a long time and are costly. EDSSs can be applied to the evaluation of alternative methods that reduce the time of the engineering phase and place greater reliance on natural processes. EDSSs will also help balance the cost of continued operation of the cleanup system against the derived public health benefit during the period of extended mass removal. EDSSs are a valuable tool to identify and balance multiple stakeholder concerns and gain acceptance for ER decisions. Finally, ER decision makers that use EDSSs would have an audit trail, and a better awareness of the actual cost for a given amount of public risk averted during cleanup.

Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under contract No. W-7405-ENG-48.

## REFERENCES

1. C. J. Newell, J. F. Haasbeek, and P. B. Bedient, OASIS: A Graphical Decision Support System for Ground-Water Contaminant Modeling, *Groundwater*, 28(2):224 (1990).
2. G. A. Gorry and M. S. Scott-Morton, A Framework for Management Information Systems, *Sloan Management Review*, pp 55-70 (1971).
3. R. H. Sprague and E. Carlson. "Building Effective Decision Support Systems," Prentice Hall, New York (1982).
4. G. Guariso and H. Werthner. "Environmental Decision Support Systems," E. Horwood Ltd., and J. Wiley and Sons, New York (1989).
5. W. A. Wallace, New Paradigms for Hazardous Waste Engineering, *Remediation*, Autumn: 419 (1991).
6. W. K. Tusa, Reassessing the Risk Assessment, *Civil Engineering*, March: 46 (1992).
7. T. E. McKone and K. T. Bogen, Predicting the Uncertainties in Risk Assessment, *Environ. Sci. Technol.* 25 (10): 1674 (1991).
8. J. V. Mitchell, Perception of Risk and Credibility at Toxic Sites, *Risk Analysis* 12 (1):19 (1992).
9. T. Rhyne, M. Bolstad, P. Rheingans, L. Petterson, and W. Shackelford, Visualizing Environmental Data at the EPA, *IEEE Computer Graphics and Applications*, March: 34 (1993).

## **THE SEDSS - A RISK ASSESSMENT BASED DECISION SUPPORT TOOL**

**Robert Knowlton, Jr.<sup>1</sup> and Erik Webb<sup>2</sup>**

**<sup>1</sup>Environmental Restoration Program, Dept. 7583**

**<sup>2</sup>Safety and Risk Assessment Department, Dept. 6331**

**Sandia National Laboratories  
Albuquerque, New Mexico 87185**

### **ABSTRACT**

The Sandia Environmental Decision Support System (SEDSS), a public-domain software package, is being developed to aid site owners, operators, and government regulators in quantitatively defining environmental restoration (ER) and waste management decisions. Most environmental decision makers face similar issues such as determining the potential for contaminant release and migration from a site, quantifying associated health and environmental risks, selecting and optimizing remediation schemes, and developing monitoring programs to either ensure regulatory compliance or determine that specified cleanup goals have been accomplished.

Additionally, site characterization and monitoring plans, historically developed through a subjective process, must provide a quantitative description and the level of confidence a decision maker has in calculations of risk. Questions that can be quantitatively addressed for both environmental restoration and waste disposal activities under this type of risk-based framework include:

- What is the environmental and human-health risk associated with a disposal or restoration site?
- How many monitoring wells are enough and where should they be placed?
- How many environmental samples are needed to characterize a site?
- What are the costs/benefits/risks associated with either the cleanup alternatives for an ER site or the alternative engineering designs for a waste disposal site?

Sandia has developed an approach to solving these problems based on extensions of Probabilistic Risk Assessment (PRA) techniques developed for the U.S. Nuclear Regulatory Commission programs in high and low-level waste disposal. The approach is based on interactive development and testing of assumptions about a particular site; statistical and geostatistical characterization of data and parameters that describe the site conditions; physical modeling of environmental transport of hazardous components; and optimization techniques for processing model results to aid in decision making. Because the SEDSS is based on physical modeling, rather than straight statistics and data display, it is distinct from most other decision support tools

currently under development.

The SEDSS is designed to be adaptive and user-friendly. It has a built-in Geographic Information System (GIS) for data storage, display, and manipulation. From a Sun workstation, the user interacts with the Graphical User Interface (GUI), which handles all interactions with the GIS data base and the process models. In addition, the SEDSS is being ported to a PC working environment, and later to a Macintosh version.

The GUI interfaces the process models (e.g., transport code) through an applications manager, which has a number of options for supplying information to a decision maker. The applications manager has modules for:

- regulatory framework
- site ranking,
- site characterization,
- monitor-well network optimization,
- risk assessment, and
- remedial alternatives and design.

The regulatory framework module is designed to allow the user to track the decision making process within a given regulatory driver. For instance, the user could track the RCRA process flow (e.g., RFI, CMS, CMI) or the CERCLA/Superfund process flow (e.g., RI/FS). The regulatory process flows are concerned with three basic steps in the decision-making process:

- Is the site safe?
- What remedial alternative(s) should be used?
- When is the remediation effort complete?

The regulatory framework option allows the user to access all appropriate modules for site characterization, risk assessment, remedial design, etc., the same as if these options were chosen independently, but these modules are accessed within the regulatory process flow when needed to supply information in the regulatory decision-making process. It should be noted that the modules (e.g., site characterization) do not differ significantly whether accessed separately or through the regulatory framework option because the basic methods stay the same, it's the point of access that differs. Most of the quantitative decision-making that is done is based on risk assessment and the application of uncertainty analysis techniques. Wherever possible, the uncertainties are quantified through the use of Monte Carlo methods, and priorities established through sensitivity analysis techniques.

The SEDSS will permit site managers and/or regulators to investigate decisions with respect to alternative designs. The system will track and document the decisions made by the user and allow for the communication, identification, and resolution of differences between site owners and regulators. This openness will help both parties take effective and efficient remediation action.

This work is sponsored by:

- DOE's Office of Environmental Restoration, through Sandia National Laboratories Environmental Restoration Program,
- DOE's Office of Technology Development, through the Mixed Waste Landfill Integrated Demonstration Project
- NRC's Low-Level Radioactive Waste Research Branch, Headquarters
- EPA's Office of Superfund and Radiation Programs, Headquarters

This technology can be transferred to the private sector for general use on RCRA, CERCLA, and waste management sites. This activity has already begun with companies that specialize in geographic information systems and the display of geologic data.

## INTRODUCTION

A strong need exists for decision support systems in the Environmental Restoration (ER) and Waste Management (WM) arenas. ER is generally responsible for the assessment and cleanup of inactive waste and release sites. WM is generally responsible for the establishment of disposal facilities for current wastes. The two areas overlap in their responsibility to be protective of human



health and the environment. The ultimate performance measure for any of this work is a safe site, whether its safe to begin with, or it is made safe through remedial action or institutional control. In defining whether a site is safe, risk assessment methodologies become the cornerstone from which quantitative risk estimates are derived, and risk management decisions are made.

Decision support tools are necessary in ER and WM for the following reasons:

- to provide a framework for risk management decision making between responsible parties, stakeholders, and regulators;
- to standardize the approach and methodologies used in quantitative risk assessment;
- to provide a mechanism for documentation/justification of assumptions and data used in an analysis;
- to provide continuity of information between all steps in the assessment/remediation process;
- to provide quantitative information to site investigators (e.g., number of samples required, cost/benefit analyses); and
- to provide a user-friendly platform to perform these necessary analyses, one which is intuitive and streamlines the analyses compared with conventional approaches.

In the area of metrics (or rather methods to aid the decision making process), Sandia National Laboratories (SNL) has developed the Sandia Environmental Decision Support System, or SEDSS. The SEDSS is a software product designed to integrate all available information and data, to analyze and evaluate this data with process models and methodologies that quantify endpoints in the decision making process. Therefore the SEDSS is supplying information to answer the following fundamental decision-making questions:

- "How clean is clean?"
- "How many samples are enough?"
- "Is the monitoring well network adequate?"
- "What sites should be assessed first (that is, site ranking)?"
- "What is the potential impact of a site to human health and the environment?"
- "What are the cost/benefit/risk criteria for the selection of remedial alternatives?"

The SEDSS is a public domain software package designed for ease-of-use on a Sun workstation platform. It is modular by design, and therefore we can integrate any number of computer codes, or process models, into the SEDSS, depending on the users needs. The SEDSS has a built in Geographical Information System, or GIS, for data storage, display and manipulation. The process models imbedded in the SEDSS allow the use of methodologies in the decision making process that are based on the physics of contaminant transport as well as statistical methods. The fact that the SEDSS is based on physical modeling, rather than straight statistics and data display, sets it apart from most other decision support tools currently under development.

The SEDSS is distinct from other decision support tools in several other major areas, as well. First, conceptual model uncertainty is handled explicitly. The conceptual model uncertainty associated with a waste site is of utmost importance. The conceptual model represents a statement of the assumptions necessary to describe the physical characteristics of a site. The conceptual model is developed relative to a performance measure. The performance measure may be related to such criteria as the risk of a site (e.g., risk between  $10^{-4}$  and  $10^{-6}$ ) or the number of samples required to adequately assess the nature and extent of contamination (which then factors into risk). The SEDSS has a Conceptual Model Manager (CMM) which allows the user to define one or more conceptual models of their waste site. Alternative conceptual models may exist due to the uncertainty in the attributes of a waste site and the transport of contaminants away from that site. Multiple conceptual models formulate a basis for testing hypotheses about a site, and the site characterization priorities.

Conceptual model uncertainty formulates the basis for point number two (i.e., setting the SEDSS apart from other decision support tools), namely, the use of multiple process models within the SEDSS to accomodate a large number of conceptualizations of a site. The process models (e.g., a solute transport code) have implicit assumptions, which may invalidate their use for certain conceptual models at certain sites. For instance, choosing one code (e.g., RESRAD) for all risk assessment calculations for all possible waste sites is inappropriate because such factors

as distance to a receptor, surface water pathway, or other implicit attributes of the code make it invalid for certain sites. Having several codes to choose from to perform the necessary calculations yields a greater probability that the conceptual model will be implemented as desired, and not have to be influenced by the implicit assumptions in a given process model. The SEDSS automatically maps the desired conceptual model to the available codes for implementation of the risk calculations.

A third point of distinction relates to the formulation of the SEDSS around two key concepts:

1) risk assessment drives most decision analysis methods; and 2) a common decision analysis, or technical approach, may be applied to all waste site investigations. These concepts are discussed in the next section.

## METHODOLOGY

The SEDSS is designed so that the integrated process models and the GIS are transparent to the user (see Figure 1). The user sits down at a Sun workstation and interacts with the Graphical User Interface, or GUI. The GUI has the look and feel of a Macintosh or Microsoft Windows application, and is quite user friendly. The GUI handles all interactions with the GIS data base and the process models. Actually the process models are incorporated as modules and are only enabled when needed, depending on the problem to be solved. The GUI interfaces the process models through an applications manager. The applications manager has a number of options to choose from in order to supply information to a decision maker for the needs already mentioned previously. Therefore, the applications manager has modules for the following:

- regulatory framework
- site ranking,
- site characterization,
- monitor-well network optimization,
- risk assessment, and
- remedial alternatives and design.

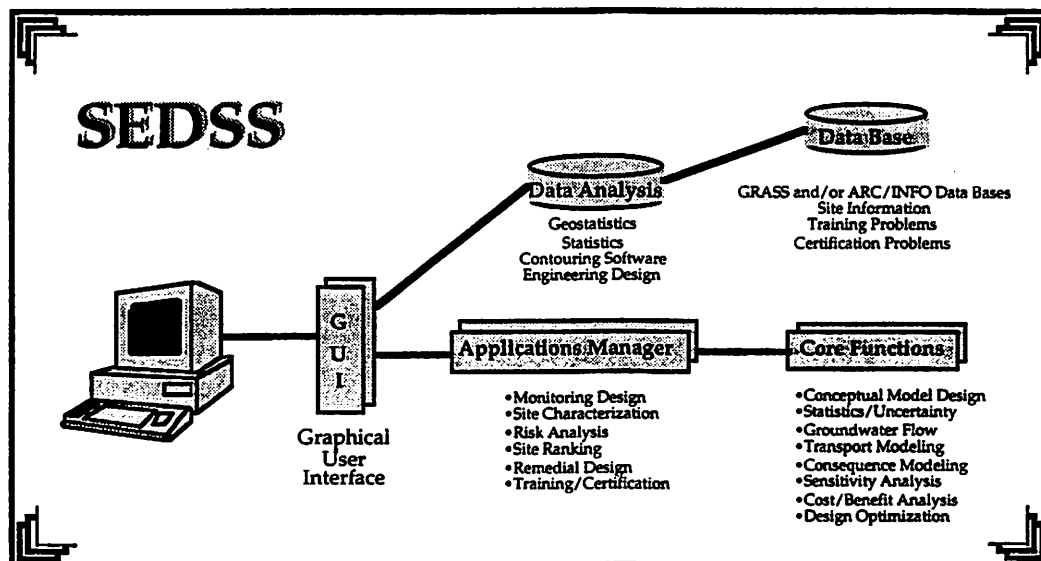


Figure 1. SEDSS Architecture

The monitor well network designer module enables a user to quantify the adequacy of a monitor well network. If the monitor well network is not adequate, the monitor well network

designer will provide information on the number of wells needed to come into compliance, and the possible locations of such wells. The methodology for the monitor well network designer is based on work by Freeze et al. (1990) and Parsons and Davis (1991). Uncertainty analyses using Monte Carlo flow and transport simulators are performed to evaluate the adequacy of the monitor well network, and an optimization routine employed to identify the need for additional wells and their locations.

In the site characterization module, routines will be available which utilize the results of a probabilistic risk assessment to help guide characterization options. Once a risk assessment is performed, the results may be analyzed to determine the relative importance of all site characterization needs. The risk results are then used to establish quantitative Data Quality Objectives, or DQOs. Once the site characterization needs are established, the site characterization module will also have statistical and process model based procedures to determine the number and locations of sample data required to meet specified DQOs. A data worth option is under development which would allow the user to identify the relative merit of collecting additional site characterization data based on uncertainty in risk and the performance measures.

In the risk assessment module, impacts to human health and the environment may be quantified. Uncertainties may be addressed quantitatively through the use of Monte Carlo techniques. In addition, the question of how clean is clean can be addressed, because the code can estimate residual concentrations of contaminants in soils based on published regulatory requirements for risk. The methodologies employed in the SEDSS for probabilistic risk assessment are based on methods developed at Sandia for the high-level and low-level radioactive waste programs for the NRC and DOE (e.g., Davis et al., 1990; Kozak et al., 1993). The use of probabilistic risk methodologies allows for the quantification of uncertainty in risk. Automation of the probabilistic framework for risk in the SEDSS, coupled with the computing "horsepower" of today's computers, means that quantitative assessments of uncertainty are now obtainable for real-time problem solving.

In the site ranking module, multiple sites are assessed with regard to risk, and the priorities for investigations amongst sites are determined based primarily on the potential impact to human health and the environment. Other attributes considered include future costs (i.e., the cost differential attributed to postponing an investigation or cleanup) and socioeconomic considerations. All requirements are considered in a multi-component decision analysis framework. Risk, cost, and socioeconomic considerations are weighted for comparison of results between sites on a common relative scale.

In the remedial selection module, a cost/benefit/risk analysis will be performed in order to evaluate the remedial alternatives for a given waste site. Uncertainty in risk, as well as cost, will play a large role in selecting a remedial alternative. Human health, ecological, and worker risks are combined with cost and socioeconomic considerations in a multi-component decision analysis framework to provide information to the risk managers to select the preferred alternative.

Training exercises will be available to learn the SEDSS. In addition, a certification option will be available to assure consistency of use for the SEDSS amongst all possible users. As with any codes, the quality of the information out of the program is directly related to the quality of the input. Limitations and implicit assumptions in the SEDSS need to be recognized by all users.

The decision analysis framework, or technical approach, which is common to all aspects of the ER and WM needs is depicted in Figure 2. The basic components of the approach are:

- establish the performance measures (including the operational definition of safety, such as  $10^{-4}$  to  $10^{-6}$  risk);
- assemble and assess all available information;
- develop a conceptual model(s) of the site;
- perform an uncertainty analysis (Monte Carlo simulations);
- evaluate the uncertainty analysis results against the performance measure and assess whether an adequate answer exists (e.g., risk is below  $10^{-6}$ );
- if an adequate answer is obtained, write up the results;
- if the answer is inadequate, perform a sensitivity and data worth analysis;

- if more data are not worthwhile, either write up the results or proceed to the next step in the regulatory process (e.g., more characterization data would not change the conclusion that a remedial alternative needs to be evaluated);
- if more data are worthwhile (e.g., more data may reduce the uncertainty in risk estimates to establish the site as safe), then collect that data;
- following the data collection, the process loop begins again by updating the conceptual model(s) of the site based on the new information gathered.

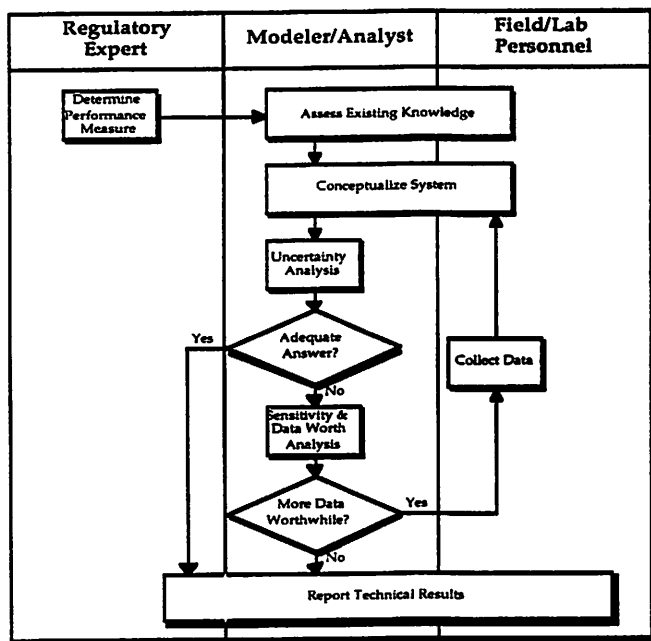


Figure 2. Decision Analysis Framework

This process flow, illustrated in Figure 2, can be applied to assessing whether a site is safe, to choosing a remedial alternative, and to assessing when the cleanup process is complete. It applies generically to both RCRA and CERCLA.

The SEDSS as it exists today has the monitor well network designer, risk assessment, and the site ranking modules enabled. All other applications modules are in development.

## REFERENCES

- Davis, P.A., L.L. Price, K.K. Wahi, M.T. Goodrich, D.P. Gallegos, E.J. Bonano, and R.V. Guzowski, 1990. "Components of an Overall Performance Assessment Methodology", NUREG/CR-5256, SAND88-3020, Sandia National Laboratories, Albuquerque, NM, 71 p.
- Freeze, R.A., J. Massman, L. Smith, T. Sperling, and B. James, 1990. "Hydrological Decision Analysis: 1. A Framework", *Ground Water*, Vol. 28, pg. 738-766.
- Kozak, M.W., N.E. Olague, R.R. Rao, and J.T. McCord, 1993. "Evaluation of a Performance Assessment Methodology for Low-Level Radioactive Waste Disposal Facilities, Evaluation of Modeling Approaches", NUREG/CR-5927, SAND91-2802, Sandia National Laboratories, Albuquerque, NM, 76 p.
- Parsons, A.M. and P.A. Davis, 1991. "A Proposed Strategy for Assessing Compliance with the RCRA Ground-Water Monitoring Regulations", *Current Practices in Ground Water and Vadose Zone Investigations*, ASTM STP 118, D.M. Nielson and M.N. Sara, Editors, American Society for Testing and Materials, Philadelphia.

## **ENVIRONMENTAL DECISION SUPPORT SYTEMS**

Dr. Jack Coleman,<sup>1</sup> John Franco,<sup>2</sup> and William Wee<sup>2</sup>

1 U.S. EPA, Center Hill Facility  
5995 Center Hill Rd., Cincinnati, Ohio 45224

2 University of Cincinnati  
Cincinnati, Ohio 45221

## **MODELING FOR ENVIRONMENTAL REMEDIATION**

For better environmental decision making, modeling environmental remediation resources at all levels is indispensable. Modeling of existing or proposed remedial resources should establish the consequences of strategic or tactical alternatives to properly support environmental management planning and decision-making. Five decision support systems are described, one strategic and four tactical. Two systems will be briefly illustrated with arrangements for demonstrating the others upon request.

## **STRATEGIC MODELING FOR ENVIRONMENTAL DECISION SUPPORT**

Balancing environmental and economic impacts of pollution control resources for emission sources, and determining impacts of present and planned pollution control costs on overall national pollution control and national output, requires strategic decision modeling. Developing environmental - economic relationships is a challenge that must be met by model development, testing and use. Strategic decision models should incorporate major linkages between economic, environmental and other appropriate sectors. These models should also be capable of disaggregation by pollutant types, fuel types, industrial classifications, and states. We will briefly describe and later demonstrate a strategic environmental decision model, called SEAS, developed for EPA.

### **SEAS (Strategic Environmental Assessment System)**

**Goal:** Determine impacts of present and planned national pollution control strategies on various pollutant emissions and national output.

**Status:** This model reflects environmental - economic relationships in a simple, doable model, providing dynamic representations of major linkages between economic, environmental and other sectors. This model can be disaggregated by pollutant types, fuel types, industrial classification, and states. It simulates historical and future environmental and economic relationships, and assesses regulations and incentives for controlling sulfur oxides, nitrogen oxides and volatile organic compounds as well as addresses:

- adequacy of present and planned pollution control resource levels to meet national air quality standards
- pollution emission changes resulting from alternative environmental and economic choices
- impacts of increasing production technology investments on the economy and pollution control
- measures to reduce environmental pollution without reducing economic growth
- strategies for "balancing" pollution control efficiencies with higher rates of economic growth.

## **TACTICAL TOOLS FOR ENVIRONMENTAL DECISION SUPPORT**

Determining cost-effective alternatives for remediation and cleanup, such as for specific Superfund and wastewater treatment sites, requires environmental decision support models to address:

- assisting federal, state and local environmental restoration organizations, and remediation contractors with the accurate selection of ARARs for a wide variety of cleanup sites
- screening potential pollution remediation and cleanup technology choices limited by environmental regulatory requirements
- selecting optimal multi-technology cleanup options for Superfund sites while interactively balancing cleanup technology designs with achievable cleanup levels, accommodating ARARs (Applicable, Relevant and Appropriate Regulations) policy and regulatory constraints
- displaying site base map with superimposed field of time-varying contaminant concentrations
- selecting and sizing collection, containment & remedial elements on the site map with a mouse and displaying cost of each element

Such environmental decision support tools have been developed at EPA to assess pollution control strategies in light of regulatory constraints. Four of the latest tools are described, and one or two of these tools will also be demonstrated. The other decision

support tools are presently discussed for further interest on the part of attendees with possible demonstration later on by special request. That is, later on, today or tomorrow, some of the other environmental decisions support tools can be demonstrated that are now briefly described:

### **PAST (Potential ARARs Screening Tool)**

**Goal:** Screening of Federal and State ARARs Regulations

**Status:** PAST is a rule-based object-oriented environmental regulation screening system which includes chemical specific, location specific, and action specific ARARs (Applicable, Relevant and Appropriate Regulations). You can select any set of contaminants, any media, and any remedial technologies, specify waste streams, respond to questions based on site characterization, and produce reports grouping ARARs by location, contaminant and remedial technology. The system can assist federal, regional, state and local environmental restoration organizations, and remediation contractors with the accurate selection of ARARs for a wide variety of cleanup sites. The demo version of PAST is limited to Federal "applicable" regulation screening.

We plan to user test the present version of PAST to determine how accurately and completely PAST encapsulates and encompasses all "applicable" regulations for each or any proposed or existing site application that users may choose. We also plan to incorporate "relevant and appropriate" regulations at both federal and state levels.

When selecting remedial technologies for PAST, one has to specify what sequences of technologies should be involved in the treatment train for each waste stream in order to do the job. And hopefully, these sequence are cost-effective so that PAST can screen each candidate sequence against regulatory constraints. The ideal method for achieving a set of treatment trains optimized for cost-effectiveness is the Sequence Optimizer called SOWAT.

### **SOWAT (Sequence Optimizer for Wastewater Treat ability)**

**Goal:** Determining optimal wastewater treatment trains.

**Status:** We have produced a rule-based "Wastewater Treatment System" sequence optimization program which incorporates wastewater pre-treatment and treatment ordering rules and exclusion factors, cost data and potential wastewater-treatment combinations. The system provides a better screening of potential technology sequences. Potential application benefits from reduced treatment train costs could be enormous for a relatively small investment in SOWAT development.

We plan to expand the SOWAT program to incorporate metals, other appropriate contaminants and technologies, and verify SOWAT for educational, permit validation and enforcement assistant applications.

Now SOWAT does an excellent job in providing sets of treatment trains ranked by least cost. All of these, starting from the least cost treatment train, can be inserted into PAST to see which candidates survive ARARs screening. Another practical engineering problem, however, emerges before any overall remediation system can be chosen. This problem arises when there are different cleanup problems presented at different locations and depths throughout a given site. This spacial variation in chemical and location

specific factors which characterize the site require some sort of cost-effectiveness optimization over the spacial distribution of chemical and location factors as well as the more obvious optimization of the treatment sequences provided by SOWAT. In fact, an overall optimization requires simultaneous sequential and spacial optimization. Fortunately, this is what the Superfund Technology Optimization Program, STOP, was made for.

### **STOP: (Superfund Technology Optimization Program)**

**Goal:** To develop and test methods for selecting optimal multitechnology cleanup options for Superfund sites while interactively balancing cleanup technology designs with achievable cleanup levels, accommodating ARARs policy and regulatory constraints.

**Status:** We were producing an advanced version of the STOP program, which would incorporate more technologies and a prototype interface with the Potential ARARs Screening Tool (PAST). If funded, future tasks will introduce interfaces between technologies and regulatory requirements to produce cost-effective treatment technologies that will comply with ARARs.

We plan to user test the present version of STOP to determine if it can accurately and completely screen the ten most cost-effective treatment sequences for proposed or existing soil remediation for each or any proposed or existing site application that users may choose.

Now that we can screen candidates satisfying regulatory, sequential and spacial optimization requirements, we want to see how our candidates perform. We need to interactively display a site with a superimposed field of contaminant concentrations upon which we can place candidate remedial elements and simulate the results. After a candidate design is configured, we need to input it into a soil and groundwater model to simulate, in real time candidate performance until we find the best configuration. Fortunately, we have such a decision support tool, called the Graphical Remedial Action & Cost Evaluation system, referred to as GRACE.

**GRACE (Graphical Remedial Action & Cost Evaluation) System** - to be applied first to groundwater contaminant remediation.

**Goal:** To facilitate evaluating cost and performance of remedial strategies, thereby expediting cost effective designs.

**Status:** We have been developing a user-friendly, object-oriented program which streamlines soil and groundwater remedial design processes by integrating unsaturated and saturated subsurface transport models and a cost database within a graphical user interface (GUI) system. The GRACE system displays a site base map with a superimposed field of contaminant concentrations upon which the user places remedial elements, such as water wells, trenches, slurry walls, or vapor wells with a mouse or a similar device. Treatment facilities can be selected and sized on the map. The cost of each element is determined and displayed, providing the user with a continuously updated estimate of fixed costs. When the design is finalized, it is translated into inputs for a groundwater model and a remedial performance evaluation is initiated. Total costs



of remediation are presented. If the design is inadequate, the simulation is modified until a suitable design is identified.

We plan to enhance GRACE interface capabilities to interactively incorporate a variety of collection, containment, treatment, and disposal technologies as well as various groundwater, soil, watershed, and agricultural models to enable its extended application to other soil remediation, non-point source and watershed applications.

For those of you who would like more information on or would like to adopt any or all of these exciting programs to your specific or general applications, please feel free to contact Dr. Jack Coleman at (513) 569-7464, Professor John Franco at (513) 556-1817, or Professor William Wee at (513) 556-4778. We also have other programs underway that you might be interested in hearing about.

**084 Reliability Based Design in Structural Engineering**

*Chair: D. Frangopol, U. Colorado*

**Time-Dependent Reliability of Rock-Anchored Structures**

*M. Chakravorty, J.E. Pytte, D.M. Frangopol (U. Colorado); R.L. Mosher (USAE  
Waterways Exp. Station)*

**Reliability Analysis of Redundant Structures by Response Surface Method**

*Y. Murotsu, S. Shao (U. Osaka, Japan); N. Chiku (Kawasaki Heavy Ind., Japan)*

**Risk Analysis of Pipeline Systems Based on Structural Reliability Models**

*M. Sinisi, G.M. Uguccione, M. Tominez (SLAF, Italy)*

## TIME-DEPENDENT RELIABILITY OF ROCK-ANCHORED STRUCTURES

Milan Chakravorty<sup>1</sup>, Dan M. Frangopol<sup>2</sup>,  
Reed L. Mosher<sup>3</sup>, and Jan E. Pytte<sup>1</sup>

<sup>1</sup>Graduate Student, <sup>2</sup>Professor, Department of Civil Engineering,  
University of Colorado, Boulder, Colorado 80309-0428, U.S.A.

<sup>3</sup>Scientific Program Officer, USAE Waterways Experiment Station,  
3909 Halls Ferry Road, Vicksburg, Mississippi 39180-6199, U.S.A.

### INTRODUCTION

When the underground environment is corrosive and the anchor-bar protection against corrosion is inadequate, structures strengthened with prestressed rock anchors are susceptible to reduced reliability over time. Case studies<sup>1</sup> suggest that prestressed rock anchors fail more often due to corrosion in free (unbonded) length than in fixed (bonded) length.

Corrosive ground condition can allow aggressive chemicals, like free chlorides, to penetrate cement grout and cause initiation of general corrosion in anchor bar. An existing model is used to predict diffusion of chlorides through protective cement grout around anchor bar and to predict time to reach a threshold value of chloride concentration at the surface of anchor bar. The available studies of the process of underground corrosion are not exhaustive and conclusive. However, studies of atmospheric corrosion of steel have advanced considerably.

In this paper, assuming that analogies can be established between atmospheric corrosion and underground corrosion, a deterioration model is developed. This model predicts uniform corrosion penetration of anchor bar and is applied to compute limit state functions under different failure modes of an anchored gravity structure.

A general purpose structural reliability program developed at the University of Colorado at Boulder is used to compute reliability indices. Results of time-variant reliability indices and sensitivity analyses are presented for typical failure cases.

### ROCK ANCHORS

As part of the structure, a rock anchor contributes to the overall stability and interaction of the ground-structure system through its various components (see Fig.1): (a) the anchor-head, (b) the free length, and (c) the fixed length. However, the anchor function is manifested in a load-tendon/bar deformation pattern that is complex and not totally understood, thus rendering it hardly amenable to exact solutions. Semi-empirical approaches<sup>1,2</sup> based on simplified assumptions are available for design of rock anchors, but the investigation into the failure of anchors remains complicated. The causes of failure of a rock anchor are often difficult to characterize as the installation procedure, corrosion protection, and workmanship may induce failure either singly or in combination. In this paper, however, for an *existing* anchor, the effects of corrosion are considered as sole cause of possible failure.

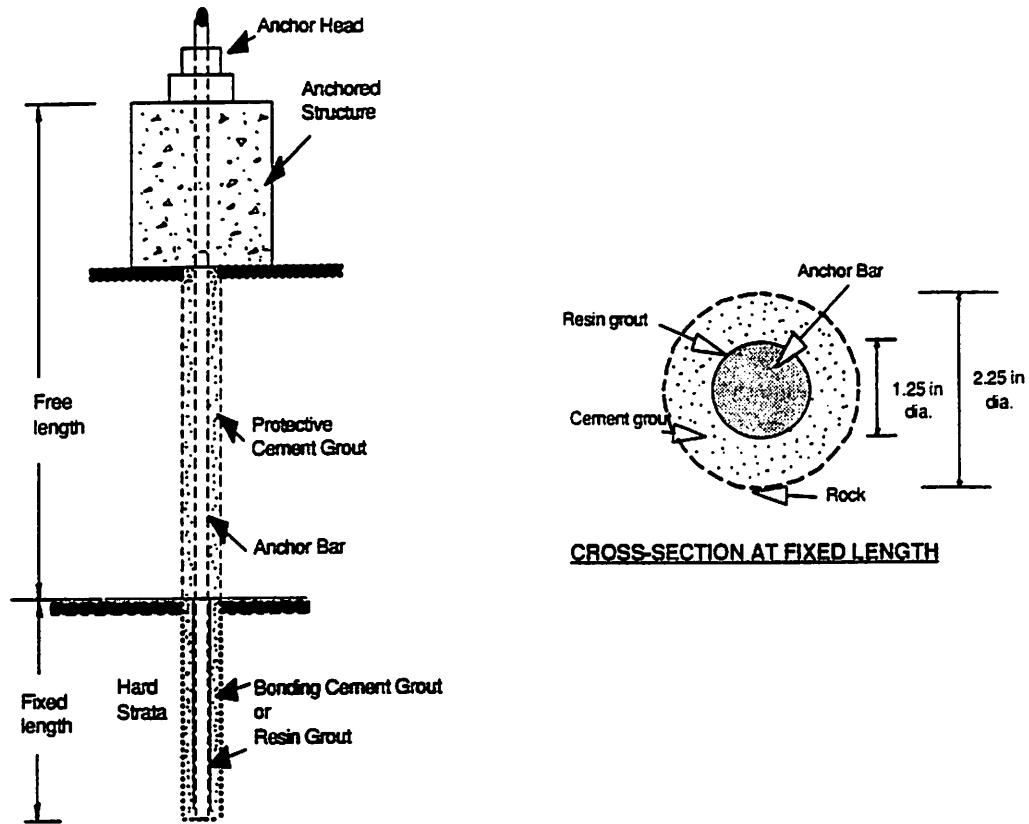


Figure 1: Typical Rock Anchor

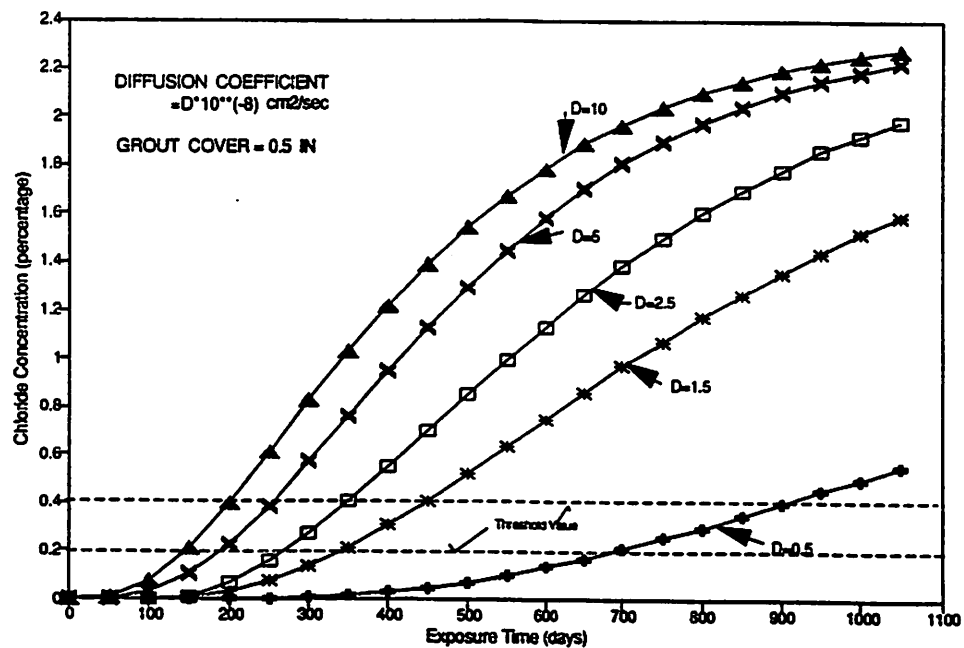


Figure 2: Chloride Diffusion in Grout  
(concentration at steel surface)

## CORROSION OF ANCHOR BAR

The intrusion of chlorides or other deleterious ions through the protective layer of a rock anchor initiates corrosion of the embedded steel tendon/bar. The protective layer often consists of cement grout alone, and in some instances in combination with polyurethane pipes and/or polyester resin grout. The leakage through outer pipe would leave only (a) cement grout or (b) resin grout and cement grout for protection. The effectiveness of resin grout in preventing diffusion of chlorides and sulfates to anchor bar in underground wet condition is not yet completely understood. The phenomenon of diffusion of chlorides into concrete has been widely studied<sup>3,4</sup>. However, very little work has been done regarding diffusion of sulfates into concrete.

## DIFFUSION MODEL

It is known that diffusion of chloride ions through concrete follows the Second Law of Diffusion:

$$\frac{\partial c}{\partial t} = \frac{D_e \partial^2 c}{\partial x^2} \quad (1)$$

where,  $c$  = chloride ion concentration at distance  $x$  inside concrete from the surface,  $D_e$  = effective diffusion coefficient, and  $t$  = time.

With appropriate boundary conditions eqn.(1) may be solved<sup>5</sup>. Given the value of the diffusion coefficient,  $D_e$ , chloride concentration at the steel surface may be obtained. For different diffusion coefficients, chloride ion concentration profile through 0.5in grout cover is shown in Fig.2. It is known that after chloride ion concentration reaches a threshold value (generally believed to be between 0.2% to 0.4% (by weight of cement) of chloride concentration<sup>6,7</sup>), the process of corrosion starts in steel bar/tendon if an electrochemical situation exists. The time for chloride ion concentration to reach this threshold value is considered as corrosion-initiation time ( $t_0$ ).

## CORROSION MODEL

Reasonable estimate of the time of corrosion ( $t_1$ ) can only be obtained from appropriate field measurements. To date neither theoretical nor empirical data can adequately predict the rate of corrosion of underground anchor bars<sup>1</sup>. From the collected data on uniform corrosion penetration in steel coupons in different environments, Townsend and Zoccola<sup>8</sup> fitted time-corrosion penetration curves to a power function:

$$C = A t_1^B \quad (2)$$

where,  $C$  = average corrosion penetration in microns determined from weight-loss,  $A$  = regression coefficient numerically equal to the penetration after 1-year of exposure,  $B$  = regression coefficient numerically equal to the slope of eqn.(2) in its natural logarithmic form, and  $t_1$  = time of corrosion in years. The mean values of coefficients  $A$  and  $B$  and their coefficients of variation and correlation are given by Albrecht and Naeemi<sup>9</sup>. These are shown in Table 1.

In absence of such data on underground corrosion of anchor bars, eqn.(2) is used as the corrosion model after including a model coefficient " $\alpha$ " such that:

$$C = \alpha A t_1^B \quad (3)$$

For different values of the model coefficient  $\alpha$ , eqn.(3) is shown in Fig.3.

Table 1: Statistical Parameters of Variable A and B  
(after Albrecht and Naeemi<sup>8</sup>)

Environment	Type of Steel	A		B		$\rho_{(A,B)}$
		$\bar{A}$	C.O.V	$\bar{B}$	C.O.V	
Marine	Carbon	70.60	0.66	0.789	0.49	-0.31
	Weathering	40.20	0.22	0.557	0.10	-0.45
Urban	Carbon	80.20	0.42	0.593	0.40	0.68
	Weathering	50.70	0.30	0.567	0.37	0.19
Rural	Carbon	34.00	0.09	0.650	0.10	-
	Weathering	33.30	0.34	0.498	0.09	-0.05

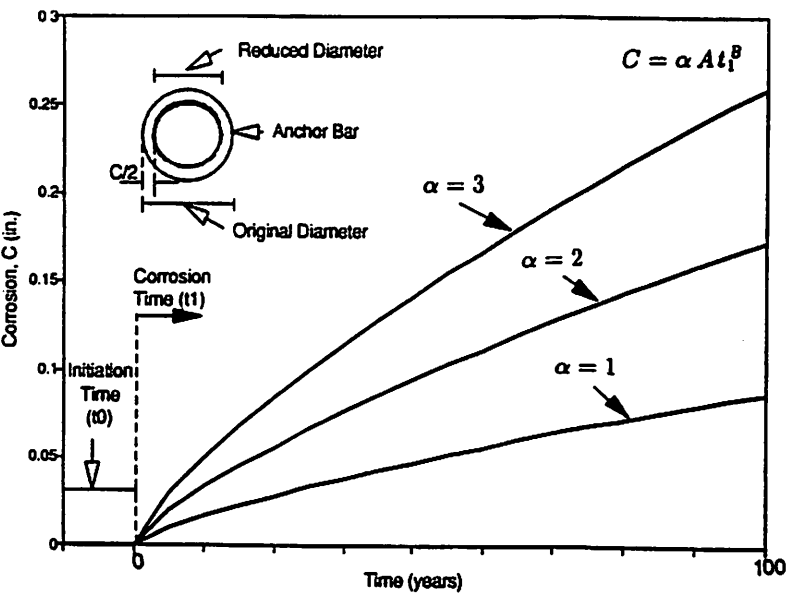


Figure 3: General Corrosion Model  
(mean value of  $A=37.8$ , Mean value of  $B=0.749$ , Ref.8)

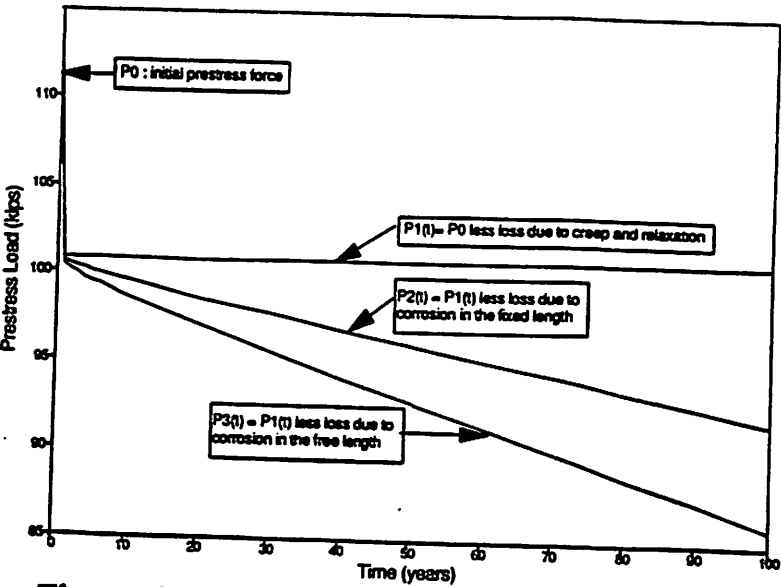
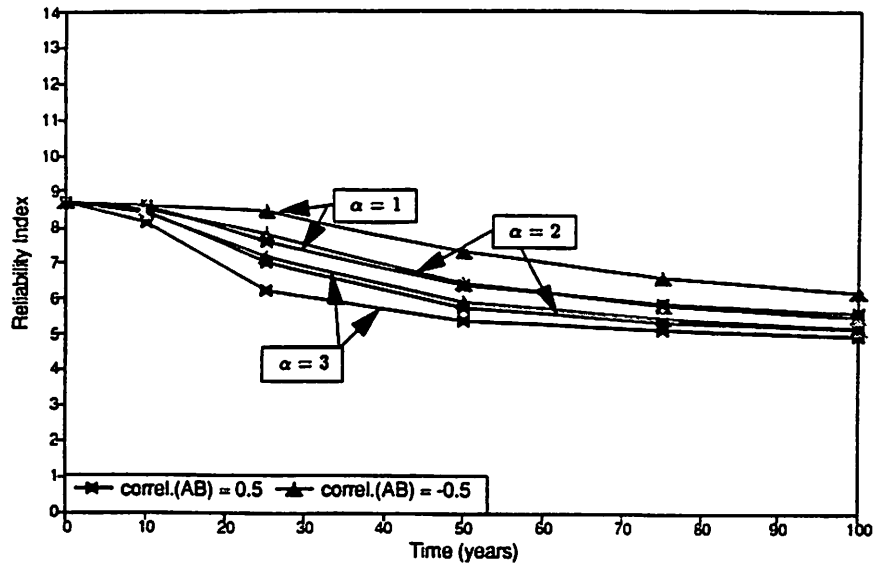
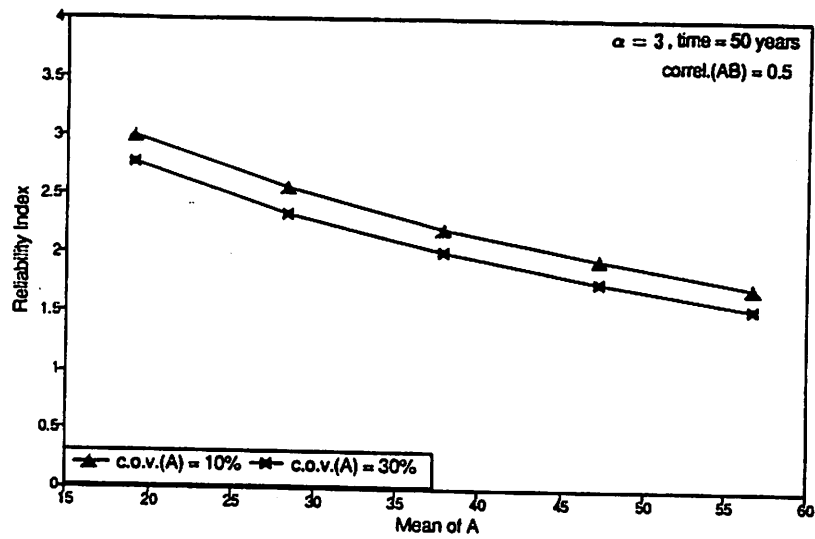


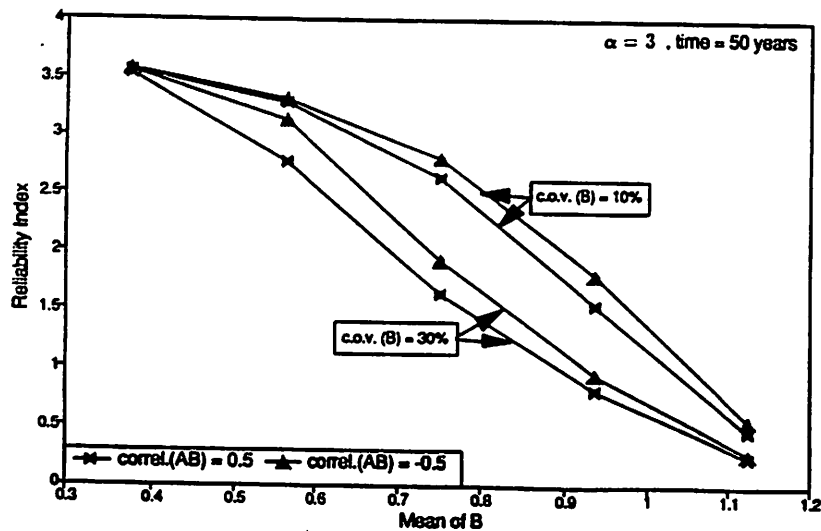
Figure 4: Time-Dependency of Prestressing Force



**Figure 5: Reliability of Anchored Structure**  
(against overturning under uniform corrosion in fixed length)



**Figure 6: Sensitivity of Reliability to Mean of Variable A**  
(uniform corrosion in fixed length)



**Figure 7: Sensitivity of Reliability to Mean of Variable B**  
(uniform corrosion in fixed length)

## ANCHOR RELIABILITY

Initial prestressing force in anchor bar is time-variant not only resulting from losses due to relaxation and creep, but also from the effect of reduced sectional area due to corrosion. Such variations under uniform corrosion conditions in both free as well as fixed length of an anchor bar in a gravity structure are shown in Fig.4.

## RELIABILITY OF ANCHORED STRUCTURES

Considering failure of anchor bar in fixed length and in free length, limit state functions are formulated for specific case of overturning of an anchored gravity structure. A general purpose structural reliability analysis program, RELTRAN (developed at the University of Colorado at Boulder) has been used to compute reliability indices of the anchored structure. RELTRAN employs First Order Reliability Method (FORM) where limit state functions ( $g_i(\mathbf{X}) = 0$ ) are replaced by tangent hyperplanes at design points in a transformed standard normal space.

The results obtained for time-dependent overturning reliability index of an anchored structure under uniform corrosion in the fixed length zone of anchor bars, are shown in Fig.5 for two different cases of correlation between regression coefficients  $A$  and  $B$  in eqn.(3). Sensitivity results for the reliability index with respect to changes in the mean values of coefficients  $A$  and  $B$  are shown in Fig.6 and Fig.7, respectively, for two different values of coefficients of variation (C.O.V.) of  $A$  and  $B$ .

## CONCLUSIONS

1. The statistical values used for characterization of the random variables used in this study must be validated through field, laboratory testing, observations, and/or expert opinions.
2. The reliability analyses performed in this study indicate the need for improvement of both design and evaluation methods for structures with rock anchors. Such improvement should be based on life-cycle time-dependent reliability concepts.

## ACKNOWLEDGEMENT

The support of this research by U S Army Corps of Engineers under contract no. DACW 39-92-K-0032 is gratefully acknowledged.

## REFERENCES

1. P. P. Xanthakos. Ground Anchors and Anchored Structures, John Willey and Sons, New York, NY (1991).
2. G. S. Littlejohn and D. A. Bruce. State-of-the Art - Rock Anchors, Foundation Publications Ltd., Sussex, England (1977).
3. S. H. Lin. Chloride diffusion in a porous concrete slab, *Corrosion*, Vol 46, No.12, Dec(1990).
4. H. G. Midgley and J. M. Illston. The penetration of chlorides in hardened cement paste, *Cement and Concrete Research*, Vol 14, New York, NY (1984).
5. H. S. Carslaw and J. C. Jaeger. Conduction of Heat in Solids, Clarendon Press, Oxford, England (1959).
6. B. B. Hope and A. C. K. Ip. Chloride corrosion threshold in concrete, *ACI Materials Journal*, Vol 84, No.4, Detroit (1987).
7. J. M. Bijen. Maintenance and repair of concrete structures, *HERON*, Vol 34, No.2, Delft, The Netherlands (1989).
8. H. E. Townsend and J. C. Zoccola. Eight year atmospheric corrosion performance of weathering steel in industrial, rural and marine environments, *ASTM*, STP No.767, Pa (1982).
9. P. Albrecht and A. H. Naeemi. Performance of weathering steel in bridges, *NCHRP*, Report No.272, Washington D.C., July(1984).



## RELIABILITY ANALYSIS OF REDUNDANT STRUCTURES BY RESPONSE SURFACE METHOD

Yoshisada Murotsu<sup>1</sup>, Shaowen Shao<sup>1</sup>, and Naruhiko Chiku<sup>2</sup>

<sup>1</sup>University of Osaka Prefecture, Sakai, Osaka 593, Japan

<sup>2</sup>Kawasaki Heavy Industries Ltd., Gifu 504, Japan

### 1 Introduction

For a large-scale structure with a high degree of redundancy, modelling of system is a very difficult work. The structure usually includes a number of failure mechanisms and each of them corresponds to one set of failure elements in the structure. Such a failure mechanism is also called a failure mode. When considering the reliability of a structure, all of the failure modes in the structure contribute to the system. However, it has been found that not all of them have equal or nearly equal probabilities of occurrence. In general, only some failure modes have high probabilities of occurrence that determine the reliability of the structure and others can be neglected. In this case, it is important to identify such dominant failure modes.

Murotsu, et al[1,2,3] proposed a so called branch-and-bound method to search for probabilistically dominant failure modes in frame structures. In that approach, only external loads and yield stresses were taken as random variables. This allowed a limit state function at each failure step to be expressed as an explicit function of the random variables which significantly simplified the probability calculation in the searching process. The further reliability analysis is performed based on those specified dominant failure modes. However, this is not to say that other random factors in the structure, such as material, geometrical, cross-sectional parameters, etc., can be neglected. How do they affect the reliability of a structure? May they cause different dominant failure modes? This paper presents an approach to such problems. The approach utilizes a dominant failure mode selected by the branch-and-bound method and develops a response surface to include all the necessary random variables. The influences that the individual random variables give to the structural reliability are investigated. Further, an algorithm is proposed to check if there exist new dominant failure modes owing to the newly included random variables.

### 2 A Dominant Failure Mode from a Branch-and-Bound Search

Consider a frame structure consisting of homogeneous elements, and with concentrated loads[1, 2]. In such a structure, element ends are potential plastic hinges. A structural failure mode consists of a series of failed element ends. It is determined in the following way. When element ends fail one by one, i.e.,  $r_1 \rightarrow r_2 \rightarrow \dots$ , the determinant of the total stiffness matrix is checked at each step. The criterion of a structural collapse is given as

$$\left| \left[ K^{(p_i)} \right] \right| / \left| \left[ K^{(0)} \right] \right| \leq \epsilon \quad (1)$$

where  $[K^{(0)}]$  and  $[K^{(p)}]$  are total stiffness matrixes in an intact state and at step  $p$ , respectively.  $\varepsilon$  is a specified constant. When failure path  $r_1 \rightarrow r_2 \rightarrow \dots \rightarrow r_p$  reaches a structural collapse, it constitutes a structural failure mode.

The branch-and-bound method[1,2] selects dominant failure modes by comparing the probabilities of formation of failure paths. Consider a failure path  $r_1 \rightarrow r_2 \rightarrow \dots \rightarrow r_p$ . Its probability of formation is an intersection probability of failure of every element end in the path which is expressed as

$$P_{fP(q)}^{(p)} = P \left[ \bigcap_{i=1}^p (Z_{r_{i(q)}}^{(i)} \leq 0) \right] \quad (2)$$

where  $Z_{r_{i(q)}}^{(i)}$  is the safety margin of element end  $r_i$  at  $i$ -th step of  $q$ -th path.  $Z_{r_{i(q)}}^{(i)} > 0$  denotes safety and  $Z_{r_{i(q)}}^{(i)} \leq 0$  denotes failure.

In an intact state, the safety margin of element end  $i$  is

$$Z_i = R_i - \sum_{j=1}^{6l} b_{ij} L_j = AZ_i \sigma_{yi} - \sum_{j=1}^{6l} b_{ij} L_j \quad (3)$$

where  $R_i = AZ_i \sigma_{yi}$  is the reference strength of element end  $i$ ,  $AZ_i$  the plastic section modulus, and  $\sigma_{yi}$  the yield stress.  $L_j$  are external loads,  $l$  the number of nodes, and  $b_{ij}$  the influence coefficient of  $L_j$  which is conducted from a structural analysis. After element ends  $r_1, r_2, \dots, r_{p-1}$  have failed, the safety margin of surviving element end  $r_p$  becomes

$$Z_i^{(p)} = R_i + \sum_{k=1}^{p-1} a_{ir_k}^{(p)} R_{r_k} - \sum_{j=1}^{6l} b_{ij}^{(p)} L_j \quad (4)$$

where  $R_{r_k}$  are the residual strengths of the failed element ends and  $a_{ir_k}^{(p)}$  the influence coefficients of  $R_{r_k}$ . When perfectly elasto-plastic behavior is assumed,  $R_{r_k}$  are equal to their original strengths. Rearranging Eq. (4) with respect to the elements whose ends are involved in the path,  $Z_i^{(p)}$  yields

$$Z_i^{(p)} = \sum_{k=1}^m (a_{ik_L}^{(p)} + a_{ik_R}^{(p)}) R_k - \sum_{j=1}^{6l} b_{ij}^{(p)} L_j = \sum_{k=1}^m (a_{ik_L}^{(p)} + a_{ik_R}^{(p)}) AZ_k \sigma_{yk} - \sum_{j=1}^{6l} b_{ij}^{(p)} L_j \quad (5)$$

where subscripts  $L$  and  $R$  in  $a_{ik_L}^{(p)}$  and  $a_{ik_R}^{(p)}$  denote the left and right ends of element  $K$ , respectively. In Eq. (5), coefficients  $a_{ik_L}^{(p)}$ ,  $a_{ik_R}^{(p)}$ ,  $b_{ij}^{(p)}$  and  $AZ_k$  are related to the geometrical, sizing and material parameters of a structure. Those relations are too complicated to be represented by explicit functions. They must be conducted from a structural analysis at each failure step. In order to speed up the probability calculation of Eq. (2), only external loads and yield stresses are taken as random variables. The safety margins of element ends as shown in Eq. (5) become linear functions in this case.

For a perfectly elasto-plastic material, the safety margin of the last element end in a complete failure path can be used as the limit state function of the failure mode. Following Eq. (5), the limit state function of failure mode  $i$  is expressed as

$$M_i' = \sum_{k=1}^m (a_{ik_L} + a_{ik_R}) AZ_k \sigma_{yk} - \sum_{j=1}^{6l} b_{ij} L_j \quad (6)$$

### 3 Response Surface of a Specified Failure Mode

The branch-and-bound method brings out dominant failure modes in a redundant structure and also provides their limit state functions. In this section, such a limit state function with only two types of random variables, i.e., the external loads and the yield stresses, is developed to include more random variables. This is performed by a response surface method.

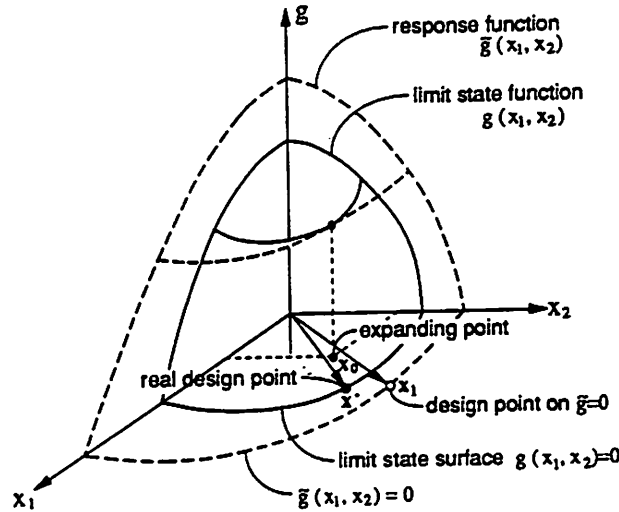


Figure 1: Response Surface by Taylor series Expansion

The response surface technique used in the present study is described as follows. Consider a real limit state function  $g(\mathbf{x})$  as shown in Fig. 1.  $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$  represents random variables.  $g(\mathbf{x})$  is assumed to be implicit for the moment. Select an initial point  $\mathbf{x}_0$ . A response surface is developed by using Taylor series expansion:

$$\bar{g}(\mathbf{x}) = g(\mathbf{x}_0) + \sum_{i=1}^n \frac{\partial g(\mathbf{x})}{\partial x_i} (x_i - x_{i0}) + \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^n \frac{\partial^2 g(\mathbf{x})}{\partial x_i \partial x_j} (x_i - x_{i0})(x_j - x_{j0}) + \dots \quad (7)$$

where the partial derivatives of the random variables  $\mathbf{x}$  can be calculated by a perturbation method. Response surface  $\bar{g}(\mathbf{x})$  fits the original limit state function  $g(\mathbf{x})$  well around the expanding point  $\mathbf{x}_0$ , while it doesn't ensure the confidence on other parts. The  $\beta$ -point  $\mathbf{x}_1$  on  $\bar{g}(\mathbf{x}) = 0$  is searched and in the next step  $\mathbf{x}_1$  is used as a new expanding point to develop another response surface. In this way, the expanding point is gradually moved to the real  $\beta$ -point  $\mathbf{x}^*$  of  $g(\mathbf{x})$ .

For the present problem, consider two random variable spaces  $\mathbf{x}' = (\sigma_{y1}, \sigma_{y2}, \dots, \sigma_{ym}, L_1, L_2, \dots, L_{6l})^T$  and  $\mathbf{x} = (\sigma_{y1}, \sigma_{y2}, \dots, \sigma_{ym}, t_1, t_2, \dots, t_n, L_1, L_2, \dots, L_{6l})^T$ .  $\mathbf{x}'$  only has external loads and yield stresses while  $\mathbf{x}$  includes new random variables  $\mathbf{t} = (t_1, t_2, \dots, t_n)^T$ . Let  $M'_i = g'_i(\mathbf{x}')$  represent the original limit state function of a dominant failure mode  $i$  selected by the branch-and-bound method. It is schematically illustrated in Fig. 2 in a two dimensional normalized space  $u_{\sigma_y}$ - $u_L$ .  $M_i = g_i(\mathbf{x})$  represents a limit state function of the same failure mode  $i$ , but includes the new random variables  $\mathbf{t}$ . As shown in Fig. 2,  $\mathbf{u}^{(i)}$  is the  $\beta$ -point on the limit state surface  $M_i = 0$ . However, since this  $M_i$  is not given as an explicit form, a response surface  $\tilde{M}_i$  is developed. Select an initial point  $\mathbf{x}_0$  on  $M'_i = 0$ , e.g., the  $\beta$ -point of  $M'_i = 0$ . The partial derivatives of  $M_i$  with respect to the external loads and the yield stresses can be directly calculated from  $M'_i$ . For instance, the following equations are obtained from Eq. (6).

$$\left. \frac{\partial M_i}{\partial \sigma_{yk}} \right|_{\mathbf{x}=\mathbf{x}_0} = (a_{ikL} + a_{ikR})AZ_k, \quad \left. \frac{\partial M_i}{\partial L_j} \right|_{\mathbf{x}=\mathbf{x}_0} = -b_{ij}$$

Only the partial derivatives of  $M_i$  with respect to the new random variables  $\mathbf{t} = t_1, t_2, \dots, t_n)^T$  must be calculated numerically. The response surface in a second order Taylor expansion form is given as follows:

$$\tilde{M}_i = M_{i0} + \sum_{j=1}^n \frac{\partial M_i}{\partial t_j} (t_j - t_{j0}) + \frac{1}{2} \sum_{j=1}^n \sum_{k=1}^n \frac{\partial^2 M_i}{\partial t_j \partial t_k} (t_j - t_{j0})(t_k - t_{k0})$$

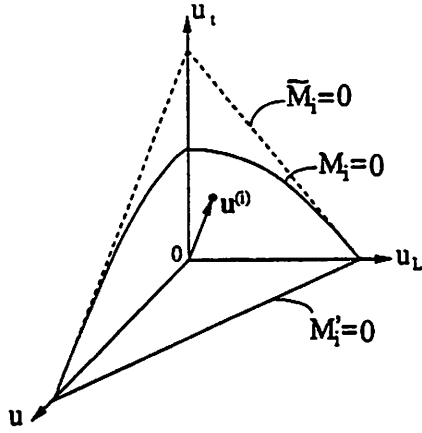


Figure 2: Limit State Function of a Failure Mode and Its Response Surface

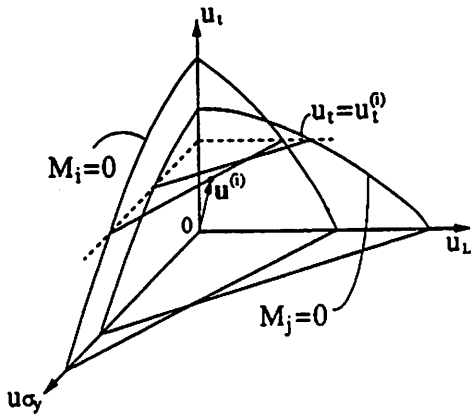


Figure 4: Dominant Failure Modes Concerned with Random Variables

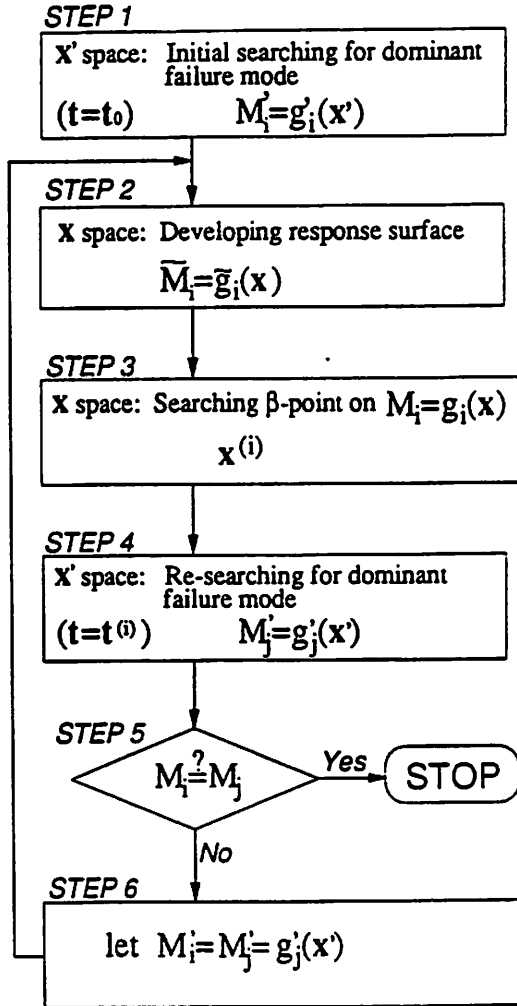


Figure 3: An Algorithm to Search Dominant Failure Modes

$$\begin{aligned}
 & + \sum_{k=1}^m (a_{ik_L} + a_{ik_R}) AZ_k(\sigma_k - \sigma_{k0}) - \sum_{j=1}^{6l} b_{ij}(L_j - L_{j0}) \\
 & + \frac{1}{2} \sum_{j=1}^n \sum_{k=1}^m \frac{\partial^2 M_i}{\partial t_j \partial \sigma_k} (t_j - t_{j0})(\sigma_k - \sigma_{k0}) + \frac{1}{2} \sum_{j=1}^n \sum_{k=1}^{6l} \frac{\partial^2 M_i}{\partial t_j \partial L_k} (t_j - t_{j0})(L_k - L_{k0}) \quad (8)
 \end{aligned}$$

#### 4 Algorithm for Searching New Dominant Failure Modes

In Section 3, a response surface has been developed for a specified failure mode to include various random variables. This can be applied to all the dominant failure modes selected by the branch-and-bound method to get more exact evaluation of structural reliability. However, there may exist other dominant failure modes which could not be found in the initial searching process where only the external loads and the yield stresses are taken as random variables. That is, the influences of other random variables to the dominant failure modes should also be checked. The sensitivity factors[4] at the  $\beta$ -point from a response surface provide some information of the relative influences of individual random variables. In this section, an algorithm is proposed to search new probable dominant failure modes. It is shown in Fig. 3.

At Step 1, an initial search at the random variable space  $x'$  provides dominant failure

Element number	Diameter $D_i$ (m)	Mean value of thickness $t_i$ (mm)	Coefficient of variation $CV_{t_i}$
1,2,5,6	0.2442	4.7867	0.05
3,4,7,8	0.2647	5.4010	0.05

Mean value of yield stress  $\sigma_{yi} = 276$  MPa  $CV_{\sigma_{yi}} = 0.05$

Correlation coeff.  $\rho_{RkRl} = 0.0$   $\rho_{tmin} = 0.0$

$\bar{L}_1 = 14.0$  kN  $\bar{L}_2 = 7.0$  kN  $CV_{L1} = 0.3$

$\bar{L}_3 = 21.0$  kN  $\bar{L}_4 = 21.0$  kN  $\rho_{L1Lj} = 0.0$

$l = 5.0$  m  $h = 6.0$  m

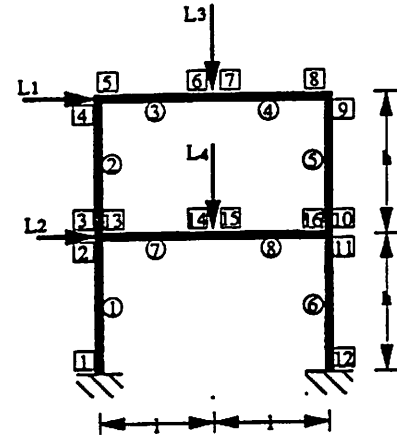


Figure 5: A Two-storied Frame

No.	Failure mode	$\beta$	PfM
1	(1,4,9,12,13,16)	5.5285	$1.6145 \times 10^{-8}$
2	(1,5,9,12,13,16)	5.9807	$1.1106 \times 10^{-9}$
3	(1,4,8,12,13,16)	5.9807	$1.1106 \times 10^{-9}$
4	(1,2,11,12)	6.0502	$7.2315 \times 10^{-10}$
5	(1,7,9,12,13,16)	6.1951	$2.9119 \times 10^{-10}$

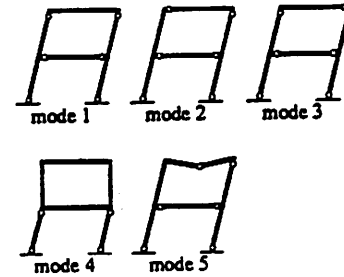


Figure 6: Dominant Failure Modes and Their Probabilities of Formation (from an initial search with fixed pipe thicknesses)

mode  $M'_i = g'_i(x')$ . The random variables  $t$  are fixed at  $t = t_0$  for the moment. Steps 2 and 3 develop a response surface in space  $x$  and get the  $\beta$ -point  $x^{(i)}$  on  $M_i = g_i(x) = 0$ . Then, at Step 4, let  $t$  be fixed at the value of  $\beta$ -point,  $t = t^{(i)}$ , and repeat the search for dominant failure modes. This is schematically shown in Fig. 4 where  $u^{(i)}$  and  $u_t^{(i)}$  in a normalized space correspond to  $x^{(i)}$  and  $t^{(i)}$ , respectively. If a new dominant failure mode is found, go back to Step 2 to search the new  $\beta$ -point by response surface method. If no new failure mode is found, go to stop.

## 5 Numerical Examples

Consider a two-storied frame structure as shown in Fig. 5. All the elements are pipes. The pipe thicknesses, the yield stresses and the external loads are assumed as normal random variables. The numerical data are also listed in Fig. 5. Fig. 6 shows the dominant failure modes selected by the branch-and-bound method with the pipe thicknesses being fixed at their means.  $P_{fM}$  denotes the probability of occurrence of a failure mode.

A response surface is developed for the most dominant failure mode, Mode 1. As shown in Table 1, the expanding point was moved three times to converge to the  $\beta$ -point.  $M$  is the value of the real limit state function at each expanding point which represents a error of convergence. In this example, branch-and-bound search routine was called every time with a new expanding point. However, although the order of the failure sequence changed a little, the same failure mode was always selected. Table 2 shows the sensitivity factors[4] of random variables at the  $\beta$ -point of Mode 1. It is seen that the external loads have much bigger sensitivity factors than other random variables. Therefore, they might be most influential to the dominant failure

Table 1: Converging Process of Response Surface

No.	$\beta$	$P_f$	$M$	path
0	—	—	$2.9343 \times 10^2$	16 12 9 1 13 4
1	5.4435	$2.6117 \times 10^{-8}$	$2.1139 \times 10^{-1}$	16 12 1 9 13 4
2	5.4474	$2.5558 \times 10^{-8}$	$-6.6577 \times 10^{-5}$	16 12 1 9 13 4
3	5.4474	$2.5558 \times 10^{-8}$	$-1.6812 \times 10^{-5}$	16 12 1 9 13 4
$\beta = 5.4474 \quad P_f = 2.5558 \times 10^{-8}$				

Calculation time 224 s (CPU SunSPARCstation2)

Table 2: Sensitivity Factors of Random Variables at  $\beta$ -point

elem. no.	$t_m$	$\sigma_{ym}$	force no.	$L_k$
1	$-6.6376 \times 10^{-2}$	$-6.9127 \times 10^{-2}$	1	$9.3632 \times 10^{-1}$
2	$-6.6390 \times 10^{-2}$	$-6.9127 \times 10^{-2}$	2	$2.3408 \times 10^{-1}$
3	0.0	0.0	3	0.0
4	0.0	0.0	4	0.0
5	$-6.6379 \times 10^{-2}$	$-6.9127 \times 10^{-2}$		
6	$-6.6380 \times 10^{-2}$	$-6.9127 \times 10^{-2}$		
7	$-8.7240 \times 10^{-2}$	$-9.0990 \times 10^{-2}$		
8	$-8.7240 \times 10^{-2}$	$-9.0990 \times 10^{-2}$		

modes. The yield stresses and the pipe thicknesses almost have the same influences.

## 6 Conclusions

The present research brings out a new approach to consider all necessary random variables in the reliability analysis based on structural failure modes. This is done by developing a response surface for a specified failure mode. The  $\beta$ -point is selected and the influences of all the random variables are investigated. These results are further utilized in a searching algorithm to avoid missing dominant failure modes. The validity of the proposed method has been confirmed by numerical examples.

## References

- [1] Murotsu, Y., Okada, H., Yonezawa, M., and Kishi, M., Identification of Stochastically Dominant Failure Modes in Frame Structure, 4th Inter. Conf. on Application of Statistics and Probability in Soil and Structural Engineering, Universita di Firenze, Italy, 1983, Pitagora Editrice, pp. 1325-1338.
- [2] Thoft-Christensen, P. and Murotsu, Y., Application of Structural Systems Reliability Theory, Springer-Verlag, 1986.
- [3] Murotsu, Y., Okada, Matsuda, A., T., Niho, O., Kobayashi, M., and Kaminaga, H., Application of the Structural Reliability Analysis System (STRELAS) to a Semisubmersible Platform, Proc. of 11th OMAE, ASME, 1992, Vol. 2, Safety and Reliability, pp. 209-217.
- [4] Madsen, H. O., Krenk, S. & Lind, N. C., Methods of Structural Safety, Prentice Hall, 1986.

## **RISK ANALYSIS OF PIPELINE SYSTEMS BASED ON STRUCTURAL RELIABILITY METHODS**

M. Sinisi, M. Tominez, G. Uguccioni

Safety and Reliability Dept. (SIAF)  
Snamprogetti SpA  
20097 San Donato (Milano), Italy

### **INTRODUCTION**

Pipelines are recognized to be one of the safest transportation systems for hazardous products. They however involve large inventories of substances and are frequently routed near inhabited areas, so that risk analysis studies are required by Authorities and by the Operators to verify that the design characteristics satisfy the required level of safety. In addition, the costs of loss of production and of repair intervention (especially offshore) makes it important to minimize the probability of failures, optimizing the design choices.

The Risk analysis studies are usually carried out on the basis of generic statistical failure rates for pipeline systems. More recently, approaches based on more refined statistical approaches (multivariate analysis<sup>1</sup>, Bayesian inference<sup>2</sup>) or on fracture mechanics methods<sup>3</sup> have been proposed. These approaches however do not allow to take fully into account the site and design specific characteristics of the failure process. A method has been developed in Snamprogetti to analyze the pipeline failure probability due to external impact, through the following steps:

- assessment of the frequency of interaction of human activities (mainly ship traffic for offshore pipelines and agricultural/excavation activities for onshore pipelines) on the basis of the analysis of the actual conditions of the pipeline route.
- assessment of the impact characteristics (impact energy) on the basis of the activities performed.
- assessment of the pipe probability of failure through structural reliability analysis methods from the accidental loads defined by the previous steps.

The paper will present the main characteristics of the technique, with application both to onshore and offshore pipelines.

### **HISTORICAL EXPERIENCE ON PIPELINE FAILURES**

Quite a number of reports have been published dealing with statistical analysis of pipelines failures<sup>4,5,6,7,8,9,10,11</sup>. The number of failures reported is not high: it ranges from 6 cases for 8600 km\*y in the British sector for the North Sea<sup>7</sup> to 290 cases in 20 years in the Gulf of Mexico<sup>5</sup>; There is a significant consensus on the failure rate proposed by the various sources (about 1 failure per

1000 km per year or less, both for offshore and onshore lines). It shall be noted that the definition of 'failure' is not unique throughout these studies; in some cases only events causing leaks are considered, in other cases all events notified to control Authorities are included. These studies also agree on the failure modes that can affect a pipeline. A comprehensive list of failure causes includes Environmental Hazards, External and Internal Corrosion, Faulty material or construction, Mechanical failures in ancillary equipment, Impacts caused by human activities along the route.

Among the possible failure causes, the most significant both for offshore and onshore pipeline is found to be the External Impact with Third Party activities. The percentage of accidents due to this cause ranges from 50% for onshore data bases<sup>8</sup> to 70%<sup>9</sup> for offshore pipelines. The other failure causes depends strongly on the design criteria adopted for the pipe; as an example the percentage of corrosion failure varies from 50% for offshore pipelines in Gulf of Mexico<sup>10</sup> to 15% for onshore gas pipelines in Europe<sup>8</sup>. The importance of the external impact cause implies that the failures should not be evenly distributed along the lines, but should be found concentrated in the areas where higher intensity of human activities is occurring. In fact, offshore data show that more than 60% of all failures are in the 'near platform' area<sup>10</sup> and that an higher failure rate is calculated for pipelines belonging to the 'Flowlines', 'Flare' and 'Loading' categories<sup>7</sup>, that are likely to be laid near to platform or other locations with high operation intensities.

The pipeline characteristics as well show a significant effect on pipeline failure rate. Most important are the diameter and thickness; it has been shown by most researchers that high diameter pipelines present a significantly lower failure rate<sup>4,6,7,8,9,10</sup>; the same effect is shown for increasing thickness (the two parameters are in effect correlated). This can be explained considering the higher resistance that a high thickness pipelines present with respect to defects, mainly due as shown before to external impact and corrosion.

The suggestions that can be drawn from the consideration of the historical experience on pipelines failures are:

- The scarcity of data on pipeline failures is an indicator of the high level of safety reached by this technology; this however also poses a limit on the significance of risk analyses based purely on the statistical analysis of the available failure data. There are also indications that the design characteristics of modern pipelines should imply a probability of failure lower than that derived from the straightforward application of the statistics.
- The data clearly indicate that external impact is the most likely cause of failure; This implies that the analysis should be addressed specifically to the areas where human activities occur and therefore the possibility of external impact shall be recognized.
- The importance of the external impact as a cause of failure also indicates that the design characteristics of the pipeline play an important role in the probability of failure, as indicated by the strong dependence of the statistical failure rate from the pipe diameter and thickness.

These suggestions lead to the conclusion that the risk assessment of a pipeline shall be able to cope with site-specific and design-specific aspects; in particular it shall be able to identify the expected frequency and characteristics of external impacts and to define the probability of failure of the pipeline taking into account the actual pipe design.

The procedures that has been developed in Snamprogetti for the risk analysis of offshore and onshore pipeline on the basis of these considerations are briefly described in the following.

## OFFSHORE PIPELINES

The accidental loads conditions which could cause seelines to fail can be schematically separated into two categories: natural and manmade. Natural are those related to environmental and/or natural occurrences and disasters such as severe sea state, hurricanes, earthquakes, landslides, sea bottom



instability, etc. Manmade hazards are those related to offshore human activities, erroneous operating conditions and materials deficiency.

The attention is focused on impact hazards related to the use and exploitation of the area in which a sealine is planned to be installed, aimed to the definition of the frequencies of interaction between the threading activities and the sealines. Impact loads and damages induced to the sealine are then deterministically evaluated.

Information on mass and water falling speeds of containers, anchors, etc., are used to compute impact energies and forces; damages induced to the sealine, mainly in terms of denting and hooking displacement, are evaluated with analytical mechanical models.

In the following, the general issues related to the evaluation of the accident frequency are described.

The commercial navigation and the deep water fishing activities can be considered as the main sources of accidental external impacts for the sealines<sup>9</sup>. The common use of defined shipping routes and the definition of specific fishing areas restrict the sealine portion at risk to the crossings with the commercial routes and fishing zones.

The following main accidental loads scenario can be identified:

- the pipe hit by ships anchors;
- the pipe hit by falling objects lost by passing ships;
- the pipe hit by sinking ships;
- the pipe hit by deep water fishing devices (trawl doors).

### Interaction with Ship Anchors

Impacts with ships anchors are strictly related to the occurrence of emergency situations on board requiring unplanned anchoring operations. Planned anchoring is in fact carried out in dedicated areas away from any subsea obstacle/structure. The loss of steerage is the main reason leading to emergency anchoring, particularly when sailing within navigation channels because of the shallow waters (risk of ship grounding) and congested canalized ship traffic (risk of collisions). The loss of steerage probability can be assessed by fault tree analysis. The relevant failure rates can be gathered and processed from available data banks and literature.

The impact with the pipeline could be:

**direct:** the anchor is supposed to hit the pipeline if falling within an interaction corridor centered on the sealine, whose width equals the pipe diameter plus the anchor width. Recent analysis<sup>12</sup> demonstrated that damages can be expected in terms of local deformations of the pipe shell up to 25% of the pipe diameter, for the largest anchors adopted (up to 26 tons);

**indirect:** the anchor is supposed to be thrown within an interaction corridor whose width equals the distance needed by the ship to completely stop (anchor dragging distance), governed by the embedded anchor efficiency, soil characteristics and initial ship velocity. This impact scenario is the worst expected, in terms of potential damages, because of the possibility of pipe hooking. Local indentation and considerable global pipe deflection (particularly for on bottom pipelines) could occur.

The expected interaction frequency is governed by the ship dimensions (influencing the anchor weight and geometry), the ship traffic intensity over the pipeline and the ship velocity, while the extent of the effects are strictly related to the on bottom pipeline configuration (pipe resting on the sea floor, trenched or buried).

A rough estimation of the interaction frequency, for both the aforementioned impact typologies, can be obtained by implementing the following relationship, assuming the ship traffic uniformly distributed over the route width:

$$N_i = \lambda n_i L_{ci} / v_i \quad (1)$$

where

$N_i$  is the occurrence per unit time relevant to the ship size class  $i$ ;

$\lambda$  is the emergency anchoring rate per ship;  
 $n_i$  is the traffic intensity over the pipeline;  
 $L_{ci}$  is the critical corridor length across the pipe;  
 $v_i$  is the cruise ship velocity.

### Interaction with Dropped Objects

The "dropped object" casualty category refers to those events in which an object can be lost or washed overboard from the ship deck because of heavy weather. From available literature, it appears that the loss of containers is the most frequent incident in open sea. However, most of loaded containers lost by containers carriers stay floated and only a small portion sinks due to a lack of water tightness (the maximum allowable container load is well below the weight of the volume of the displaced water).

Sinking mass of the largest standard containers (49 feet) can be in the order of 100 tons with terminal velocities up to 3 - 5 m/s (depending on the object orientation during sinking<sup>13</sup>. Large impact energies can then be expected. A considerable portion of this energy should be dissipated in the container deformation, at the impact, being its stiffness lower than that of the pipe shell. However, plastic deformations can be induced to the pipe if resting on the sea bottom.

The interaction occurs if the container is lost within a corridor across the pipeline whose width equals the container length plus the pipe diameter. A rough estimation of the expected number of interaction can be obtained by applying the same relation (1), where  $n_i$  is only the container carriers traffic.

### Interaction with Sinking Ships

The ship foundering (due to heavy weather, structural failure, fire/explosion on board etc.) and the collision with incoming ships are the main causes of ship sinking.

In case the sinking event occurs within an area across the pipeline whose width equals the ship length plus the pipe diameter, the interaction with the pipeline could occur. The impact with the pipeline can be:

direct: the ship hits directly the pipeline with the hull;

indirect: the ship hits the sea bottom and then lies over the pipeline.

In both cases, because of the large impact energies involved in this event, large pipe indentations are expected, particularly for pipes resting on the sea floor. Nevertheless, this should not necessarily imply pipe rupture as the stiffness of the ship hull can be significantly lower than that of the pipe shell (a large portion of the impact energy will then be dissipated in the hull deflection) and the ship hull could not produce a notch on the pipe wall.

A rough estimation of the expected frequency of this event can be obtained by applying the following relationship:

$$N_i = \lambda_i n_i L_{ci} \quad (2)$$

where

$\lambda_i$  is the casualty rate expressed in terms sinking events per unit length sailed and ship. This value, depending on the ship size and characteristics, can be found in specific data banks<sup>14,15</sup>.

### Interaction with Fishing Activities

Outside the commercial shipping routes crossing areas, the external impact hazards for a seeline is dominated by the fishing activities carried out by the use of trawl gears. In this type of fishing, the fishing vessels tows a system constituted by a bag net that is maintained close to the sea bed by means of two doors also ensuring the required opening of the net. This activity can be carried out even in deep water (up to 1000 m) and, because of the trawl doors acting directly on the sea bottom,

it represents an hazard for any unburi pipes and cables. The trawl doors can weight up to 1300 kg and are usually towed by the fishing vessels at velocities of about 3 -4 knots.

Because of the high probability of occurrence expected for this event, in case of crossing of a specific fishing area, this scenario is usually covered by the pipe design. Anyway, field test demonstrated that impacts by trawl doors should not damage significantly the pipeline<sup>16</sup>, apart from local damages on the concrete coating (if present). On the contrary, if hooking occurs (e.g. along a pipe portion in free span) possible damages for the fishing vessel/devices can be expected.

## ONSHORE PIPELINES

A tool for the integrated assessment of the Risk related to onshore pipeline interaction with third party activities has been developed. The main tasks are the probabilistic definition of the impact scenario using Event Tree technique and the failure probability quantification with structural reliability methods; both these tasks will be described in the following.

### Definition of impact scenarios

One of the main task in assessing the Risk related to onshore pipelines is the definition of the impact interaction scenarios between agricultural and civil works machines and the pipelines since, as mentioned, Third Party activities are responsible of 50 % of the total number of failures.

Improving the knowledge regarding the interaction modalities and a characterization of the machines involved in both agricultural and civil works can significantly reduce the uncertainties related to the quantification of the pipelines failure probability.

The interaction scenario depends on the energy of the machines working in the area crossed by the pipeline. To assess the scenario it is therefore necessary to identify the types of works and the corresponding machines. This analysis is done for typical land uses of the areas crossed by onshore pipelines, e.g. Urban, Industrial, Agricultural, Rural, using an Event Tree approach (figure 1.)

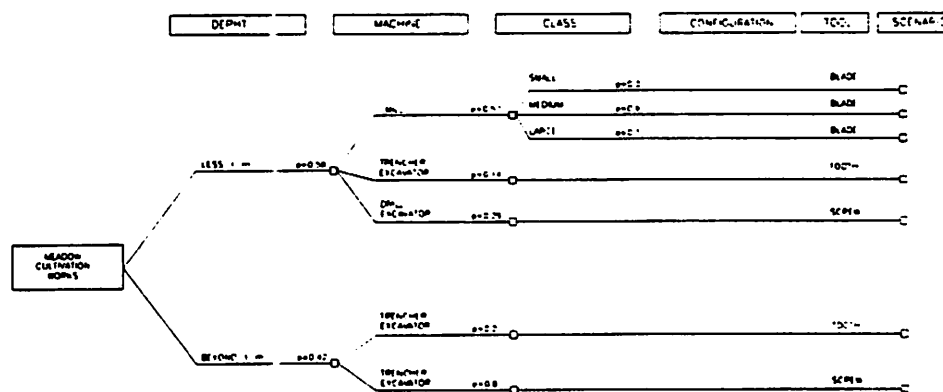


Fig. 1: Event Tree representation of possible impact scenarios

The Event Tree approach allows to take directly into account the types of works carried out, the associated machines used, machines classes/sizes and the tool types.

Developing each Event Tree it is possible to compute the probability of occurrence of each impact scenario, defined in terms of both machine and tool; adding the information related to the Machines/Tools masses and their working velocities it is possible to associate to each combination its impact energy.

Summarizing over each Machine/Tool group the impact energy, weighted with impact scenario occurrence probability, the impact energy cumulative distribution (i.e. the probability of exceeding a given impact energy) is calculated for each of the five typical areas and each Machine/Tool.

A typical impact energy cumulative distribution is shown in Figure 2 for the excavator machine and the tooth tool.

### Impact Energy Cumulative Distribution

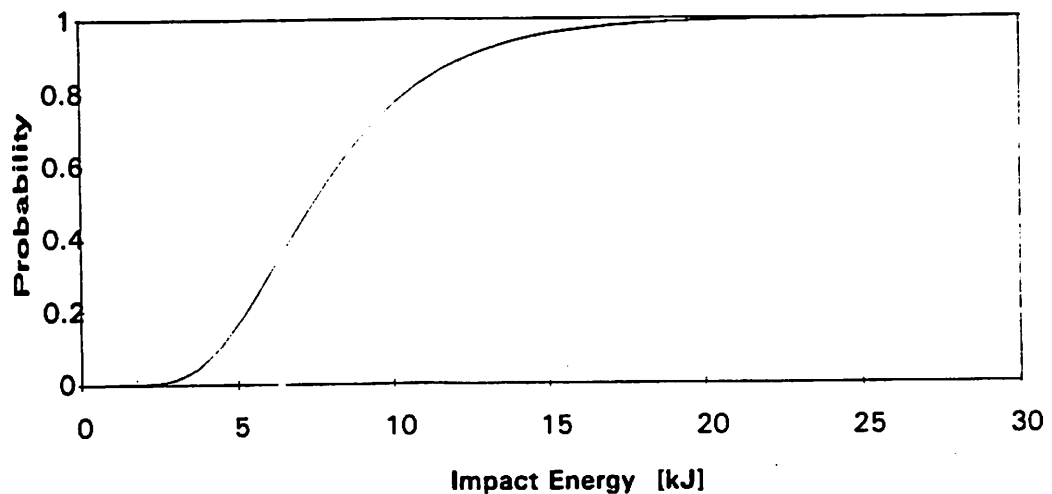


Fig. 2: Impact scenario computed cumulative energy distribution

The impact energy distributions are the main input to the probabilistic assessment of the defects induced to a pipe by Third Party activities and thus to the consequent pipelines failure probability.

The adopted Event Tree definition of the impact scenarios has the advantage that can be easily tailored to represent a site specific situation, both in terms of machine types/sizes and machines usage, simply changing the machines or working activities probabilities. It can also be easily updated to take into account changes in machine masses and working velocities simply modifying a data base. A program for the calculation of the impact energy distribution based on this approach (IMPACT) has been developed in Snamprogetti for use within pipeline risk assessment studies.

### Failure probability quantification

The state of the art of the Structural Reliability Analysis tools makes it possible an assessment of the structural failure probability in a numerical/analytical way rather than making reference to global and non specific historical failure data.

Historical failure data can be adopted for the quantification of release occurrence due to failures for causes different from the Thir Party activities, such as corrosion, land-slides, material defects.

The steps that shall be carried out for the probability quantiifcation with mechnaical reliability modeling are:

- characterization of the incidental scenarios (i.e. definition of the impact energies)

- identification of the involved pipeline failure modes (e.g. puncture, gouging, denting, etc.) and the applicable failure criteria
- probabilistic modelling of the pipeline mechanical data

The main advantages of this procedure is that the calculated failure probabilities take directly into account the uncertainties related both to the pipeline mechanical data and load data, are therefore site specific and referred to the specific pipeline design.

**Mechanical Reliability Modeling.** In the following the procedure to compute the failure probability of a structural/mechanical component or system will be briefly outlined; for a more detailed information see e.g. <sup>17, 18</sup>.

In the next paragraph an application to the evaluation of the pipe puncture probability is presented. It is possible to define the behaviour of a structural component or system by the so-called *limit state function*  $g(X)$  which allows to discriminate between the safe and unsafe states of a system with the following rules:

$g(X) > 0$	safe state
$g(X) = 0$	limit state
$g(X) < 0$	unsafe / failure state

where  $g$  is a function of Load and Resistance,  $X$  is a vector including both the random and deterministic variables.

Then the failure probability can be calculated by:

$$p_f = \int_{g(X) \leq 0} f_X(x) dx$$

where  $f_X(x)$  is the joint probability density function of the random variables included in  $X$  and  $g(X) \leq 0$  is the failure domain.

The integral can be evaluated both using simulation methods (Crude, Importance and Adaptive Sampling Montecarlo) or with the so-called Form/Sorm methods or better with a combination of the mentioned methods.

In the numerical example presented hereafter, a Form/Sorm method with simulation correction will be used.

**Numerical Example.** The methodology outlined is applied to the calculation of the probability of pipeline puncture due to impact with an excavator.

Table 1 summarizes the pipeline data and the distributions adopted in the example, the impact scenario (i.e. impact energy distribution, tool width and length distribution, etc.) have been calculated using the method presented.

Variable	Distr. Type	Expectation	Std.Deviation
Yield Stress (MPa)	Lognormal	442	33
Thickness (mm)	Lognormal	13.4	1
Impact Energy (kJ)	Lognormal	23.7	7.21
Working Depth (mm)	Normal	1250	333
Tooth Width (mm)	Normal	27.5	7.5
Tooth Length (mm)	Normal	100	16.7
Diameter (")	Deterministic	36	
SMYS (MPa)	Deterministic	413	
Oper. Pressure (MPa)	Deterministic	7	

Table 1: Characteristic of the random variables and deterministic parameter

the impact scenario (i.e. impact energy distribution, tool width and length distribution, etc.) have been calculated using the method presented.

The calculated failure probability, i.e. the probability of having a puncture given the impact, is calculated to be 0.078 and the dimensions of the release area can be roughly evaluated from the tooth width and length giving the maximum contribution to the failure probability (26 and 96.7 mm respectively). The release area calculated in this way is only an estimate of the expectation of the leak area distribution; the actual leak area distribution is assessed by a Montecarlo simulation with Importance Sampling scheme.

Moreover, fixed the safety coefficient and the internal pressure, the effect on the puncture probability of changing the pipe diameter have been investigated. The pipeline wall thickness is related to the diameter by means of the following formula:

$$t = \frac{P \cdot D}{2 \cdot k \cdot SMYS}$$

and it is calculated fixing the safety coefficient  $k$  to 0.62 and the pressure to 7 MPa.

The resulting puncture probability, as a function of the pipe diameter, is shown in Fig. 3 for two different levels of impact energies; in both cases this confirms the behaviour shown by incidental data, that is that for a given safety coefficient and internal pressure the pipelines safety increase with the diameter, due to the increasing wall thickness.

Nevertheless the ratio between the 48" pipe and the 16" pipe puncture probability is quite different in the two cases, namely 40 for average impact energy of 24 kJ and 10000 for 8.1 kJ, showing that the availability of large amount of impact energy greatly reduces the importance of increasing the wall thickness.

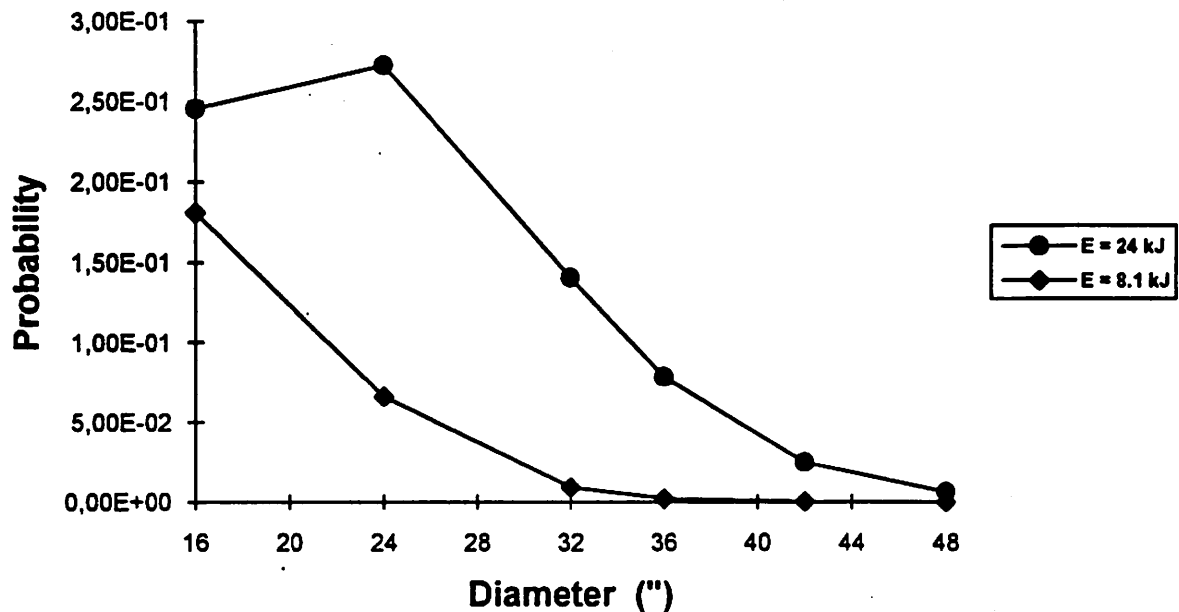


Figure 3: Calculated puncture probability vs. pipe diameter

## CONCLUSIONS

The main aspects of two procedures for the risk assessment of pipelines have been presented. The focus is on the possibility to perform a site-specific, design-specific analysis for the most important failure mode, i.e. the failure due to impact with third party activities. For offshore pipelines a simplified approach to the assessment of the probability of interaction with the human activities along the pipeline route has been presented. For onshore pipelines, an integrated approach to determine the impact scenario (in terms of impact energy and impacting object dimensions) and to assess the pipeline safety with mechanical reliability methods has been illustrated, together with a typical application example. The techniques have been applied in the risk assessment of offshore and onshore pipelines and has proven to be applicable and efficient within the context of the pipeline design process.

## REFERENCES

1. R.F. de la Mare, Y.L. Bakouros, Predicting the reliability of pipeline systems using the discriminant analysis technique. 8th Conference on Offshore Mechanics and Arctic Engineering, 1989
2. J.F.C. Brok, E.A. van Duyvenbode, L. Kilaas, An enhanced integrated methodology to determine the reliability function of a specific pipeline and riser system, *Reliability Engineering* 12, 1985
3. K.A.J. Williams, Application of risk assessment to pipeline and sub-sea systems. *Advances in Subsea Pipelines engineering and techniques*, 1990
4. R.F. de la Mare, O. Andersen. Pipeline Reliability. Veritas Report 80-0572, 1980

5. T. Andersen, A. Misund. Pipeline reliability: an investigation of pipeline failure characteristics and analysis of pipeline failure rates for submarine and cross-country pipelines. *Journ. of Petroleum Techn.*, April 1983
6. K.W. Blything. In service reliability data for underground cross-country pipelines. SRD Report R 326, 1984
7. A.G. Cannon, R.C. Lewis, C. Scrivener. The reliability of pipe systems operating in the British sector of the North Sea. Reliability 85 Conference, 1985
8. European Gas Pipeline Incident Data Group. Gas pipeline incidents. *Pipes and pipelines Int.*, Jul-Aug 1988
9. P. Hokstad. Reliability data for subsea pipelines. SINTEF Report STF75 A89037, 1989
10. J.S. Mandke. Evaluation of offshore pipeline failure data for Gulf of Mexico. OMAE Conference, 1990
11. A. Adams. UK Experience in offshore pipeline operations. II British Gas International Pipeline Piggings Conf., 1993
12. Zeepipe Development Project. Anchor Damage Study. Snamprogetti, 1991
13. Troll-Mongstad Conceptual Risk Analysis. Snamprogetti 1993
14. Lloyd's Register. Casualty returns 1978-1987
15. EEC. The maritime environment, traffic and casualties. COST 301 final report. 1987
16. Vassdrags. Influence of bottom trawl gear on submarine pipelines. Main Report Report 601124, 1975
17. R.E. Melchers. "Structural Reliability Analysis and Prediction". Ellis Horwood Ltd., 1987
18. A.H.S. Ang, W.H. Tang. "Probability Concepts in Engineering Planning and Design". J. Wiley, 1984



**085 Transportation Risk (II)**

*Chair: M. Kazarians, Kazarians & Assoc.*

**A Zone Model for Determining Atmospheric Contaminant Transport Aboard  
Human-Crewed Spacecraft**

*S. Jones, M. Paul, F. Issacci, I. Catton, G. Apostolakis (UCLA)*

**Commercial Space Transportation Regulation: An Evolution in Risk Management**

*R.K. Gress, D.E. Lang (USDOT)*

**System Safety Management in the UK Air Traffic Services**

*R. Profit (Natl. Air Traffic Services)*

## **A Zone Model for Smoke Transport Aboard Human-Crewed Spacecraft**

S. Jones, M. Paul, F. Issacci, I. Catton, G. Apostolakis

Mechanical, Aerospace and Nuclear Engineering  
University of California  
Los Angeles, CA 90024-1597

### **ABSTRACT**

A one-dimensional transport, deposition and agglomeration model for smoke particles has been developed for application to a microgravity environment. The purpose of this model is to determine the concentration of smoke as a function of time and space for application in a probabilistic fire safety assessment of habitable spacecraft. This concentration model is then used to determine the time until smoke detector response and the net deposition along the transport path. The latter can be used to determine the time until damage occurs to critical systems and/or human exposure.

The lack of a sufficient database of microgravity combustion information and the unknowns associated with the design of a human-crewed spacecraft introduce a great deal of uncertainty in the applying this model. Therefore, an input parameter sensitivity analysis was performed. However, this information was unavailable at the time of publication.

### **INTRODUCTION**

The risk to the crew from fires aboard spacecraft may be considerable. The crew must not only rely upon the spacecraft systems but also upon the maintainability of a breathable environment. Their lack of regress makes the threat of atmospheric contamination a significant issue.

All spacecraft materials must satisfy NASA fire safety requirements. Particularly, most of these requirements pertain to flammability. In an attempt to achieve a non-flammable wiring insulation with good mechanical properties, current applications implement various fluoro-

polymer wire insulations. Although these insulations do realize very admirable thermal characteristics, the products of thermal degradation do pose a significant health hazard.

One of the foremost threats to wiring thermal integrity is the threat of excess current flow. These excess current loads, ranging from low trickle currents to full short-circuits, generate heat via ohmic heating. This heating can be sufficient to promote thermal degradation of the wire insulation.

The evaluation the consequences of an overloaded wiring event consists of a temporal competition between the time for damage to occur and the time for detection, suppression and mitigation. A key element in this evaluation is the development of models which can predict the source, transport and deposition of offending species as a function of time and space.

For example, suppose a wire were to overheat at location A within some chamber. To predict the detection time, one must determine the concentration of smoke at a smoke detector at location B. The model required must not only quantify the source of smoke generated as a function of time, but also the transport of smoke from A to B. Furthermore, the deposition along the path must also be described to determine the attenuation of particulate concentration. Additionally, one may be interested in the time for smoke damage to occur of some key system located at position C within the chamber. As before, one must develop models for the source, transport and deposition of smoke particulates from the source at A to the target at C. Once these models are developed, the detection and damage times are simply the time at which some crucial threshold limit of smoke concentration at that point is achieved.

Microgravity environment experiments naturally focus upon quantifying the source of potential threats. All other aspects of the problem, given an event has occurred rely upon determining the nature of the generated species. To quantify the source of smoke, for example, one must know the rate of smoke produced and the size distribution of particulates generated. Subsequent smoke transport and deposition calculations and hence damage and detection time estimates are dependent upon an accurate assessment of these values.

Regardless of how accurately we attempt to model the transport and deposition of smoke particles, substantial uncertainties will still remain. Not only does substantial uncertainty exist in the model parameters, but inherent to the models themselves are assumptions which introduce uncertainty. Additionally, uncertainty is introduced due to geometrical concerns. Because a specific design of a human-crewed spacecraft is not the focus of this study, scenario specific parameters such as the geometrical configuration of the chamber.

A probabilistic assessment of the models of transport and deposition determines the sensitivity of the final result (damage time or detection time) to variations of the input parameters. Each input parameter is assigned a probability density function which signifies the state-of-knowledge of the value of that parameter. Parameters that are well known have very narrow probability distributions, while those parameters with large uncertainty have wider distributions. Once distributions have been assigned to each of the model input parameters, a Monte Carlo simulation (or similar technique) can be used to determine the distribution of the model output.

## MODEL DEVELOPMENT

To develop models for the transport and deposition of smoke, one must first determine which mechanisms are dominant or crucial to generate accurate predictions. In an ideal world, one could model all phenomena regardless of their actual contribution. However, due to the fact that multiple iterations must be performed for a parameter sensitivity analysis we must limit our modelling efforts to the dominant phenomena. However, due to the uncertainty associated with the scenario of interest, the model must be general enough to accommodate many configurations. For example, the modelling of transport must include the mechanisms of convection and Brownian motion. Although the effects of Brownian motion (ordinary diffusion) may be negligible when compared to convective transport, it must be included to account for situations with no flow. The development of the one-dimensional transport model for smoke begins with these two mechanisms.

We have developed a computer code which consists of one-dimensional model for the transport and deposition of smoke particles in a channel flow configuration. The size of the channel is an input because of the inability to define a specific scenario. This channel is divided into a number of control volumes, each of which may contain a source of particulates. The assumption is made that the concentration is uniform over each control volume. The source term and ambient flow rate used by the computer code are treated as user defined input.

The computer code output is the concentration of smoke within each of these control volumes as a function of time. Further refinement of the computer code will include the simulation of a smoke detector in one of the control volumes by recording the time at which a specific threshold concentration is surpassed.

As stated above, the one-dimensional smoke transport and deposition model begins with convection and ordinary diffusion. Other transport mechanisms are either too scenario specific, such as thermo- and electro-phoretic effects, or are deemed to be negligible. Convective motion is straightforward, but diffusive motion includes some rather interesting wrinkles. To determine the diffusion coefficient of an entrained particle we must know the particle diameter. Given this information, the calculation of diffusion coefficients follows well established techniques. Furthermore, since the diffusion rate and detector threshold is dependent upon the particle size, we must determine the particle size distribution as a function of time and space. This requires the development of a particle agglomeration code to predict the size distribution as a function of time. It has been shown that particles agglomerate into clusters. These clusters have different transport characteristics than their individual particle counterparts. The existing theoretical and empirical models for this agglomeration behavior are extremely limited in application to a microgravity environment due to the absence of sedimentation effects. The computer code assumes an exponential growth of cluster size.

The deposition of particulates is assumed to occur at the boundaries of each of the control volumes. Determination of the deposition is key to quantifying the time to damage of smoke sensitive equipment and also in determining the attenuation of the net number of particles with time.

The method of calculation used in the transport model takes advantage of the heat transfer - mass transfer analogy. Incorporating well established heat transfer correlations, the model accounts for deposition via diffusion through a boundary layer. Other deposition mechanisms

such as thermo- and electro-phoretic effects are neglected since these are scenario specific. The computer code allows the user to input the flow velocity. Once solving for the flow conditions, the code automatically selects the corresponding mass transfer relationship to determine the deposition coefficient.

Analyses are underway which will determine the applicability of the above computer code. To test the validity of the model, a specific scenario will be simulated and an input parameter sensitivity analysis is to be performed. This sensitivity analysis will take the form of a Latin Hypercube simulation.

## CONCLUSIONS

A one-dimensional model for the transport, deposition and agglomeration of smoke particles has been developed for application to channel flow in a microgravity environment. The input parameters include the spatial dimensions, the smoke production rate and the ambient flow velocity. Model output is the detection time and the net deposition along the path from which one can generate estimates of the time until damage occurs.

The work in progress constitutes a Latin Hypercube simulation to account for the parameter uncertainty. Distributions are being developed for the input parameters. Mean values of these distributions are taken from experiment data, smoke detector specifications and geometrical configurations of the proposed space station design.

The development of this model may have extensive use in a safety assessment of the threat to station systems and crew from smoke particulates. This model can be used as a predictive tool for determining the smoke exposure to both the crew and critical systems within the craft. In addition, since the model can be used as a predictive tool for smoke detector response, this model may be used a design tool for the fire safety manager.

## **COMMERCIAL SPACE TRANSPORTATION REGULATION: AN EVOLUTION IN RISK MANAGEMENT**

**Ronald K. Gress and Derek E. Lang**

Licensing and Safety Division  
Office of Commercial Space Transportation  
U.S. Department of Transportation  
400 7th Street, S.W., Room 5402A  
Washington, D.C. 20590

### **INTRODUCTION**

The first commercial space launch licensed by the U.S. Department of Transportation's Office of Commercial Space Transportation (OCST) was conducted in 1989. Since then, OCST has issued over 27 licenses to commercial space launch companies and overseen more than 35 licensed launches. The number of commercial space launches projected by U.S. industry steadily rises and the innovative industry continues to develop new concepts in space transportation. These include new vehicles and launch concepts such as orbital launch vehicles released from aircraft and launched from the sea. There are concepts for single-stage-to-orbit vehicles capable of returning to earth. These reusable vehicles would be designed to incorporate aircraft-like maintenance and turn-around characteristics. In addition, new industry initiatives such as individual constellations of up to 60 or 70 communications satellites in low earth orbit and reentry vehicles also present new safety issues.

The risk management framework necessary to assure that these activities are conducted safely is challenged to evolve with an industry that is not only becoming more diverse, but also more complex. OCST is challenged to assure public safety while maintaining a robust regulatory program that easily accommodates industry's innovations and growth. This paper provides a summary of the development of OCST's risk management program and illustrates the complexities of managing risks for a new industry.

### **RISK MEASURES AS A REGULATORY DECISION TOOL**

Federal Executive Order No.'s 12498 and 12291 direct safety regulators to use risk assessments to assure safety regulations address real and significant risks to public safety and base regulatory actions on the potential costs and benefits. Similarly, risk assessment

is a principal component of OCST's licensing and regulatory decisions on a case-by-case basis. For example, OCST requires that all license applicants identify and address the public safety risks posed by the proposed operations as part of their application. The applicants conduct failure analyses and calculate the resulting hazards due to launch, overflight of populated areas, and eventual reentry of the launch vehicle back to earth after reaching space. These risks are commonly measured in terms of expected values, or expected casualties, as defined by Equation (1):

$$E_c = \sum_i P_i \frac{A_{Hi}}{A_i} N_i \quad \text{Equation (1)}$$

where  $E_c$  = Expected casualty

$P_i$  = Impact probability density

$A_{Hi}$  = Hazard area associated with an impact on  $A_i$

$A_i$  = the area in which debris impacts can occur

$N_i$  = Number of people in  $A_i$  at risk

Some examples of the resulting estimated risks associated with the overflight of land masses during the launch phase of various launch vehicles are provided in Table 1.<sup>1,2</sup>

Launch Vehicle	Launch Site	Flight Azimuth (deg)	Overflight Expected Casualties (per event)
Delta 6925	Cape Canaveral AFS, FL	95	$3.7 \times 10^{-6}$
Atlas Centaur	Cape Canaveral AFS, FL	90	$4.0 \times 10^{-6}$
Scout	Wallops Island, VA	90	$8.47 \times 10^{-7}$

Table 1. Example Launch Land Overflight Risks

In addition, OCST implements a statutory risk-sharing regime by setting insurance requirements to cover maximum probable third party and government property losses resulting from the launch operations. OCST uses a risk-based analytical concept to determine "Maximum Probable Loss." This methodology identifies the maximum loss accident scenario that has a probability of occurrence greater than the threshold which has been set by OCST. Based on an analysis of the accepted risks in other currently regulated activities, the threshold probabilities were set at one in ten million for third party casualties and one in one hundred thousand for government property losses that may result from the licensee's launch activities. While it is *possible* that losses could exceed the resultant insurance requirements, it is not *probable*. Typical insurance requirements using this concept have ranged from \$1-164 million depending on the computed risks.<sup>3</sup>

As technology progresses into new realms and space activities become more visible to the public, OCST continues to refine and develop new risk management tools to fulfill its safety responsibilities. OCST has utilized performance criteria to which applicants must design and operate their systems in developing special approval criteria for the COMET reentry vehicle which is designed to return from earth orbit to a designated landing site. Current plans call for the COMET reentry vehicle to land by parachute in Utah. Because this would be the first commercial ballistic reentry vehicle to land on the continental United States, it was important to develop safety criteria that would address the public's safety

concerns and promote acceptance of this new transportation activity and yet not inhibit potentially innovative design and operational approaches by the applicant.

The first criterion limits the number of estimated off-site landings to no more than three in one thousand in order to assure that the vehicle will perform as intended. The other two criteria limit the probability of any casualty (which includes serious injury) to the local and global populace to no more than one in a million. In the case of these latter criteria, using *probability of any casualty* versus *expected casualty* shifts the focus from a more abstract concept to a more direct consequence of an off-site landing (e.g., the remote likelihood of occurrence of any casualty). Yet, a simple mathematical proof can be used to show that this form of risk measure can be computed with the same level of complexity necessary to calculate expected casualty.<sup>4</sup>

## PROBLEMS IN RISK QUANTIFICATION

Because analytical risk methodologies are not an exact science, quantifying risks for the purposes of developing regulatory requirements is not always easy. In some cases, traditional methodologies do not adequately characterize the true risks. For example, the models for predicting risks due to objects that decay from orbit and randomly reenter back to earth were developed in the early 1960's for U.S. Government programs.\* In the context of regulating commercial activities, these models sometimes predicted risk levels which appeared very conservative and inconsistent with the limited empirical data available. Some risk estimates implied that random reentries of rocket motors left in orbit would impact close enough to individuals to be readily observed, or result in other observations (such as holes in roofs), on an annual basis; yet finding this type of evidence is rare. Reexamination of these models suggest that additional research in the areas of likelihood of survivability of a reentering object, the surviving object's characteristics (e.g., size, ballistic coefficient, terminal velocity), the effects of sheltering, variations in population distribution, and even the time of day, may provide more accurate predictions.

Often there is insufficient empirical data to accurately conduct the reliability analyses necessary to conduct risk assessments. For example, the number of times vehicle components have been flown in space simply is not enough to be able to develop statistical distributions with any statistical confidence for assessing reliability. Performance for solid rocket motors which can only be fired once must be analyzed based on empirical data collected from static tests on the ground and rely on manufacturing quality control to maintain repeatability. Similar problems exist with high cost, limited production composite structures where analytical methodologies can estimate strength characteristics, but reproducibility is based on almost "engineering model-shop" manufacturing processes.

In other instances, traditional methodologies for measuring risks may not be useful for regulatory decision-making purposes. In the case of on-orbit collision probabilities, the scientific measure of risks has typically been the time between collisions, usually on the order of  $10^4$  to  $10^5$  years for low earth orbiting objects for example.<sup>5</sup> From a risk management perspective, space operations and subsequently the space environment will undoubtedly change significantly before even the lower bound is reached. Thus, a more meaningful risk measure may be more desirable for making regulatory decisions about how commercial space operations are conducted. Because these risk assessment tools have limitations, OCST continues to conduct research to develop new tools and approaches that will allow OCST to make effective and judicious regulatory decisions.

---

\* Events like the reentry of NASA's large Spacelab or Soviet satellites containing nuclear power sources were extreme examples of this situation, but they heightened concern of reentering objects from orbit.



## RISK MANAGEMENT CHALLENGES

There are many challenges in effectively and efficiently managing the risks to the public from commercial launch activities. The discussion below raises just a few important examples of the issues that affect the risk management process from a regulatory perspective.

The growth and dynamics of the commercial space transportation challenge OCST to assure that its licensing requirements keep pace with industry's innovations while maintaining public safety and public acceptance of commercial launch activities. One approach used by OCST to develop regulatory requirements that will not hinder industry is to rely on performance criteria, i.e., define safety goals versus specifying methods for achieving safety. Performance criteria provide industry with a great deal of flexibility in choosing how to design and operate a vehicle, as long as it is capable of clearly and adequately demonstrating that the choices satisfy the safety criteria. However, in making design decisions, facing general high-level performance-based safety criteria can present a difficult problem to a company compared to the imposition of very specific design specifications. This performance-based approach relies heavily on the maturity of the applicant and may pose problems when the applicant must decide how it might approach its safety demonstrations and what approaches would be acceptable to OCST. Thus, the added flexibility provided by performance criteria may actually create additional costs to the applicant in trying to find an acceptable methodology for demonstrating safety.

Moreover, developing criteria that provides flexibility while maintaining safety requires significant research. For example, in developing criteria for the safety evaluation of commercial launch sites, one might assume that because the government has been involved in conducting launches and operating launch sites safely for over 45 years, current operating practices at government launch sites would be appropriate regulatory requirements to ensure public safety. However, this is not necessarily the case. While commercial space launch activities should be regulated only to the extent necessary to assure public safety, examination of the historical evolution of government launch site "safety" requirements shows that many requirements had little, or no, relationship to public safety, but rather were driven by other important mission-oriented concerns. For example, the requirements for redundant tracking (e.g., radar) systems resulted from the destruction of a perfectly good launch vehicle and its payload because of a loss of the single tracking system. No longer being able to determine the location and movement of the vehicle and to ensure that it had not changed direction such that the public would be exposed, the vehicle was destroyed. Thus, the requirement for redundant tracking systems was introduced more to improve mission success than to protect the public. While the dual role of redundant tracking meets the needs of mission success and public safety, the regulator's concern is to develop requirements to assure public safety and not mission success. Thus, OCST's functionality studies and risk analyses designed to understand the "real and significant" hazards posed by launch operations and the dynamic interrelationships between launch personnel, procedures, safety equipment and risk are being used to develop appropriate requirements to assure public safety.

Voluntary industry standards may be one solution to retaining the flexibility offered by performance criteria, yet providing an applicant guidance in determining what safety demonstrations will satisfy OCST. In other fields where industries have developed their own standards, the respective Federal regulatory agencies, such as the Federal Aviation Administration and Nuclear Regulatory Commission, have adopted these standards as part of their regulatory framework. This "self-regulation" streamlines the Federal regulatory process and creates a cost-effective means for industry to assure public safety. Such standards might cover component interfaces, hardware design margins, and analytical methodologies for estimating reliability or risk. Voluntary industry standards also retain

the flexibility of offering a number of acceptable options from which an applicant may choose. OCST initiated a workshop as a catalyst for commercial industry to examine the potential benefits of voluntary industry standards.

OCST has also developed several aids to assist applicants in analyzing the risks posed by their proposed operations. Prior to the creation of the commercial launch industry, the government typically conducted launch operations and took responsibility for assessing safety, and early license applicants did not know how to approach the problem of determining the risks of collision with other orbital objects. Therefore, OCST developed a relatively simple tutorial to educate the companies on how to measure the probability of a collision and aid these companies in understanding the risks posed by their proposed operations.<sup>6</sup> OCST does not require the use of the methodologies described in the aids, so applicants may choose to use other approaches, the validity of which will be assessed by OCST on a case-by-case basis.

Public acceptance of commercial space transportation activities is also important. Unlike National Aeronautics and Space Administration (NASA) or Department of Defense (DOD) programs which are conducted by the government for national interests, hazardous commercial activities (whether space-related or otherwise, such as airports, nuclear power plants and transportation of hazardous materials) confront public scrutiny before being allowed in the public's "backyard." Drastic changes in the type of operations or how operations are typically conducted understandably raise public concerns. For example, the final preparation of satellites prior to launch typically includes many hazardous activities including the handling of explosives and fueling activities that include highly volatile and toxic propellants. For government operations, these preparations had always been performed in remote areas, but a commercial company opened up a facility within a city adjacent to a launch range. Public concern regarding the potential dangers led OCST and the Environmental Protection Agency to jointly perform an assessment of the potential accidents and the public exposure for a worst case incident. The study examined the facility's design criteria which was markedly different from that of the government's, its operating policies and procedures, the use of Fault Tree Analyses and vapor dispersion models given an explosion and release of toxic materials. The study found that the new technology used in the construction and operation of the facility resulted in operations that are safe to the public and even under worst case conditions, there was a significant safety margin.<sup>7</sup> Thus, OCST's interactions with the public are an important part of addressing concerns and maintaining public confidence in the safety of commercial space transportation activities.

## CONCLUSION

In summary, OCST continues to refine its use of risk assessment tools and its risk management program to assure safety in a growing and dynamic commercial environment. OCST must address a broad spectrum issues, similar to the Nuclear Regulatory Commission, Environmental Protection Agency, and Food and Drug Administration, in order to protect public safety and give the public confidence in space transportation activities. In some cases, public safety is identifiable and quantifiable; while in others, the need for assurance of safety is a function of public perception and confidence. Thus, there is a need for continued balance between industry growth and public education. OCST has made a commitment to utilizing performance criteria to the extent possible to allow flexibility to the industry and allow industry to be innovative, while maintaining adequate levels of safety. At the same time, OCST continues to educate the industry and the public as part of its risk management strategy for assuring safety.

## REFERENCES

1. "Commercial Launch Baseline Assessment: U.S. Air Force Eastern Space and Missile Center," U.S. Department of Transportation/Office of Commercial Space Transportation, Washington, D.C. (1988).
2. "Commercial Launch Baseline Assessment: NASA Goddard Space Flight Center Wallops Flight Facility," U.S. Department of Transportation/Office of Commercial Space Transportation, Washington, D.C. (1989).
3. R.K. Gress, Derivation of maximum probable loss for commercial launch operations, *Proceedings of the International Conference on Probabilistic Safety Assessment and Management*, (1991).
4. "Impact and Kill Probability Procedures," SSD-TDR-64-138, Space Systems Division Air Force Systems Command, Los Angeles, pp. 145-148 (1965).
5. "Hazard Analysis of Commercial Space Transportation", U.S. Department of Transportation/Office of Commercial Space Transportation, Washington, D.C. (1988).
6. "On-orbit Collision Hazard Analysis in Low Earth Orbit Using the Poisson Probability Distribution," U.S. Department of Transportation/Office of Commercial Space Transportation, Washington, D.C. (1992).
7. "Safety Evaluation of Astrotech Payload Processing Facility, Titusville, Florida", U.S. Department of Transportation/Office of Commercial Space Transportation and U.S. Environmental Protection Agency, Washington, D.C. (1990).

## SYSTEM SAFETY MANAGEMENT IN THE UK AIR TRAFFIC SERVICES

RICHARD PROFIT

United Kingdom Civil Aviation Authority  
National Air Traffic Services  
CAA House  
45-59 Kingsway  
London WC2B 6TE

### Introduction

Formal risk assessment techniques were first applied in the United Kingdom civil aviation industry in the early 1960's in the evaluation and certification of aircraft for "all weather operations". Risk assessment has also played an important part over many years in defining the safety standards for the air traffic services, perhaps most significantly in the definition of aircraft separation criteria for North Atlantic traffic. However, unlike the process used in the certification of aircraft systems, less attention was paid in the past to the application of structured risk assessment programmes to air traffic service engineered systems, procedures and the air traffic controllers' task.

There is a well-established culture within the UK Civil Aviation Authority that '*safety is the primary purpose of air traffic control (ATC)*'. However, a safety review conducted in 1990 concluded that safety cannot be applied intuitively and there was a clear requirement for the introduction of a formal Safety Management System within the UK National Air Traffic Services (NATS), particularly in the light of the public inquiries into recent public transport and off-shore oil industry disasters, where management failures were seen as contributing causal factors. An important aspect of this more formal approach to Safety Management has been the adoption of a structured programme of risk assessment in the design of new air traffic service systems and the presentation of the results by means of Safety Cases - on similar lines to the approach used for a number of years in the UK's Nuclear Industry. In simple terms, a Safety Case defines the system safety requirements and presents the evidence, arguments and assumptions used to show the degree of compliance with these requirements.

The completed Safety Case provides an assurance to the managers who are responsible for the safety of ATC operations, and also to the regulatory authorities, that the potential hazards of a new system and its associated procedures have been identified and appropriate controls provided. Furthermore, a Safety Case remains a 'live' document once a new system is in operational service, and it is maintained to provide continued assurance

that safety management procedures are in place to ensure that the design, construction, maintenance and operation of the system continue to meet the safety objectives throughout its life cycle.

### **Basic Principles of Safe Air Traffic Control**

In order to define the context for risk assessment it is necessary to consider the structure of the current air traffic control system to identify the built-in safety features that have withstood the test of time so far. Commercial air transport flights are normally confined to protected airspace under the control of a specific ATC agency. There are demanding licensing requirements for pilots to fly in this controlled airspace and equivalent requirements for the controllers providing the air traffic control service. To interface the two, suitable air/ground communications and navigation facilities are available along the airway routes.

To avoid route conflicts between aircraft, plans for intended flights are first submitted by the aircraft operators to the ATC agencies concerned. Departure rates from airports are regulated to reduce mid-air congestion and safe separation between aircraft is maintained by the use of radar to resolve possible conflicts, or by procedural methods where radar cover is not available. Radar plays a vital part in ensuring safety while expediting traffic flow and permitting maximum utilisation of the limited airspace capacity available, over western Europe in particular.

From the ATC perspective, safety is achieved through the maintenance of clearly defined and internationally agreed separation criteria between individual aircraft. The dimensions of the volume of airspace assigned to each aircraft are designed to allow for the performance accuracy of the surveillance radars and navigational aids in use, aircraft navigation and altimeter accuracy, and human factors that could erode safety levels.

The objective of this complex system of air traffic control is to maximise traffic flow while minimising the risk of a mid-air collision - potentially the most catastrophic type of accident that could be caused by an air traffic service or where the service might be cited as a contributory factor. There are other types of accident where the air traffic service could be a causal factor, but the focus of this paper is the risk of a collision caused by a loss or degradation of air traffic control. Any changes to the equipment and procedures that constitute this well-proven system need to be subject to thorough assessment if the excellent safety record is to be maintained.

### **NATS Safety Analysis Programme**

NATS' key safety policy is to minimise the risks of causing an aircraft accident as far as is reasonably practicable. It follows that the risk assessment process requires judgement on a tolerable level of risk for those aspects of aircraft operation that are within the ability of the air traffic services to influence. As part of the safety case process, all new systems are screened for their safety significance from the outset and a safety analysis programme is undertaken for each system found to be safety related. (As well as the manufactured equipment, the definition of a 'system' includes the supporting facilities, procedures and people that in combination achieve an air traffic service function). The analysis programme covers all phases of system development and operation. The programme is conventional in that hazards arising from failure conditions in the system are identified and then analysed to determine their severity. The probability of occurrence is estimated and it is then possible to assess whether the risk of such an occurrence falls within what is tolerable to NATS.

This is an iterative activity throughout the design and development process and responsibility for detailed hazard analysis will often be delegated to the contractor. The results of this activity are incorporated in the Safety Case. Hazard analysis affects design, and in an ideal world, the result would be a system that was hazard free. In practice, it should at least be possible to ensure that new systems contain no surprises and a strategy should be in place to control any unresolved hazards that remain. This process obviously requires a close working relationship between the equipment manufacturers, the project management teams and the safety regulators.

### **Hazard Identification and Analysis**

Once an adequate system definition has been established, a Preliminary Hazard Analysis is undertaken. At this stage the focus is on the functions and vulnerabilities of the system rather than on detailed analysis; the aim is to define clearly what constitutes a failure condition of the system. Having identified the hazards, the preliminary hazard analysis evaluates them to determine their severity and, if possible, provides an initial estimation of their probability of occurrence. Preliminary Hazard Analysis may well lead to a modification to the design to eliminate some of the hazards or to mitigate their consequences. On completion of the Preliminary Hazard Analysis, with any necessary iteration to accommodate design changes, those features of the system requiring detailed assessments are identified for incorporation in the safety assessment plan. The process is extended in parallel with the development programme to include sub-systems, environment, software and further design changes.

### **Hazard Classification.**

Most hazardous industries, including the aviation industry, use the severity of accidents or degree of loss as a basis for hazard severity classification. But for ATC we have adopted a different approach because the probability of a mid-air collision resulting from the loss of ability or failure to control aircraft cannot be estimated in the same way. This is because the dimensions of the airspace assigned to individual aircraft are, as far as is reasonably practicable, large enough to reduce the probability of random collisions and give sufficient reaction time for the air traffic controllers, pilots or on-board collision avoidance systems to avert such an event. It follows that maintenance of aircraft separation standards is fundamental to a safe ATC service. Separation standards cannot be maintained if air traffic control is lost as a result of equipment failure, and sudden total loss of the ability to control air traffic must therefore be regarded as the worst case event, even though a mid-air collision may not be the result. This is the basis of NATS approach to Hazard Severity Classification. Hazards are classified according to the severity of their affect on ATC, taking into account exposure time to the hazard, availability of fallback systems and the subsequent effects on system capacity and controller workloads. The effects on ATC are manifested as loss or degradation of the control function. The following definition of the highest category of air traffic system hazards illustrates the rationale:

A Category 1 hazard is defined as a sudden inability to provide any degree of air traffic control within one or more airspace sectors for a significant period of time. In other words, controllers have no possible means of controlling aircraft and separation will be eroded. The most obvious example would be a total loss of communications between controller and aircraft in a given sector of airspace for longer than a critical time period.

There are three lesser categories of hazard used in NATS analyses which are defined in terms of varying degrees of degradation of the ability to control aircraft and the likely consequent effect on the ability to maintain safe separation.

### Probability Classification.

The next stage in NATS approach is to estimate or define the probability of a particular hazard occurring. Probabilities are likely to be expressed in qualitative and/or quantitative terms, thus it is necessary to have both types of definitions. The units are in terms of probability of event per operational hour in an ATC sector - a sector is a division of airspace.

**Table 1. Probability Classification.**

Probability Class	Qualitative Definition	Quantitative Value $P_s$ (Probability of event per operational hour per sector)
Frequent	Likely to occur often.	$P_s > 10^{-3}$
Probable	Likely to occur many times during system life.	$P_s = 10^{-3}$ to $10^{-4}$
Occasional	Likely to occur sometime during system life.	$P_s = 10^{-4}$ to $10^{-5}$
Remote	Unlikely to occur, but possible.	$P_s = 10^{-5}$ to $10^{-6}$
Improbable	Very unlikely to occur.	$P_s = 10^{-6}$ to $10^{-7}$
Extremely Improbable	Extremely unlikely, if not inconceivable, to occur.	$P_s < 10^{-7}$

### Tolerability Of Risk.

Having defined severity and probability of a hazard, an estimate is made of the risk associated with the hazard. Obviously the more severe the potential hazard the less tolerable the risk of it occurring. For any severity category, a tolerable level of risk has been classified according to the probability of occurrence. There are four classification bands:

A: Unacceptable.

B: Undesirable, but may exceptionally be acceptable with the approval of the Director General Air Traffic Operations - the principle risk 'owner' in NATS.

C: Acceptable with the agreement of the Operating Authority - usually the General Manager of the unit that will be operating the new system.

D: Acceptable.

**Table 2. Risk Tolerability Classification.**

Probability of Event per Operational Hour per Sector		Severity CAT 1	Severity CAT 2	Category CAT 3	CAT 4
Frequent	$>10^{-3}$	A	A	A	C
Probable	$10^{-3}$ to $10^{-4}$	A	A	B	D
Occasional	$10^{-4}$ to $10^{-5}$	A	A	C	D
Remote	$10^{-5}$ to $10^{-6}$	A	B	D	D
Improbable	$10^{-6}$ to $10^{-7}$	B	C	D	D
Extremely Improbable	$<10^{-7}$	C	D	D	D

The table indicates the probability with which a particular hazard can be tolerated per operational hour per sector. In some cases, particularly for Category 4 events, failure probabilities that are tolerable from the safety aspect may not be acceptable for commercial reasons. Lower probability levels would then be required with a cost benefit justification rather than safety risk.

### **Products of the Risk Assessment Process**

This risk assessment scheme provides a number of products that play an important part in safety management. For example:

- It provides a means of identifying and quantifying safety requirements which can then be translated into reliability and integrity requirements for system components. These are the specified safety targets that contractors would be expected to meet.
- The requirements provide a target for assurance activity and hence the focus of the system Safety Case. Where there are system performance shortfalls, and the risk of hazards not reduced to a tolerable level, mitigation actions can be put in place to control the risk while remedial action is implemented.

### **Role of the Safety Case**

All of these activities can be controlled using the system Safety Case as a primary management document, and this document provides the basis for the safety assurances required by both the operational managers and the safety regulators. Developed properly, a new system safety case can deliver the following benefits in addition to safety assurance:

- Reliability and integrity design features are prioritised according to the safety significance of the system. This avoids over-engineering less critical components.
- Shortcomings (potential hazards) are identified so that residual risks can be managed until rectification can be implemented.
- Cost savings can be made by reducing unforeseen system deficiencies. In other words, there should be a reduction in system outages and the consequent need for in-service modification and rectification.



- Measurement of system performance gives a true measure of both the quality of the Safety Case and the effectiveness of Quality Management within NATS. This is feedback to which most people can relate and see results of their activities as tangible benefits.

### **The Human Factor**

The previous sections have described the formal risk assessment approach adopted by NATS for engineered systems. However there remains another aspect that has not yet been subjected to formal hazard analysis, and this is the human factor element - the dominant cause of ATC safety related incidents.

The experience of other industries has shown that the satisfactory treatment of human errors gives rise to one of the most difficult problems in quantitative risk analysis, that of Human Reliability Analysis (HRA). HRA includes any method by which human reliability is estimated. Studies have shown there is a wide disparity in the effectiveness of existing HRA methods and that there are serious problems in performing HRAs regardless of the method in use. The tasks of both controller and pilot involve a significantly larger proportion of human intervention than is the case with process operators workers in other industries on which previous work has concentrated.

The fact that there are problems should not necessarily deter attempts to perform HRA. The experience would help identify areas in which further research is most needed and even if it proves difficult to quantify probabilities in some areas, the analysis may still highlight the aspects of the controllers' and pilots' tasks that contribute most to the risk. NATS is currently undertaking a trial application of formal risk assessment to ATC operations, including the human factors component, with the aim of assessing the feasibility of the approach and identifying the areas in which more research is needed. Even if we are not successful, the trial should at least highlight where there is a human factor dependency, even though the analysis may not be able to proceed from there.

### **Conclusions**

Since 1950 there has been a dramatic improvement in the safety of scheduled air services. However, public perception of the risks of flying is not related to accident rates per flying hour or passenger-kilometres. It is more probably related to the number of recent accidents - accidents per annum - and this yearly total has been broadly constant because of the growth in air traffic.

As air travel is expected to double in terms of annual passenger hours flown by the year 2005, the number of accidents per annum could rise, even though the accident rate remained constant. Hence there could be a perception that flying was becoming more dangerous. The downward trend in accident rates must therefore be maintained if we are to sustain high public confidence in air transport safety. Human factors, from both the pilot and air traffic controller's perspective, provide the greatest uncertainties for risk assessment, and will be a key development area. In addition, technology will continue to play a pivotal role in the coming years and systems complexity will continue to increase. Significant changes are on the horizon in communications, navigation and air traffic management that will bring about the need to consider air transport as a totally integrated system involving airborne, ground and satellite systems. Risk assessment techniques for the identification of safety and reliability requirements will need to be refined and adapted to ensure that these developments make a positive contribution to air transport safety.

**086 Impact of Different PRA Methodologies on the Results of  
Nuclear Power Plant PSAs (II)**

*Chair: J.H. Bickel, INEL*

**The Search for Dependencies or How Could Two Current Design Nuclear Power Plants  
Produce IPE Results Three Orders of Magnitude Different?**

*F.R. Hubbard (FRH); A. Mosleh (U. Maryland)*

**Impact of Methodology and Design Changes on Turkey Point IPE Results**

*C.N. Guey, W.A.Skelley (Florida Pwr. & Lt.)*

## **THE SEARCH FOR DEPENDENCIES OR HOW COULD TWO CURRENT DESIGN NUCLEAR POWER PLANTS PRODUCE IPE RESULTS THREE ORDERS OF MAGNITUDE DIFFERENT?**

Frank R. Hubbard,<sup>1</sup> Ali Mosleh<sup>2</sup>

<sup>1</sup>FRH, Inc.  
P.O. Box 65359  
Baltimore, MD 21209

<sup>2</sup>Department of Nuclear Engineering  
University of Maryland  
College Park, MD

### **ABSTRACT**

Individual plant examinations (IPEs) which are available for similar plants, report widely different core damage frequencies. Core damage frequencies vary by as much as three orders of magnitude when using modeling methods that could produce similar results for similar plants. This paper poses one of the central issues to be discussed during a session where results will be presented from a number of IPEs and compared. Its result section will ultimately only be written after the session is over.

### **DISCUSSION**

The objective of this session is to examine the extent to which such large differences may result from differences in modeling dependencies. The dependencies to be discussed are specifically those between related systems, between redundant trains of individual systems, and between multiple operator actions in the same scenario. Experience has shown that other differences in IPE modeling can probably not result in differences as great as two orders of magnitude in core damage frequency for similar plants. These other differences include differences in plant design and operation. Risk assessment is an art which is sufficiently mature so that the experience data for components and initiating events is basically shared by all practitioners. The same analyst modelling two similar plants would probably not produce drastically different core damage frequencies, even when she/he uses plant specific input data. The implications are that approaches to modeling and the degree to which actual plant performance is modeled may be an important cause for large differences in core damage frequency. It is further postulated

that the more detailed the plant model is made, the higher the core damage frequency. More detailed probably means more accurately accounting for dependencies.

If differences in results for similar plants are mainly due to differences in representation of dependencies, and since NUREG-1335 is not asking the licensees to report much detail about such differences, then reviewers are left with two alternatives:

1. to regard any IPE that reports core damage frequency values that are too low as being inaccurate

or

2. to examine in exhaustive detail all the differences, to insure that both the high CDF and the low CDF submittals are acceptable

Differences in core damage frequency of greater than one order of magnitude for two plants which are of similar design can probably not be produced by differences in input data. That is, they probably not be produced by using different component failure rates or initiating event frequency data. Neither can enhanced redundancies between comparable systems or different plant model quantification methods account for differences of greater than one or two orders of magnitude..

There seems to be no reason to believe that the use of different intersystem modeling methodologies, i.e. the use of large vs small event trees, should produce large differences in CDF. However, the use of large event trees may contribute to a propensity for modeling dependencies in more detail. Forcing the analyst to be more explicit about scenarios may lead to more dependencies being flushed out. Since a missed dependency can turn a  $10^{-2}$  redundant train into a guaranteed failure, it may be possible to make large changes in core damage frequency from small differences in dependency. The most significant dependencies, those which are capable of producing the largest swings in core damage frequency, are most those from support systems. To produce a four order of magnitude difference, however, would require numerous differences in treatment of support system dependencies. (Only recently have tools been available for making very clear what the dependencies are that are built into large logic models such as those built into the RISKMAN® large event tree models. Rule\_Tester by FRH, Inc. is one such microcomputer analysis tool.)

Although differences in component failure rates or initiating event frequencies may not produce large differences in core damage frequency, common cause failures between like components in redundant trains if not accounted for in detail may produce larger differences

Two operator actions which inadvertently appear in a single scenario without being treated as dependent may also considerably skew IPE core damage frequency results. By the time that IPE models are complete they usually include numerous (~50) manual actuation and recovery/repair actions. It is easy, if two of these actions occur in the same event (scenario), and their dependence on each other is not recognized, to inadvertently reduce the frequency of a scenario by two orders of magnitude. Each action that occurs in a single accident scenario is depend on the preceeding actions in that scenario. For example, if the first action fails then the success of the second one in the scenario may be considerably reduced since almost all actions during any scenario are crew-based, i.e.. they are decided on and acted upon by the plant operations team directed from the control room not by individuals acting independently.

## **SUMMARY**

The discussion during the PSAM II session will attempt to unravel the modeling differences that could be responsible for large variations in core damage frequency for similar plants. The results of at least two such IPEs will be examined and the treatment of various types of dependencies compared.

## **REFERENCES**

1. "Individual Plant Examination for Severe Accident Vulnerabilities," Generic Letter No. 88 20, 10CFR§59.54(f), Code of Federal Regulations (Nov. 23, 1988).
2. Baltimore Gas and Electric, Calvert Cliffs Probabilistic Risk Assessment, December 1993.
3. TU Electric, Individual Plant Examination Comanche Peak Steam Electric Station, RXE-92-01A, August 1992.
4. Florida Power and Light, Individual Plant Examination St. Lucie Plant, December 1993.
5. Individual Plant Examination: Submittal Guidance, NUREG-1335, August 1989.

## **IMPACT OF METHODOLOGY AND DESIGN CHANGES ON TURKEY POINT IPE RESULTS**

Ching N. Guey and W. A. Skelley

Florida Power and Light Company  
JPN/JB  
700 Universe Blvd  
Juno Beach, FL 33408

### **1. INTRODUCTION**

After the initial submittal of Turkey Point IPE<sup>1</sup> in June 1991, Turkey Point IPE has been refined and applied to reflect both the modelling improvements, plant changes, and operation and maintenance activities. The original IPE methodology will be first described, followed by the evolutionary changes of the IPE in response to the plant application needs.

### **2. ORIGINAL IPE SUBMITTAL**

The original IPE submittal was based on a joint effort via technology transfer between FPL PRA team and SAIC PRA consultants. The CAFTA suite of codes<sup>2</sup> were used to perform the IPE on personal computers. Functional event tree was used to delineate the accident sequences. Sequence quantification was based on a large fault tree linking process. The dependencies of the frontline systems on the support systems are embedded in the system fault trees. In addition, the impact of various initiators on the various system configurations is also addressed in the system fault trees by condition-specific failure events. Both plant specific and generic data were used in the quantification. The quantification process involved truncation of cutsets below certain probability values based on an iterative process. The iterative process resulted in the

cutsets that were important contributors for the given plant configuration, plant model and failure data at the time the IPE was performed. After the cutsets were generated, they were evaluated one by one to incorporate appropriate recovery actions manually. A scoping model was then developed to provide a crude estimate of the new core damage frequency as a result of changes of initiating event frequency, hardware failure data or operator action failure probability. This scoping model has certain limitations and may be enhanced as described in the next section.

### **3. METHODOLOGY CHANGE/REFINEMENT AFTER IPE SUBMITTAL**

After initial IPE submittal, several areas of modelling improvements were made to address the need of plant O&M support. These include: (1). reducing the impact of truncation by artificially elevating the failure probability of certain important events and create a more "robust" scoping model (2). including the recovery events directly in the fault tree model (3). incorporating more realistic plant response for Chemical Volume Control System and other procedural enhancements. (4). considering time-dependent offsite power recovery with multipliers to account for the effect of shorter mission time of power related failure events<sup>3</sup> (5). Other changes to facilitate the searching and ranking of the contribution of various components and systems. These changes do not affect the overall results significantly but make the applications to operations and maintenance activities more easily. The number of cutsets in the later versions of the scoping model increases significantly. For example, for the application to on-line maintenance risk assessment, the original IPE model was expanded from a total of approximately 3000 cutsets to approximately 6000 cutsets.

There are several implications of the model refinement. First, the sensitivity of the model to surveillance interval has been more accurately assessed due to the larger number of components included in the scoping model. Secondly, the incorporation of the human recovery actions in the fault tree model directly provides a more consistent recovery for all cutsets. However, for certain other applications (e.g., external events risk study), the artificial human actions need be considered carefully to avoid meaningless cutsets. Thirdly, the more streamlined and more realistic model changes provides a more useful perspective to the relative safety significance of various components and systems. Finally, the more realistic consideration of the offsite power recovery makes loss of offsite power related scenario less important than the original IPE.

### **4. DESIGN CHANGES AND EVOLUTION OF IPE RESULTS**

Several actual and conceptual design changes were evaluated based on the enhanced IPE model. These include: (1). Installing additional service water connections to charging pumps (2). Replacing the service water tower by a dedicated diesel-driven service water pump, and (3). Eliminating black start diesels. Each of the design changes is described briefly together with the corresponding core damage frequency change.

(1). Installing additional service water hose connections

Use of service water to provide cooling to the charging pumps which in turn cools the reactor coolant pump seals avoids a seal LOCA. In the original plant design only one hose connection was available. The IPE identified a plant hardware change to add two hose connections such that all three charging pumps can be cooled by service water connections. The core damage frequency changes from  $2.2\text{E-}4/\text{Yr}$  to  $1.0\text{E-}4/\text{Yr}$ .

(2). Replacing the service water tower by a dedicated diesel-driven service water pump

Hurricane Andrew destroyed service water tower. A dedicated diesel-driven service water pump was installed. The core damage frequency changes from  $9.35\text{E-}5/\text{Yr}$  to  $9.55\text{E-}5/\text{Yr}$ .

(3). Eliminating the Blackstart Diesel Generators and Adding a Diesel-driven Standby Feedwater Pump

After Hurricane Andrew, it was determined that the five blackstart diesels represented significant burden and did not provide commensurate safety benefits. In order to provide decay heat removal backup capability under loss of grid scenarios, a dedicated diesel-driven standby feedwater was considered to be installed. The core damage frequency would change from  $5.72\text{E-}5/\text{Yr}$  to  $5.71\text{E-}5/\text{Yr}$ .

In addition to the design changes, several plant O&M related activities were also evaluated using the IPE. These activities included the RHR pump IST test interval optimization, the on-line maintenance of several major equipment while in LCO<sup>4</sup> (Limiting Condition of Operation). These applications revealed the limitations of using the PRA model for assessing the safety significance of certain plant operations and maintenance activities. For example, the failure data of the standby components do not distinguish between the time dependent nature of the failure and the demand type of the failure. It is thus difficult to assess the effect of the test frequency on the component failure and thus the safety impact on the plant.

## 5. CONCLUSIONS

The Turkey Point IPE represented a use of the state-of-the-art PRA technology. Because of the inherent limitations of technology, the IPE results not only evolve with the actual plant changes but also with the underlying data, assumptions and modelling techniques. For certain applications, refinement of the model and approximations have to be made to achieve the most effective response to plant O&M request. The main limitations include computer memory requirements (truncation probability), the human actions treatment (conditional incorporation of human actions in the model while considering the dependency of multiple recovery actions), and lack of consistent data (failure probability of standby failures or demand failures and common cause failure probability). Another factor that may contribute to further applications of the IPE is a more universal acceptance criterion of the risk change associated with an acceptable



plant change. Although, the acceptance criteria are not directly related to the IPE methodology, the uncertainties and limitations of the IPE technology constrains the PRA to only an input to the decision-making process.

It is clear from the experiences of development and applications of the Turkey Point IPE that the objectives of the PRA dictate the level of detail, the data requirements and the modelling assumptions. As design changes and operational activities vary, refinements to the model and data are necessary to provide meaningful and useful perspectives.

**References:**

1. Turkey Point IPE Submittal, June 1991
2. CAFTA, RMQS, Versions 2.2c and 2.f
3. M. Lloyd and R. Anoba, "A Convolution Approach to Account for Time Dependencies in Severe Accident Cutset", Thermal Reactor Safety Topical Meeting, Portland, Oregon, 1991
4. Ching Guey et. al., "Applications of IPE to Assess Maintenance at Power", ANS Transactions, June, 1993

**087 Causal Factors in Human Reliability: Experiments and Databases**

*Chair: A.A. Dykes, PLG*

**On the Use of Data Collected During Crew Reliability Experiments at PAKS Nuclear Power Plant - Status Report**

*A. Bareith, Z. Karsa (Inst. for Electric Pwr. Res.); A.J. Spurgin; I. Kiss (Nucl. Pwr. Plt. of Paks); L. Izso (Tech. U. Budapest)*

**Causal Identification of Human Errors Towards Intelligent CAI System for Plant Operation**

*Y. Furuhashi, K. Furuta, S. Kondo (U. Tokyo)*

**Development of a Human Error Data Bank**

*S.E. Taylor-Adams, B. Kirwan (U. Birmingham, England)*

**Causal Factors of Operator Unreliability: An Application of Simulator Data**

*D. Orvis, P. Moieni (Accident Prevention Grp.); A.J. Spurgin*

## **ON THE USE OF DATA COLLECTED DURING CREW RELIABILITY EXPERIMENTS AT PAKS NUCLEAR POWER PLANT - STATUS REPORT**

Attila Bareith, Zoltán Karsa  
Research Fellows  
Institute for Electric Power Research (VEIKI)  
1368 Budapest, POB 233, HUNGARY

Anthony J. Spurgin  
Consultant  
4252, Hortensia St., San Diego, CA 92103, USA

István Kiss  
Nuclear Technics Engineer  
Simulator Center, Nuclear Power Plant of Paks  
7031 Paks, POB 71, HUNGARY

Lajos Izsó  
Associate Professor  
Department of Ergonomics and Psychology, Technical University of  
Budapest  
1111 Budapest, Egri J. u. 1., Building E III/11, HUNGARY

### **BACKGROUND**

In the frame work of a joint US - Hungarian project sponsored by the US - Hungarian Research Fund and the Hungarian National Committee of Technological Development the first ever operator reliability experiments for a Soviet-design, VVER-type reactor were carried out at the Simulator Center of the Paks Nuclear Power Plant, Hungary in the autumn of 1992. The primary objective of the project is to provide input to the ongoing probabilistic safety assessment of the Paks NPP and to provide insights to be useful as far as training and operation is concerned. The data collection was based on the extension of the methodology developed by the Electric Power Research Institute (EPRI) under the Operator Reliability Experiments (ORE) project (Spurgin et al., 1990).

Five accident scenarios were selected for the experiments as follows:

- 1. Small Loss of Coolant Accident
- 2. Single Steam Generator Tube Rupture

- 3. Simultaneous Loss of 3 Reactor-coolant Pumps
- 4. Feedwater Line Rupture
- 5. Inadvertent Closure of Main Steam Isolation Valve

## **DATA COLLECTION AND ANALYSIS**

The experiments covered 120 simulator sessions with the participation of all the 24 control room crews working at the four units of the Paks plant. The observations took place during the regular operator refresher training programme. A comprehensive data bank was created during the simulator sessions including:

- Completed scenario specific observer forms addressing:
  - Communications
  - Man Machine Interface (MMI)
  - Use of procedures
  - Leadership style
  - Cognitive information processing
  - Stress
- Questionnaires completed during post-test interviews
- Observers' notes recorded during debrief sessions
- Information on operators' subjective feeling of fatigue
- Event files recorded by the simulation computer comprising:
  - Operator actions
  - Key plant parameters
- Computer output from a Computerized Operator Assessment System (COPAS) specially modified for the experiments
- Video recordings of all simulator sessions and debriefings

The data analysis methodology used to achieve the project goals is based on the experience obtained from the ORE project. However, changes have been made due to lessons learned during the data analysis process. The analyses performed have been focused on the following areas:

1. Identification of major influences of Human Factors (HF's) on performance and establishment of a causal relationship of group responses for developing advice to training (with the involvement of training personnel), operation and for developing a tool for application to HRA
2. Analysis of HF data for correlations between HF data, measures of crew performance and time data
3. Generation of Time Reliability Curves (TRC's) using time and normalized time, where the normalization factor is the median time taken by the crews to response
4. Integration of crews results using normalized time

The initial data analysis covered the construction of TRC's for all Human-system Interactions (HI's) to find "best fit" analytical expression using linear and non-linear regression, and various standard probability distributions including Lognormal, Weibull and Gamma. Correlations were developed between Skill-Rule-Knowledge definition of crews response and their performance. A control chart approach was selected to better meet the display requirements for training and operations. Logarithmic normalized response times have been plotted in the control charts versus crew for each HI. Experimental bounds from the ORE project, 95% and 99% ranges have been used for upper and lower control chart limits, with missing data indicated by blanks in the data field. Control charts can clearly show which crews are grouped together and which are outside of limits. The charts can also be used to identify systematic influences on the crew performance and random

problems of individual crews. HI time order plots by crews can facilitate the comparisons between crew performances and the search for specific data patterns. Data sets composed of charts and descriptive statistics were combined together in abstracted form in order to integrate all of the essential data and help draw conclusions about the crew performance over the range of scenarios. The observer records were analyzed to understand the causes of crew deviations. As a result, a causal hierarchy has been produced. This hierarchy has been used to understand the distribution of errors and deviations associated with each path, see Figure 1.

For the statistical analysis of the data two basic sets of data files have been created as follows:

1. 32 between-crews data files named  $PNP_{i,j,k}$  corresponding to the 32 observation points each containing background (concerning crew experience), global (concerning global measures of accident scenarios) and observation point level variables, summing up altogether to about 150 variables. In  $PNP_{i,j,k}$  the indices have the following values:

$i = 1, 2, 3, 4, 5$  (serial number of scenario)

$j = 1, 2, 3, 4, 5, 6$  (serial number of malfunction within a scenario)

$k = 1, 2, 3, 4$  (serial number of required action as response to a malfunction)

2. 24 within-crew data files named  $CREW_l$  corresponding to the 24 operator crews each containing ergonomic (concerning ergonomic level of MMI), global (concerning global measures of accident scenarios) and observation point level variables, summing up again altogether to about 150 variables. In  $CREW_l$  the index  $l = 1, 2, 3 \dots 24$  (serial number of crews).

All the variables had a markedly non-normal distribution, and therefore non-parametric statistical hypothesis testing procedures have been used. For instance, the TRC's based on time response data approximated to a lognormal distribution. The statistical analysis has been carried out by the use of the SPSS/PC+ and MS-EXCEL packages.

The global performance of the crews in each scenario was assessed by 3 experienced training staff members (instructors, and co-operating engineers on duty) using a 5-degree scale. This score was taken as a measure of global - observation point level - performance and therefore this value, as a variable, was treated with special emphasis in the statistical evaluation.

## RESULTS

A major finding of the initial data analysis is that most of the human interactions fit standard distributions. Generally, the lognormal distribution was found to be the best approximation. This is in accordance with the results gained from the ORE project. It should be noted however, that in some cases the time response data could be grouped into 2 or 3 different categories that have distinguishing features and, therefore, cannot be described precisely with a single distribution. On the other hand, for the Paks data, the categorisation scheme based on human cognitive behaviours does not seem to be appropriate at this time. No specific correlations were found for these categories. The differences in the distribution of response times representing different levels of cognitive information processing (S-R-K) are not meaningful. This maybe because the crews mainly rely on the knowledge to diagnose and respond to accident sequences and use the procedures as a backup. Three generic correlations were developed in the ORE project based on procedure logic. For the Paks data the use of such categories also seems questionable because of the way the crews operate and use the procedures.

The analysis of control charts shows that crew responses are, for the most part, very consistent. Where the crews do not deviate from the expected actions their performance

variability looks corresponding smaller than equivalent US data. The variability of crew performances is associated with specific malfunctions. In certain scenarios it appears that the accident can be controlled if the board operators are well trained in their area of expertise. However, some other scenarios need the complete resources of the crew to bring the accident to a satisfactory state.

The results indicate that crew responses are randomly ordered within the control ranges. Comparisons made between control plots do not indicate transfer of skills from one crew to another. A detailed analysis of causes of crew deviations has resulted in the development of a causal hierarchy shown in Figure 1. This relationship can usefully be applied to both HRA, and training and operation purposes.

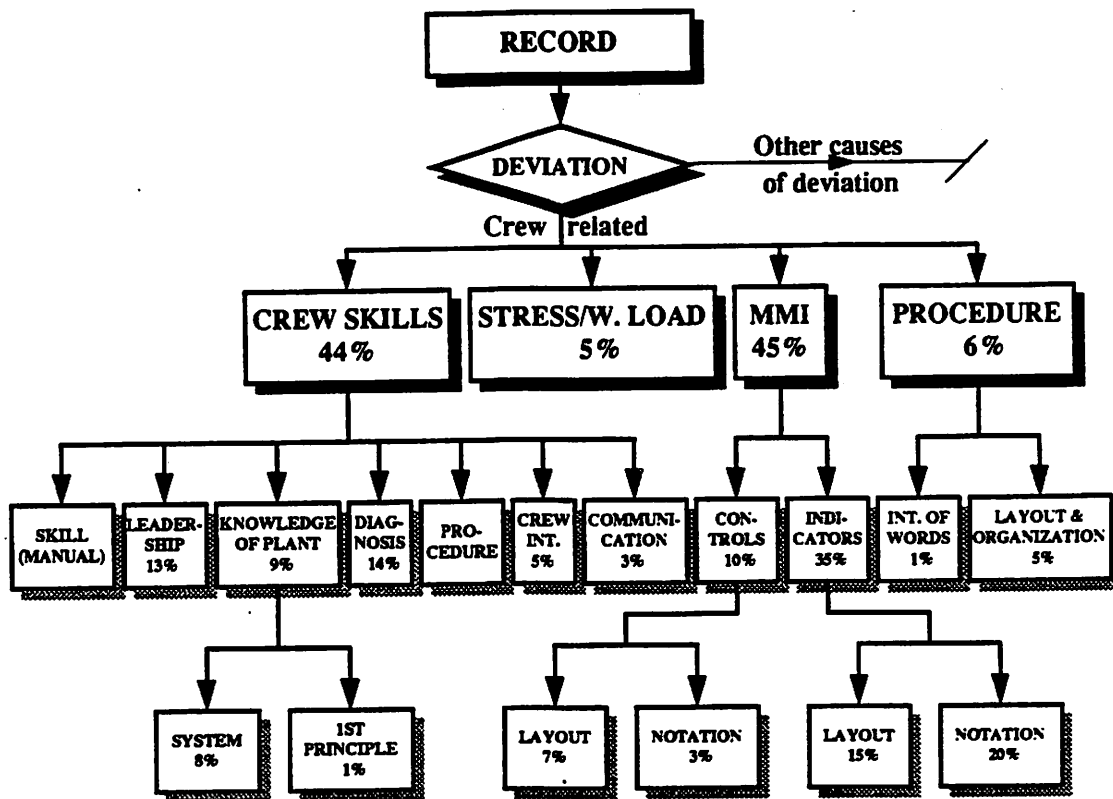


Figure 1. Breakdown of deviations into root causes

Based on the insights derived from the distribution of deviations in the hierarchical array given in Figure 1, a decision tree has been constructed for use in the Paks human reliability analysis. The decision tree reflects the categories in the figure along with the influence of the scenario, in terms of its effect on the ability of the crew to control the scenario.

The decision tree approach has been selected for the Paks HRA quantification since it is capable of embodying the insights from the simulator experiments, is scrutable, can be applied by others than HRA experts, consistent and can be used in conjunction with expert judgement techniques. The direct incorporation of simulator results into a framework that can be used in the HRA is a fundamental step forward in the development of HRA methodology. This step can only be accomplished because of the depth of data collected on the crews' performance and the influence of MMI, procedures, crew skills, leadership, etc., on the crew performance.

From the PNPi\_j\_k set of data files it was calculated - using the Kruskal-Wallis 1-way ANOVA and the Spearman rank-correlation methods - that the global performance is highly determined by the quality of leadership style and also by the quality of the internal as well as external communication. Table 1 and Table 2 are a representative of this process:

**Table 1.** Kruskal-Wallis 1-way ANOVAs for the global scenarios by GLOBPERF

SIGNIFICANCE	GLBLSTYL Mean Rank	GLBINFLS Mean Rank	GLBQINCM Mean Rank	GLBQECOM Mean Rank
Scenario 1	0.05	0.03	0.02	
Scenario 2	0.00	0.01		
Scenario 3		0.08		0.00
Scenario 4		0.05		0.00
Scenario 5	0.03			

**Table 2.** Spearman rank-correlation coefficients with GLOBPERF for the global scenarios

SIGNIFICANCE	GLBLSTYL	GLBINFLS	GLBQINCM	GLBQECOM
Scenario 1	-0.518 (p=0.01)	0.599 (p=0.00)	0.600 (p=0.00)	
Scenario 2	-0.463 (p=0.03)	0.917 (p=0.00)	0.737 (p=0.00)	
Scenario 3		0.497 (p=0.01)		0.806 (p=0.00)
Scenario 4			0.469 (p=0.02)	0.745 (p=0.00)
Scenario 5				0.602 (p=0.00)

Legend for the variable names used in Table 1 and Table 2:

GLOBPERF = GLOBal PERformance score

GLBLSTYL = GLoBal score of Leadership STYLE

GLBINFLS = GLoBal score of INFLuence of Leadership Style on performance

GLBQINCM = GLoBal score of Quality of INternal CoMMunication

GLBQECOM = GLoBal score of Quality of EXternal CoMMunication

Similar analyses have been carried out for each observation point using the PNPi\_j\_k set of data files and the results can be interpreted taking into consideration the particular requirements of each task situation: when the critical requirement is effective communication, the performance correlates with communication measures, when good work organization is necessary, the leadership style becomes important and these measures correlate with performance, and when individual operators have to give their undivided attention to control tasks there are correlations with cognitive and stress levels.

From the CREW1 set of data files the influence of the ergonomic effect of the MMI usage was studied. The main results were identifying some control room layout and procedure usage problems. Operators turn to procedures when they have difficulties and it is not clear what to do. But this association shows, that the majority of the operators prefer to use their knowledge of the plant. Also the operators suggested during the debriefing sessions that the procedures could be improved in either the form or content.

## CONCLUSIONS

The results show that the EPRI data collection methodology can be applied very successfully to 440 MW(e) VVER type PWRs. During the experiments two developments were made to extend the capability of the EPRI approach. This was in the area of automated data collection, using the COPAS system, and an increase in the observer data. These additional data improved the insights derived from the experiments. These insights were in the following areas; use of procedures, the effectiveness of the man-machine interface, crew skills and leadership.

Analysis of the time data indicated variable crew responses dependent on the difficulty of the scenarios, crew organization and knowledge, leadership and procedure use. The statistical analysis confirmed the time analysis findings.

The Paks NPP is considering to adopt symptom-based procedures, and upgrading the instrumentation and control systems of the plant, this upgrade would include the man-machine system. These changes would make the plant even more safe than it is now. The insights derived from the experiments should help Paks personnel in their pursuit of safety.

The experiments were also envisioned to provide input to the PSA. The insights from the experiments have been used to construct decision trees for the HRA. The headings for the trees and their order are derived from the experiments. The branch probabilities are ranked according to the data. This is a significant step in the process of using simulator results in the HRA.

## ACKNOWLEDGEMENTS

The authors wish to thank the Directors of Paks NPP for permission to carry out the simulator experiments. We thank Mr L. Pákai, Head of the Simulator Center, E. Holló PSA project manager and the EPRI project managers D. H. Worledge and A. Singh for their encouragement and support. We would like to thank the control-room crews and the simulator staff for their co-operation in the experiments.

## REFERENCES

- Spurgin, A. J. et al., 1990, Operator Reliability Experiments Using Power Plant Simulators, Electric Power Research Institute, EPRI NP-6937, Final Report, Electric Power Research Institute, Palo Alto, California, USA.
- Landy, Frank J., 1989, Psychology of Work Behavior, Brooks/Cole Publishing Company, Pacific Grove, California, USA



## CAUSAL IDENTIFICATION OF HUMAN ERRORS TOWARDS INTELLIGENT CAI SYSTEM FOR PLANT OPERATION

Yutaka Furuhashi, Kazuo Furuta, and Shunsuke Kondo

Department of Quantum Engineering and Systems Science,  
Faculty of Engineering, the University of Tokyo  
Bunkyo-ku, Tokyo 113, JAPAN

**Abstract:** This paper proposes a methodology for identifying causes of human errors in operation of plant systems, considering operator's cognitive process on the assumption that the process can be modeled as means-end analysis. We developed a prototype CAI system for training of plant operation procedures, which system has a capability of identifying causes of trainees' errors based on the methodology. By means of dynamic planning method, adequate causal identification of errors is possible, and the appropriateness of the method was verified by experiment.

**Keywords:** Causal identification of human errors, CAI, Plant operation, Means-end analysis, Dynamic planning method

### INTRODUCTION

Since plant operators finally play a crucial role for the assurance of system safety, they are required to be familiar with various situations in the system including non-normal or emergent states. However, rapid improvement in system hardware reliability precludes operators from experiencing such situations in their real jobs. Man-to-man instruction is said to be the best solution, but unfortunately resource of human instructors is limited. It is therefore expected to develop an effective methodology for training of operators to be able to cope with such situations applying Computer Assisted Instruction (CAI) systems.

CAI systems have been gradually utilized in various fields following the recent rapid progress of high-performance, low-cost computers and software. Most of these CAI systems, however, are not able to solve problems in training domain, and a same training method is used all through the training course regardless of training topics or understanding level of trainees. In order to ameliorate these problems, and to provide man-to-man-like instruction using a computer, it is required to develop intelligent CAI systems which:

- (1) can solve problems in training domain,
- (2) allows dialogue between the system and trainees with mutual initiative, and
- (3) performs high-level individual instruction<sup>1,2</sup>.

To realize the third ability, CAI systems should have a capability to select an instruction strategy appropriate for the understanding level of each trainee, and to know why the trainee

committed errors, i.e. to identify the cause of errors. Hence, to establish methods of classification and identification of human errors and their causes in training domain is one of the key issues in realizing intelligent CAI systems.

In the present paper we propose a methodology to identify the causes of trainees' errors for realizing intelligent CAI systems, based on the consideration of trainee's problem solving process. And then a prototype CAI system has been developed to verify the method. The problem domain of the system is procedural plant operation, where a series of operations is performed step by step under circumstantial judgement in order to attain some given goal. In relation to the SRK human cognitive model proposed by Rasmussen<sup>3</sup>, trainees are assumed to act based not on the skill acquired but on their knowledge and rules about operations. *Accomplished trainees* are defined as those who have valid knowledge and rules enough to solve the domain problems, and who can use them correctly to plan reasonable actions. The sequence of operations generated by accomplished trainees is defined as *the standard operation*. To realize adequate causal identification of errors, dynamic planning method is adopted by incorporating a planner into the prototype CAI system.

## METHODOLOGY

### Causal Classification of Errors

There is no definite way so far to classify human errors and their causes: every proposed classification views human errors from a certain aspect. Swain and Guttman, for instance, classify human errors as omission, commission, etc. for HRA study<sup>4</sup>. Rouse and Rouse proposed classification of human errors from a viewpoint of human information processing<sup>5</sup>, while another classification which clearly discriminates the manifestations of errors from their causes was proposed by Hollnagel aiming at objective analysis of human errors<sup>6</sup>. These proposals, however, classify not purely error causes but error types or mixture of error types and error causes. From a viewpoint of training, it is significant to classify the causes of human errors based on the problem solving process of trainees, because it enables us to point out the malfunctions in the trainee's way of thinking. Human information processing model proposed by Rouse and Rouse is a method in this category, but it is too general for the present purpose. Thus we firstly consider human information processing specific to plant operation.

In operation of plant systems, operators are considered to take goal-driven problem solving behaviour. According to Newell and Simon<sup>7</sup>, information processing of such behaviour can be modeled as means-end analysis, i.e., a problem solver

- (1) assesses the difference between the present and the goal states,
- (2) selects an appropriate operation to reduce the difference, and then
- (3) executes the operation to move into a new state.

The second step is considered to consist of three steps: operators firstly predict the state attained by operation, check the applicability of operation under the present circumstance, and lastly check the conflict between other operations already planned. As there exists possibility of causing an erroneous action in each of these steps, we believe that this can be a practical framework for causal classification of human errors in plant operation.

The summary of causal classification based on the framework is shown in Table 1. In the first step of assessing the difference, misunderstanding the present state (C1) is a candidate of mistake. In the second step of selecting an operation, forgetting the existence of operation (C2), misunderstanding the effects of operation (C3), misunderstanding the preference conditions of operation (C4), misunderstanding the preconditions of operation (C5), and misunderstanding the conflicts between operations (C6) can be error causes. Confusion in information processing (C7) is a general mistake for all three steps. We do not consider misunderstanding of the goal state, because goal states to be achieved are explicitly given in advance in the system. A mistake in the third step, i.e. omitting execution which cannot be clearly distinguished, is considered to be included in confusion in information processing.

**Table 1. Causal classification of operator errors.**

Step in Means-end Analysis		Case of Error	
Assessment of difference		Misunderstanding the present state (C1)	
Selection of an appropriate operation	Prediction of the state attained	Misunderstanding the effects of operation (C3)	Forgetting the existence of operation (C2)
	Check of applicability	Misunderstanding the preference conditions of operation (C4)	
		Misunderstanding the preconditions of operation (C5)	
	Check of confliction	Misunderstanding the conflicts between operations (C6)	
Execution of operation		Confusion in information processing (C7)	

### Causal Identification of Errors

In the prototype CAI system, trainee's entered operation is judged inappropriate when the operation is not applicable due to unsatisfied preconditions, or when the operation does not have the same effects as the corresponding standard operation. In such cases, error type of a single operation is identified by judging whether or not

- (1) an useless operation was performed,
- (2) the operation was omitted,
- (3) intention was partly right but a wrong operation was selected, or
- (4) intention was wrong (any other categories).

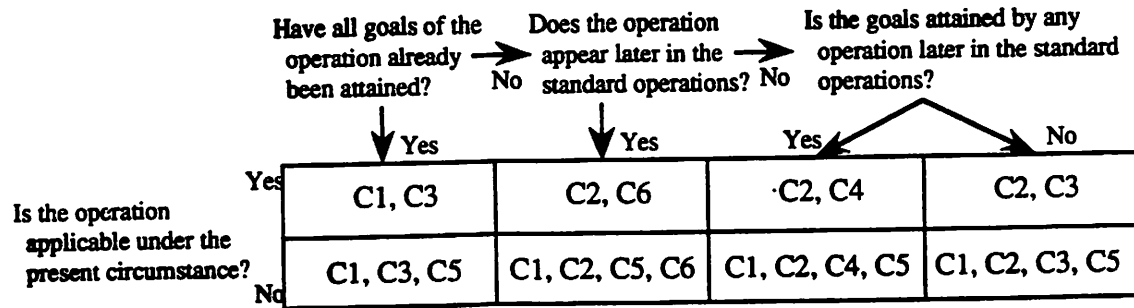
The second type can be further divided into simple omission and sequence error after the series of trainee's inputs has been traced. At present, however, we do not do so, because our primary aim is to point out the cause of errors immediately after having classified trainee's commitment.

An erroneous operation is identified and classified into the above four error types using the following three criteria.

- (1) If all goals of the operation have been already attained in the present state, the operation is concluded unnecessary.
- (2) If the operation appears later in the sequence of standard operations, the error is of the second type, i.e., omission or sequence error.
- (3) If the goals are attained by an operation later in the sequence of standard operations, trainee's intention is judged correct (the third type), otherwise the error is concluded of the forth type.

The system also checks whether or not the erroneous operation is applicable under the present circumstance, in addition to these criteria. Combining this criterion and the three criteria described above, a matrix of error types shown in Figure 1 is obtained. Each element of the matrix corresponds to some of error causes proposed in the previous section. According to the matrix, for instance, when an input operation is not applicable and brings about no change in the present state, C1, C3, or C5 can be the cause of this error.

Since this matrix gives more than one causes for an error, the system asks questions corresponding to each cause to narrow the candidates. For instance, when a trainee is suspected to have misunderstood the preconditions of a certain operation (i.e., C5 is included among the probable error causes), the preconditions of the operation will be the topic of question. If the answer is correct, the corresponding error cause will be eliminated from the candidates. When the trainee perfectly answer all questions asked, i.e., no candidate remains, C7 (confusion in information processing) will be given as the cause.



**Figure 1.** Causal identification of operator errors.

Items in each frame represent probable causes of errors. The symbols correspond to the causal classification of errors shown in Table 1.

## Knowledge Representation

The knowledge in the system is the operation of plant systems, which is represented in four clauses: the contents, preconditions, preference conditions, and effects of unit operations. This definition is suitable for planning based on the means-end analysis. Presuming no interdependence of operations, operations can easily be added or eliminated. Based on the definition of the rule-based behavior described in the SRK model, a rule is defined as a subroutine consisting of a sequence of operations to achieve a certain goal in the problem domain. For instance, the normal sequence of operations required for starting up a plant system is integrated into a subroutine of "starting".

## Planning

The algorithm used in the built-in planner is based on the means-end analysis. The planner firstly identifies two subroutines (rules) in which the initial and the goal state are included respectively, and makes a rough plan using the subroutines, without considering the constituent operations. Lastly the planner unfolds each subroutine, checks the suitability of individual operations in detail, and makes up a series of operations. If insufficiencies or inconsistencies are found, supplemental operations are added, or some operations are eliminated to correct them. To resolve interference between subgoals, a heuristic rule is used that an operation belonging to a certain subroutine is prior to the one independent of a particular subroutine. This hierarchical planning simulates both rule-based and knowledge-based cognitive behaviour of plant operators, and also cut off the search space for selecting operations. The operations which the planner builds up can be considered as standard operations for a given goal.

## DESCRIPTION OF THE PROTOTYPE CAI SYSTEM

### Architecture

The system consists of the following five modules.

- (1) A knowledge base which stores the definition of operations and rules to be utilized for planning or causal identification of errors.
- (2) A planner which produces a series of standard operations for a given goal based on the knowledge base.
- (3) A controller which checks inputs from the trainee and identify the causes of errors when the entered operation is judged inappropriate for the present situation. This module controls the whole system.
- (4) A trainee's database stores every record of trainee's input and the results of error analysis. For every erroneous input, the following four items are recorded: the standard operation

expected, the entered operation, error type and causes of the error identified.

- (5) User interface which consists of an input-output window and a graphic display window of plant state. The input-output window contains of two message windows for output and buttons for input, which cover every possible input item. One message window indicates plant state in texts, and the other is for questions from the system.

Every module has been implemented on an EWS using the Prolog and C language. An expert shell G2 is also used for the graphic display window of the user interface.

### Flow of Training

The system gives initial and goal states to the trainee at the beginning of training, and then the built-in planner plans the sequence of standard operations. The trainee indicates operations one by one as inputs to the system, using a mouse and buttons. The state of plant system displayed changes when the entered operation is judged appropriate, otherwise an error analysis program is invoked to identify the cause of error. The result is recorded in the trainee's database. If the operation is not standard but applicable, the plant state deviates from the one supposed in the expected operation. Conventional CAI systems, which statically prepare the sequence of recommendable operations, cannot flexibly cope with such deviation. In this system, as illustrated in Figure 2, the planner is directed to plan a new sequence of standard operations from the new state generated by the operation. By means of such dynamic planning, the next operation appropriate for the situation is available at any moment, which enables adequate causal identification of trainees' errors. This procedure continues till the trainee succeeds to attain the goal state or he/she quits from training.

### EXPERIMENT

An experiment was performed to verify the adequacy of the error identification method. The problem domain used is the procedure to fill up sodium into the primary coolant system of a fast reactor. Twenty seven unit operations and eight subroutines (rules) are prepared for this domain. Five trainees, who have been taught the overview of the procedure and the definition of each operation, used the CAI system. After the training sessions, the causes of errors identified by the system were compared with those identified by oral interview. The result is given in Table 2. The causes identified by the prototype CAI system were proper for 22 cases among 27 errors observed, among which the results for 12 cases were completely identical. The causes of errors were often identified only partly by the system when the trainees became

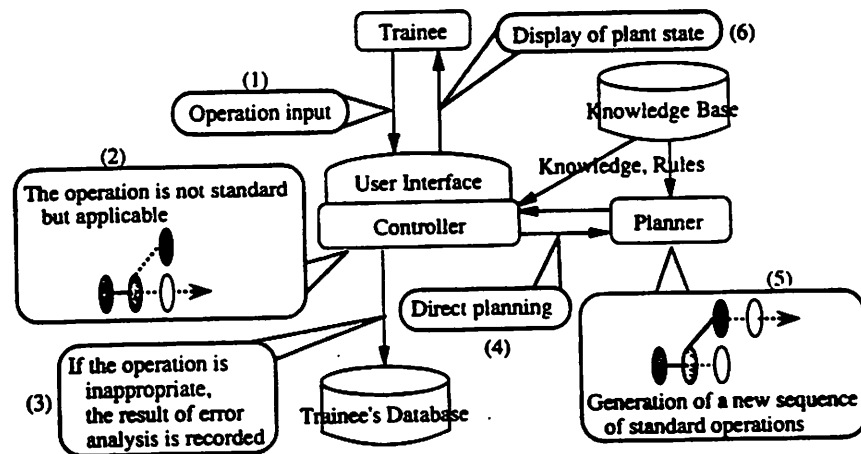


Figure 2. The system architecture and outline of dynamic planning.

**Table 2. The result of experiment.**

Appropriateness of the Result of Causal Identification		Number of Cases Observed	
Appropriate	Complete match	12	22
	Partial match	10	
Inappropriate		5	
Total		27	

aware of their mistakes during answering questions and gave correct answers. The system could not identify meaningful causes at all when the trainees operated by just guessing, which was the main reason of failing causal identification.

As for the error types, 24 errors were of omission or sequence error, among which 5 cases were applicable and the rest 19 cases were inapplicable. Other 3 cases were of unnecessary operation, all of which were applicable, and no other error types were observed. This indicates that the trainees knew which operation to take in the future but did not exactly know when to perform. On the other hand, among 11 cases of the type of omission or sequence error, the identification of which were completely successful, "forgetting the existence of operation (C2)" appeared 9 times, while "misunderstanding the conflicts between operations (C6)" only 3. This means that the trainees did not correctly understand the correspondence between states and operations, rather than believed in a wrong sequence. These characteristics were, however, average tendencies of the trainees, and variations between individuals exist. For instance, most of errors committed by a certain trainee were sequence errors caused by ambiguous knowledge, while another trainee often performed unnecessary operations due to misunderstanding of the plant state.

## CONCLUSION

A methodology for causal identification of human errors in plant operation has been proposed, considering operator's problem solving process. A prototype CAI system for training plant operation procedures has been developed based on the methodology. By means of dynamic planning, the standard operation appropriate for present situation is ready at any moment, which makes proper causal identification of errors possible. The appropriateness of the identification method was verified by experiment. Consequently, the method is expected to contribute to the realization of man-to-man-like instruction using a computer with its ability of pointing out the causes of trainee's errors and the characteristics of his/her defect.

## REFERENCES

1. S. Otsuki and Y. Yamamoto, "Paradigm and environment of intelligent CAI", *Joho-shori*, vol.29, no.11 (1988) (Japanese)
2. E. Wenger, *Artificial Intelligence and Tutoring Systems*, ohm-sha (1990) (Japanese translation)
3. J. Rasmussen, "Skills, Rules, and Knowledge: Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models", *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-13, 257 (1983)
4. A.D. Swain, H.E. Guttman, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278 (1983)
5. W.B. Rouse, S.H. Rouse, "Analysis and classification of human error", *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-13, no.4 (1983)
6. E. Hollnagel, "The phenotype of erroneous actions", *Int. J. Man-Machine Studies*, vol.39 (1993)
7. A. Newell, and H. Simon, *GPS-A Program that Simulates Human Thought*, Computers and Thought, Feigenbaum, E.A. and Feldman, J. eds., McGraw-Hill, NY (1963)

## **DEVELOPMENT OF A HUMAN ERROR DATA BANK\***

**Sally E Taylor-Adams and Barry Kirwan**

**Industrial Ergonomics Group,  
School of Manufacturing and Mechanical Engineering,  
University of Birmingham, B15 2TT, England.**

### **INTRODUCTION**

In the UK, Human Reliability Assessment (HRA) is playing an increasing role in determining and reducing risk attributed to human error, in a range of industries such as nuclear power and chemical plants. Since the genesis of HRA in the early 1960's, a recurrent problem has been the lack of quantitative human error data with which to either quantify directly the likelihood of human errors occurring, or upon which to base more flexible and generic human error quantification tools, or indeed upon which to validate such tools.

This lack of human error data has not been for the lack of effort since there has been a reasonable number of attempts since the 1960's to generate human error databases, (for a review see Topmiller et al 1982). However most of these attempts have long since been abandoned for numerous reasons, but in particular because of the difficulty of combining the "elemental" human performance data within them into realistic human error tasks relevant to, eg., nuclear power plants. The one surviving data bank from the first two decades of HRA is the databank enshrouded within the Technique for Human Error Rate Prediction (THERP: Swain and Guttman, 1983), which is a mixture of real and expert opinion based data.

The post-Three Mile Island 1980's saw attention switching away from databanks onto structured and unstructured judgement based techniques (eg. the Success Likelihood Index Method, and Absolute Probability Judgement), and techniques which relied on their own implicit databases, such as THERP, and the Human Error Assessment and Reduction Techniques (HEART: Williams 1986; for a review of all these techniques see Kirwan et al, 1988). Such techniques have been successfully employed in PSA's, and have in most cases reasonable "face validity" with practitioners and regulators, even if not with the academics.

However in the past few years there has once again been a desire for human error databanks (see ACSNI, 1991), for several reasons;

\* This work is being funded by the UK Health and Safety Executive, Nuclear Safety Research Programme. The views expressed in this paper are the authors', and do not necessarily reflect those of the sponsor.

- For use directly in HRA's/PSA's.
- For use by techniques which need calibration data (eg. SLIM).
- For validation of HRA techniques.

More generally, human error data is desirable because it will give more confidence in the whole HRA process. This is becoming of increasing importance as HRAs and their results increasingly tend to dominate PSA predictions of the risk of a plant. Furthermore, as HRA predictions have become more important in PSA's, so too has the ability to predict the effects of error reduction interventions on error probabilities. Thus, typical HRA's in the UK currently also allow the determination of what intervention measures are required to reach acceptable human performance targets (human error probabilities), within the PSA.

This specification of error reduction methods requires a more detailed understanding of the causes or mechanisms of the human error in the first place, since if the causes of the error are not understood or modelled, then error reduction mechanisms will be of suspect quality and effectiveness. This HRA capability therefore requires that for each human error modelled, it is desirable to know what factors caused the error (the Performance Shaping Factor (PSF)), and how the error manifested itself in terms of the internal mechanism of failure within the human operator (called the Psychological Error Mechanism (PEM)). If these two aspects of human error are known, then HRA and error reduction become more credible, and more powerful.

This resurgence in interest in a human error databank has led to a number of projects in this field, such as the NUCLARR database (Gertman et al, 1988), and the derivation of a small amount of incident-derived data in the UK (Kirwan et al, 1990). In particular this latter project collected data not only on the overt manifestation of the error (ie. "what happened", known as the External Error Mode (EEM)), but also on the PSF's and the most likely PEM for each datum collected. Whilst this was not easy, the data derived can be applied (in PSA's or in validations) with more confidence since they are better described and understood than most existing data.

The project described in this paper therefore attempts to develop a more extensive database of human error probabilities, which for some of the data at least will contain detailed information on the PSF and PEM's for a datum, as well as the EEM. The primary uses of the database will be for HRA-in-PSA usage, validations and calibration data, as well as, in the longer term, perhaps for the development of better generic HRA prediction tools based on the analysis of empirical data.

Having defined the background to the nature and direction of the database project, the remainder of the paper describes interim progress, and future work.

## OBJECTIVES AND SCOPE OF THE PROJECT

This is a three year research project aimed at developing a computerised human error database containing information on human error probabilities useful for HRA and PSA applications, ie for direct HRA usage, for validations, and for calibration of techniques. The system is also required to be user- friendly. It will contain data from a range of industries.

## PROGRESS TO DATE

The project is outlined below. Initial literature reviews have enabled the collation of a large amount of robust human error data, and other data collection work is in progress at



this time. The results briefly presented below will focus on the project stages concerned with the task analysis, data collection efforts so far, the taxonomies underpinning the database, the prototype user interface and the major tasks remaining.

1. Literature Review
2. Hierarchical Task Analysis
3. Human Error Data Collection
4. Development of a Human Error Taxonomy
5. Development of Extrapolation Rule Feasibility
6. Development of the User Interface
7. Usability and Validation of the System
8. Documentation

### **Hierarchical Task Analysis**

A task analysis phase of work has been carried out via discussions with HRA and PSA assessors, which has enabled a detailed task analysis of the human reliability quantification process in PSA to be developed. In particular the type of data, action or human error types that need to be quantified, and how analysts utilise data, have been identified. Particular significance was placed on determining all the processes and stages through which an analyst proceeds when conducting a HRA, and why this information is so important, to determine what human action/error types are difficult to quantify and why, and what human actions have to be quantified regularly. A structured interview methodology was considered the most effective mechanism for gaining information on the above data prerequisites.

The main results from the task analysis suggest that quantification of human error in a HRA is primarily facilitated by assessor judgement/experience, (see Taylor-Adams and Kirwan, 1993). Human Reliability Quantification techniques such as THERP and HEART are used moderately often, THERP is used if the assessor has sufficient resources, and HEART if resources are in short supply. Other human reliability techniques such as SLIM, PC, APJ and HRMS are rarely used. Should the assessor generate a human error probability (HEP) which appears unreasonable, then a variety of possible solutions are used to check the applicability of the HEP. Firstly the analyst may seek the opinion of the operator or client to check the reliability of the HEP, or equally they may use another technique to check reliability.

In general the type of human actions/errors analysts in HRA have to quantify are skill and rule based errors, but usually a wide variety of human errors have to be quantified eg. latent errors, diagnosis errors, operator violations etc. Human action/errors which are difficult to quantify are cognitive errors, long timescale type errors, rule violations and misdiagnosis. Comparing regularly quantified error types with those which are difficult to quantify we can see there is an overlap between diagnostic error, rule violations and mistakes. This would therefore seem to suggest that the development of a human error data base should concentrate on collecting HEP's in these areas, so that the data assessors are using are valid and useful. The type of information (1-11 below) and functions (12-14 below) assessors wish to see obtained in a human error data base are;

- |                                  |                            |
|----------------------------------|----------------------------|
| 1. Task Description              | 9. Industry                |
| 2. Error Description             | 10. Data Pedigree          |
| 3. External Error Mode           | 11. Reference Source       |
| 4. Psychological Error Mechanism | 12. Data Comparisons       |
| 5. Performance Shaping Factor    | 13. Wide variety of tasks  |
| 6. Human Error Probability       | 14. Database to be Updated |

7. Upper/Lower Bound
8. Opportunity for Error

The first 12 points have been included in the prototype database, whereas the last 3 will be considered at a further time.

### Database Taxonomies

The evolution of a comprehensive human performance taxonomy has been a continuing objective in human factors research, Fleishman and Quaintance (1984). Such a taxonomy must be able to describe all types of behaviour and depict all possible errors, thus making it comprehensive.

It is fundamental to the development of a human error database that the databank is constructed for the purpose of generalisation and extrapolation of data from the database to HEPs required for HRAs/PSAs. A taxonomy is therefore necessary to structure the data collection and to provide all the qualitative information relevant to a particular HEP datum. This taxonomy, or set of taxonomies needs to include information on what, why and how an error occurred and a description of the task/error scenario and mutually exclusive database.

Four taxonomies have been devised for explicit use with the CORE-DATA (Computerised Operators Reliability and Error Data) database, and these include an External Error Mode (EEM), Psychological Error Mechanism (PEM), Performance Shaping Factor (PSF) and Task taxonomy. Development of CORE-DATA's EEM taxonomy involved a comprehensive listing of 27 EEM's which originated from taxonomies such as those found in the human error and performance literature. These 27 EEM's were then categorised under Swain and Guttman's framework and checked for mutual exclusivity, which can be found in Figure 1. The taxonomic framework is based on a 4 level hierarchy which facilitates EEM identification and retrieval,

1. Error of Commission
  2. Time Errors
    3. Action Too Long
    4. Accidental Timing with other event/circumstance

The psychological error mechanism (PEM's) taxonomy originated from a variety of taxonomies and these uncovered 58 PEM's. The PEM's were then provided with a brief definition and example of the PEM in action eg. Stereotype Takeover:- operator replaces a familiar operation/procedure with a similar operation/characteristics for actual operation/procedure *ie. changes gear with the left hand when in a right hand car*. This enabled mutual exclusivity and categorization of PEM's to be determined, which resulted in the PEM's being arranged hierarchically and reduced the 58 PEM'S to 32. An example of the PEM taxonomy can be found in Figure 1.

Development of the PSF taxonomy involved the collation of PSF's from a variety of human reliability assessment techniques or methods such as THERP, PHECA, and HEART. These methodologies produced a listing of more than 200 PSF, therefore to make the listing more manageable Bellamy's 8 taxonomy headings were used as a means to separate the PSF, (see Bellamy 1991). The PSF taxonomy contains 100 PSF, but the taxonomy has been simplified via a hierarchical approach so that the user can proceed to their own required level of detail. It is apparent that a comprehensive PSF taxonomy is needed to help categorise any potential influencing factor. A equipment/task (see Figure 1 for example) and human action taxonomy have also been constructed and these will also enable further methods for abstracting data from the database.

## **Figure 1:- Examples of the Proposed PEM, EEM and Task Taxonomies**

1. **Stereotype Takeover**
  - 1.1 Frequency of Previous Use
  - 1.2 Assumptions
  - 1.3 Substitution
2. **Memory Failure**
  - 2.1 Bounded Rationality
  - 2.2 Mistake Among Alternatives
  - 2.3 Place Losing Error
  - 2.4 Mental Blocks
3. **Thematic Vagabonding**
  - 3.1 Hyperactivity
4. **Encystment**
  - 4.1 Persistence
5. **Over Demanding/Cognitive Overload**
  - 5.1 Bounded Rationality
  - 5.2 Identification Prevented
  - 5.3 Freeze
  - 5.4 Reduced Capability
6. **Risk Recognition Failure**
  - 6.1 Underestimate Demand
  - 6.2 Overconfidence/Over Estimate Abilities
    - 6.2.1 Risk Tolerance
    - 6.2.2 Oversimplification

### **Example of Proposed PEM Taxonomy**

#### **Alarms**

1. **VDU Alarms**
  - 1.1 High pressure VDU alarm
  - 1.2 Single VDU Alarm
  - 1.3 VDU Alarms
2. **Low Level Alarm**
3. **Acid Add Time Alarm**
4. **Alarm feed preparation system Alarm**
5. **Low Surge Tank Alarm**
6. **Alarm Annunciators**

#### **Switches**

1. **Multi-Position Switches**
  - 1.1 10-Position Rotary Selector Switch
  - 1.2 2 Position Switch
  - 1.3 Rotary Control 3 Position Switch
2. **Toggle Switch**
3. **Motor Operated Valve Switch**
4. **Changeover Switch**
5. **Switchover of Selector Switch**
6. **Turbine Switch Board**

### **Example of the Task Taxonomy**

## Data Collection To Date

It is generally agreed throughout the reliability engineering domain that there is no readily available truly believable comprehensive compendium of human reliability data, Meister (1984). However human error data can be collected from a variety of sources and CORE-DATA currently contains data from each of these sources (the numbers in brackets are correct at the time of going to press, but will increase as the project continues);

1. Real Operating Experience (46 data points);
2. Simulator Data (416 data points);
3. Expert Judgement Data (152 data points);
4. Literature Data (509 data points);
5. Synthetic Data from human reliability quantification techniques (45 data points).

In an ideal world all data would preferably be abstracted from real operating experience or robust industrially relevant experiments. Unfortunately there are difficulties in collecting this type of data due to the politically sensitive nature of the data, or, lack of data collection schemes. Consequently we have to assimilate data from a variety of different sources to complement real data or missing data for specific task scenario's. However this research project has recently implemented a human error data collection scheme in a large company and is still collecting data from other sources. It is therefore anticipated that many new HEP's will be added to the database over the next 18 months, which will help the lack of data problem.

## Database Computerisation

A prototype screen design system has been developed for CORE-DATA, and limited usability trials have been carried out to date. The user of the system can access data according to the following aspects (or certain combinations of these aspects);

1. Industry type (eg. Nuclear, Offshore, etc);
2. Level of Operation (eg. Normal, Emergency, Maintenance);
3. Human Action (eg. Installs, Diagnoses, etc);
4. External Error Mode (eg. Error of Omission, Commission, etc);
5. Psychological Error Mechanism (eg. Encystment, Thematic Vagabonding, etc).

## FURTHER WORK

Further work will include validation/verification of the taxonomy which shall continue during the development of CORE-DATA. Hence as more data are made available the taxonomies will be tested to check if the taxonomy is exhaustive and comprehensive. It is anticipated that the internal and external validity and comprehensiveness of the taxonomies can be tested, via setting up controlled experiments with real HRA assessors, using them to find specific HEP's and their associated qualitative information. This type of validation exercise would determine the taxonomies reliability in the real world, as comprehensive scenarios' would be used to test the database system. The internal validity would be tested via determining the consistency of usage of the database.

A major phase of the project in 1994/95 will involve the development of a prototype set of extrapolation rules. These rules will allow extrapolation from a datum in the data

base to specific PSA operator tasks.

These rules will be based on PSF and this will enable a specific HEP, associated eg. with a nuclear task to be compared to a similar task in the petro-chemical industry and for the HEP to be expertly manipulated depending on the PEM or PSF. The development of prototype extrapolation rules will enable HRA assessors to use data from different source industries confidently, and will enhance the credibility of human reliability in terms of forwarding the methodology of HRA.

## ACKNOWLEDGEMENTS

The authors would like to thank Mike Gray (Health and Safety Executive), Helen Rycraft (British Nuclear Fuels), Peter Ackroyd (Nuclear Electric) and George Poullos (Birmingham University) for their inputs during this project.

## REFERENCES

- Advisory Committee on the Safety of Nuclear Installations; Study Group on Human Factors, second report: Human Reliability Assessment - A Critical Overview. Health and Safety Commission, HMSO, London.
- Bellamy, L.J., 1991, The quantification of human fallibility, *Journal of Health and Safety* 6:13-22.
- Fleishman, E.A., and Quaintance, M.K., 1984, "Taxonomies of Human Performance: The Description of Human Tasks," Academic Press Inc, London.
- Gilmore, W.E., Gertman, D.I., Gilbert, B.G., and Reece, W.J., 1988, Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR). Guide to Data Processing and Revision:- Part 1 Technical Overview, Volume 3. United States Nuclear Regulatory Commission. NUREG/CR-4639, EGG-2458. Washington DC 20555.
- Kirwan, B., 1988, A Comparative Evaluation of Five Human Reliability Measurement Techniques, in Sayers, B.A. (ed), *Human Factors and Decision Making*. Elsevier Applied Science Publishers. Barking, Essex.
- Meister, D., 1984, Human Reliability, in Muckler, F.A. (ed). *Human Factors Society Review: 1984*, Human Factors Society, Santa Monica, California, USA.
- Swain, A.D., and Guttman, H.E., 1983, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. NUREG/CR-1273. Sandia National Laboratories. USNRC.
- Taylor-Adams, S.E., and Kirwan, B., 1993, *Human Reliability Data Requirements*. International Journal of Quality and Reliability Management. To be Published.
- Topmiller, D.A., Eskel, J.S., and Kozinsky, E.J. (1982). *Human Reliability Data Bank for Nuclear Power Plant Operations*, vol 1: A Review of Existing Human Reliability Data Banks. NUREG/CR-2744. USNRC.
- Williams, J.C. (1986). *HEART - A Proposed Method for Assessing and Reducing Human Error*. Ninth Advances in Reliability Technology Symposium - 1986.

## Example of the EEM taxonomy

### Errors of Omission

- Omits entire task
- Omits a step in the task

### Errors of Commission

#### - Time Errors

- Action too early
- Action too late
- Latent error prevents execution
- Action too long
  - Accidental timing with other event/circumstance
- Action too short
  - Accidental timing with other event/circumstance

#### - Qualitative Errors

- Act incorrectly performed
  - Action too much
  - Action too little
  - Action repeated

#### - Selection Errors

- Right action on wrong object
- Wrong action on right object
- Information not obtained/transmitted
  - Communication Error
- Wrong information obtained/transmitted
  - Communication Error
- Substitution/intrusion error

#### - Sequence Errors

- Incorrect sequence
- Action in wrong direction
- Misalignment/orientation error

### Extraneous Acts

- Rule violations

# CAUSAL FACTORS OF OPERATOR UNRELIABILITY: AN APPLICATION OF SIMULATOR DATA

Douglas D. Orvis,<sup>1</sup> Parviz Moieni,<sup>1</sup> and Anthony J. Spurgin<sup>2</sup>

<sup>1</sup>Accident Prevention Group  
16980 Via Tazon, Suite 110  
San Diego, CA 92127

<sup>2</sup>Consultant  
4252 Hortensia St  
San Diego, CA 92103

## INTRODUCTION

The motivation for studying and improving the proficiency and reliability of control room operators is multifaceted, all resulting in some kind of cost saving to the operating utility: 1) achieving higher plant availability factors; 2) reducing the risk of accidents having associated consequences and costs; 3) reducing the risk of damaging plant equipment; 4) improving relationships with regulators; and 5) verifying the effectiveness of their training program and avoiding undue remedial programs or unnecessary interactions with regulators. Various estimates indicate that so-called human error contributes to 70-80% of industrial accidents including errors in design and maintenance as well as in operations. One utility reported a loss of \$4M due to 79 events involving human error. Clearly, there are economic as well as safety incentives to identify and reduce causes of human actions that lose millions of dollars. Collecting and analyzing simulator data for causes and trends is one way to recognize and correct problems before they cost a lot of money.

Regulators, utilities and INPO have begun to compile statistics on types and causes of "inappropriate actions" by control room and plant personnel; however, the data is collected post facto. By routinely collecting data during simulator training and requalification exercises and analyzing the data for types and causes of "deviations" or "inappropriate actions", the operating plant can take corrective actions before such "deviations" occur in the plant or lurk as "resident pathogens" (Reason, 1990) which increase the probability of operator error and thereby increase the probability of a catastrophe.

This paper demonstrates how simulator data can be used to quantify the relative importance of various immediate or proximal causal factors and discusses how such data may be applied to identify and quantify the influences of deficient organizational factors. (See also the PSAM II paper by Bareith, et al. for a similar treatment of simulator data.)

## BACKGROUND

Probabilistic risk assessment (PRA) has evolved over the past two decades in four distinctive phases: Machine, Milieux, Man, and Management. The first two phases dealt respectively with accident sequences initiated and propagated by failures and successes within plant systems and hardware (Machine); and those initiated by natural phenomena, fires or floods (Milieux). Studies of the "anatomy of accidents" show that human error contributed significantly to the probability of accidents. The "Man" phase of PRA evolution included research to develop methodology for human reliability analysis (HRA).

Rather novel among the HRA research efforts, however, was the initiation of measurements of NPP operating crew reliability at simulators to obtain data *in lieu* of actual accidents but in preference to "expert opinions". Simulator measurement programs were initiated in the U.S., Taiwan, France and Finland. We were principals in the design and execution of the Operator Reliability Experiments (ORE) program

the design and execution of the Operator Reliability Experiments (ORE) program sponsored by the Electric Power Research Institute (EPRI) and participating utilities (Spurgin, et al., 1990; Orvis, et al., 1990). Insights expressed in this paper are attributed partly to our participation in the ORE, but do not necessarily represent the views of EPRI or participating utilities.

Currently, PRA methodology is in the fourth phase: Management (and Organizational Factors). In the aftermath of Chernobyl, Bhopal, Challenger and many other actual catastrophes, varied deficiencies in sociotechnical organizations are revealed to be pervasive, underlying causes. We are participating in this advancement of PRA methodology (Orvis, et al., 1993) and believe that empirical data collected during simulator exercises can help to identify and quantify the effects of organizational factors.

Experience has shown that neither operators nor training instructors are very reliable sources for answering such questions as: "What do operators do, correctly and incorrectly, when they are responding to an accident?", or "If crew response is incorrect, is it a random event or caused by some deficiency in the sociotechnical system?". Instead, a structured and routine data collection and analysis program can provide answers. Data so acquired and analyzed also provides a) a means for evaluating the effectiveness of training [e.g., see Spurgin, et al. (1993)], b) support for plant-specific PRA studies including an empirical basis for weighting factors of Performance Shaping Factors (PSFs) and c) insights into factors in the plant or organization which influence or cause operator unreliability.

#### SUMMARY OF REPRESENTATIVE CAUSAL ANALYSIS EFFORTS

Reports of empirical studies of human performance and reliability are rather scarce in the open literature. The preponderance of reports that exist deal with *post facto* analysis of abnormal plant events involving human error or inappropriate human actions during operation and maintenance of plants. Summary reports are published by INPO based on the HPES. Similar *post facto* analysis of LERs and in-plant events have been reported (IAEA, 1990) which provide some attribution to various causal factors.

Rare in the literature are reports of data gathered during simulator exercises. Some studies report results from an older form of automatic data collection of operator manipulations (e.g., Yoshimura, 1988). Results of more intensive efforts which include human observers are reported by Norros (1986), Mosneron-Dupin (1988) and numerous reports by the authors of this paper (Spurgin, et al., 1990; Orvis, et al., 1990). A recent application of these techniques is reported in this conference. (Bareith, 1994) The following paragraphs review some of the studies that relate to the theme of this paper.

#### Waylett's Use of HPES

Waylett (1986) takes exception to reports of investigations of plant incidents that too often state "The operators responsible...have been counseled and provided remedial training". Waylett notes that causes are often not deficiencies in the operators or their training but other factors, including the design of the control room and quality of the operating procedures. Waylett presented two breakdowns of causes of incidents. INPO Human Performance Evaluation System (HPES) 1984 data shows that about 10% of the events were attributed to training but about 24% of corrective actions involved more training. Data from FP&L's Preventable Occurrence Study (POS) of 79 events showed that 27% were attributed to training deficiencies but 73% to other causes.

#### Hurst's Studies of Event Data

A novel extension of the analyses of event data is provided by Hurst *et al.* in a multi-dimensional and multi-level causal factors in a sociotechnical hierarchy. Data on causes of failure in pipework and vessels at nuclear and chemical plants indicate about 33-41% of the immediate causes of failure are human contributions, including operator error, induced impact and incorrect installation. Hurst extends the investigation into the hierarchy of the sociotechnical system to identify the underlying causes of events and presence or lack of effective preventive mechanisms under control of management decisions. The studies cited also quantify the contributions of each category to the total number of events investigated. The initial



steps in the studies, however, are the 1) assembly of data on events and 2) identification of the "immediate" cause. It is advocated herein that data from simulator exercises can be treated in a similar fashion to not only provide the basis for reduction of "immediate" causes but also to provide insights into the causal factors lying more deeply in the organization.

#### Norros' Analysis of Simulator Data

Norros and Sammatti (1986) reported on data collected at the Loviisa simulator involving two accident scenarios and 8 or 12 crews, respectively. Although observing instructors felt crews had performed well overall, the data revealed that all crews had committed deviations (3 to 9 per crew).

The deviation data were analyzed for causal factors in five phases for each scenario: observation, diagnosis, decision, execution and feedback. Causal factors were analyzed in a matrix of decision and execution functions versus error causes as summarized in Table 1. These data suggest that improved procedures might reduce the 17 to 30% of the deviations while improved technical training might reduce the 34 to 56% "knowledge" category and team training, the 14 to 16% "cooperation" category.

Table 1. Distribution of Deviations by Causes for Two Scenarios (Norros and Sammatti, 1986)

CAUSE CATEGORY	PERCENTAGE OF TOTAL	
	Scenario 1	Scenario 2
Control Room	5.5	3.2
Procedures	30.1	17.4
Cooperation	13.7	16.2
Knowledge	34.3	55.5
Disturbances	5.5	0
Simulator Effect	11.0	7.7
Total Number of Deviations	73	155

#### EPRI-Utility Sponsored Studies

Many of our reports on the EPRI research emphasize the collection and interpretation of data on crew time-responses, e.g., Spurgin 1990, but data were also collected on "deviations" committed by crews. A deviation is defined as: "a departure from a reference response to a given accident situation", i.e., what the crews did in contrast to: 1) verbatim following of emergency operating procedures (EOPs); 2) expected response per scenario design (trainer expectations); 3) management preferences in given situation; plus 4) spurious activities by crew. The commission of a "deviation" did not necessarily imply significant safety-related consequences; the data were analyzed later for impact.

The data were collected during crew requalification drills using five or six challenging scenarios, which were replicated at the respective plant simulators and repeated in successive years at the same simulator.

**Causal Factor Matrix.** We developed a taxonomy of deviation types and causes in a matrix format: crew response phases versus causal factors. Crew response phases are the

cognitive or detection-diagnosis-decision making (DDD) phase and the execution (or action) phase. The principal categories of deviation type are 1) mistakes (inappropriate intention leading consequentially to flawed DDD and actions) and 2) slips/lapses (inappropriate action after forming correct intent.) The causal factor matrix includes:

#### Deviation Cause Categories for DDD Phase.

- 1) Emergency Operating Procedure (EOP) Related
  - a. Select wrong EOP
  - b. Not follow EOP Exactly; miss steps
  - c. Misinterpret EOP
  - d. Inadequate EOP
- 2) Problem with Instrumentation or Cue Missed
- 3) Poor communications among crew

#### Deviation Cause Categories for Execution Phase.

- 1) Cognitive "slip" (e.g., executed wrong action but knew better)
- 2) Lack of Training/Knowledge (e.g., executed correct intended action at wrong panel or control)

The causal matrix includes two additional columns: impact level; and recovery.

**Impact Levels.** Four levels of impact were defined. Level 1 deviations are minor representing less than perfect performance; Level 2 affect crew efficiency where they may have to backtrack; Level 3 could result in damage to the plant; and Level 4 means a possible reduction in plant safety.

**Recovery.** Especially for PRA applications, it is important to know the likelihood that deviations will be detected and recovered.

A comprehensive report of the data remains unpublished; an extract of the data was presented at an ANS meeting (Orvis, et al., 1992). Table 2 summarizes the breakdown of causal factors based on published data from three PWRs. These data indicate that most (89%) of the initial deviations occurred in the DDD phase and most of those (67%) remained unrecovered. This implies that once a crew forms an intent, it is unlikely to discover its error. By contrast, only 11% of the initial deviations occurred in the execution phase and most (85%) of these were recovered. The dominant (75%) causal factors are seen to be EOP-related based on data from three PWRs. These results could be interpreted to mean that post-TMI control room design reviews have been effective in reducing the contribution of MMI deficiencies. In addition, the changeover to symptom-based procedures seems to have two effects that affect the relative importance of causal factors: 1) reduces the importance of operator knowledge since the procedures take the role of an expert system; and 2) failure to follow the procedures exactly is recorded as a "deviation" in the data.

Although training and on-the-job experience can compensate for some human factor deficiencies in procedures and MMI, the additional training effort and potential influence on crew reliability make it worthwhile to identify and correct such problems. But investigation of deeper lying causes might show that the ineffectiveness of training is not due to deficiencies in the training program per se, but to flaws in the climate and culture of the organization, e.g., the attitudes of operators or their managers toward the value of training for accidents that "can't happen" that they bring to the simulator sessions.

#### WHAT THE DATA SHOW

Tables 1 and 2 are representative of the summary data that can be obtained. When sufficient data are available, richer analyses can be made as suggested below.

**Sort by scenario:** The data may show that one or more scenarios are more difficult for all crews as illustrated in Figure 1; this is clearly a symptom of a systematic problem. (Figure 1 is a hypothetical representation of trends observed in limited data.) Investigation may reveal causal factors such as a) the procedure is flawed (e.g., steps out of order or invokes confusing 'AND' or 'OR' conditions), b) a section

Table 2. Summary: Causes and Recovery of Deviations

CAUSE CATEGORY		FRACTION OF TOTAL NUMBER OF DEVIATIONS
<b>SUMMARY OF CAUSES FOR D-D-D PHASE BY INCREASING IMPORTANCE</b>		
Crew Communications Problems		5%
Cues/Indications Missed		9%
Difficulties Using EOPs		75%
	<b>FRACTION OF EOP RELATED DEVIATIONS</b>	
Inadequate EOP	9%	
Selected Wrong EOP	14%	
Misinterpret EOP	19%	
Not Follow EOP	38%	
<b>EXECUTION PHASE</b>		<b>11%</b>
<b>RECOVERY:</b>	<b>FRACTION OF ALL DEVIATIONS RECOVERED</b>	
D-D-D Phase	37%	
Execution Phase	85%	

of the procedure is similar to a well-practiced section, but slightly different, c) crews have never or not recently been exposed to this scenario or portion of procedures.

Such data can be used to monitor and trend the reliability of crews or training effectiveness over time, as also illustrated in Figure 1. Initial results revealed flawed procedures for scenarios SGTR/LHS and ISI/ATWS. After modifying the procedure and training on them, measurements taken in Year 2 indicate much improvement with those two scenarios. Later years may again show a worsening trend, as illustrated. Training and operations managers can review such data and make appropriate plans to improve or sustain crew reliability.

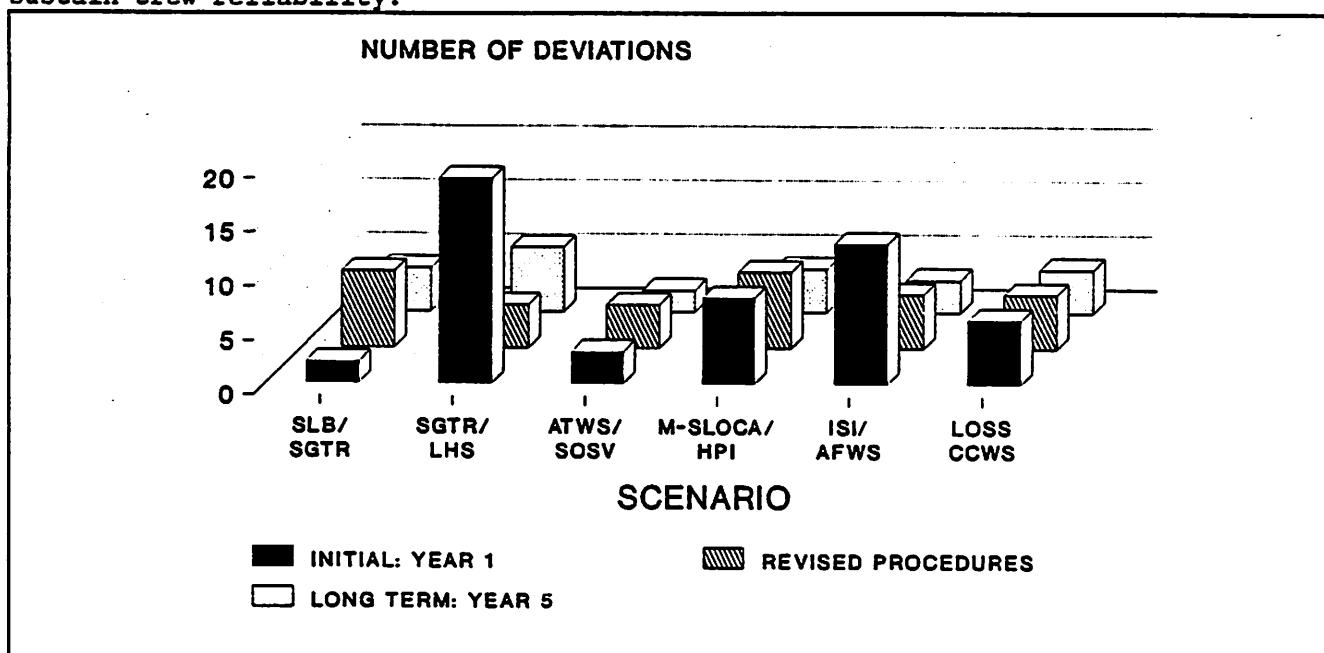


Figure 1. Deviations for Key Scenarios over Several Years

Sort by crew: The data may reveal that many of the deviations in one scenario or

across all scenarios were committed by one or two crews (not illustrated). Investigation may reveal causal factors such as a) the SRO lacks some basic reading skills causing difficulties in reading the procedures; b) the crew has deficient team skills in communicating and working together; c) the crew may have a member in a new position and in need of more training and more experience. These may not be revealed in normal job situations nor by observation during simulator exercises because the performance seems nominal. An example is described by Molden (1989) where analysis of simulator data, indicated that the performance of one crew was consistently inferior to the others. Review of the video tapes showed that one control board operator consistently "dropped out" of the crew early in each scenario and actually became a distraction to the SRO, thereafter.

## CONCLUSION

First, you have to get the data! Once recorded, crew reliability data for many crews over many scenarios and spanning various time periods, before and after changes in control room design or procedures or training program may be sorted and analyzed to study causal factors. At present, there is no wide-spread application of such data collection and analysis in the industry.

Results of data analysis can be applied not only to improving the plant hardware and software to promote higher crew reliability but also in a plant-specific "living PRA" to assess the safety significance and cost benefits of such improvements. To study influences of organizational factors, data must be collected on the culture and climate of the organization at various levels.

## REFERENCES

- N.W. Hurst, et al., "A classification scheme for pipework failures to include human and sociotechnical errors and their contribution to pipework failure frequencies", *Journal of Hazardous Materials*, 26 pp 159-186, Elsevier, NY (1991).
- D.D. Orvis, P. Moieni, and V.Joksimovich, "Organizational and Management Influences on Safety of Nuclear Power Plants: Use of PRA Techniques in Quantitative and Qualitative Assessments", Draft NUREG/CR-5752, U.S. NRC (1993).
- J.E. Molden, "Research in operations: lessons learned", *Proc. of Eighth Symposium on Training of Nuclear Facility Personnel*, Gatlinburg, (1989).
- F. Mosneron-Dupin, et al., "Human factors data and the use of simulators", *ESRRDA Seminar on Human Factors*, Bournemouth, UK (1988).
- L. Norros, and P. Sammatti, "Nuclear power plant operator errors during simulator training", VTT-446, Technical Research Center of Finland (1986).
- D. D. Orvis, et al., "Applications of observations from simulators to assess crew reliability", *Proceedings American Nuclear Society 1992 Annual Meeting*, Boston, MA (1992).
- D. D. Orvis, et al., "Operator Reliability Experiments at Maanshan", EPRI NP 6951-L, Electric Power Research Institute (1990).
- J. Reason,, *Human Error*, Cambridge University Press, New York (1990).
- A. J. Spurgin, et al., "Operator Reliability Experiments Using Power Plant Simulators", Volumes 1, 2, and 3, EPRI NP-6937, Electric Power Research Institute (1990).
- A. J. Spurgin, P. Moieni and D.D. Orvis, "Some thoughts on the use of data for assessing training effectiveness", 1993 SCS Simulation Multiconference, Society for Computer Simulation, Arlington, VA (1993).
- W. J. Waylett, "Can training improve human performance?", *Proceedings of International Topical Meeting on Advances in Human Factors in Nuclear Power Systems*, ANS/ENS, Knoxville, TN (1986).
- S. Yoshimura, et al., "An analysis of operator performance in plant abnormal conditions", *IEEE Fourth Conference on Human Factors and Power Plants*, Monterey, CA (1988).
- International Atomic Energy Agency (IAEA), "Human Error Classification and Data Collection", IAEA-TECDOC-538, Vienna (1990)

**088 Risk Based Methods for Reliability/Availability/Maintainability**

*Chair: S. Lydersen, Norwegian Inst. Technol.*

**Some New Measures of Reliability Importance with Applications to Reliability Centred Maintenance**

*S. Lydersen (Norwegian Inst. Technol.)*

**"INTEGRIT" - A Parametric Reliability and Maintainability Methodology and Safety Risk Management Tool**

*R. Vote, T. Barritt, R. Blanchford (ELINTECH)*

**On-Line VS. Off-Line Maintenance in Nuclear Power Plants - Insights from a Cycle-Wide O&M Cost Model**

*J.R. Hewitt, L.A. Bennett, R.L. Durling (ERIN Eng. & Res.)*

**A User-Friendly Program for System and Component Availability Monitoring and Its Potential Application in Maintenance Rule Implementation**

*D.M. Kapinus (Commonwealth Edison); T.A. Petersen (NUS)*

## **SOME NEW MEASURES OF RELIABILITY IMPORTANCE WITH APPLICATIONS TO RELIABILITY CENTRED MAINTENANCE**

Stian Lydersen

Department of Mathematical Sciences  
The Norwegian Institute of Technology  
N-7034 Trondheim, Norway

### **INTRODUCTION**

During the last decades, several measures of reliability importance have been suggested. However, the potential for practical use of these measures is larger than seems to have been realized so far. One reason may be that the practical engineering interpretations have not been emphasized enough. This paper presents some new measures of reliability importance:

- 1) Reliability importance for component classes.
- 2) Cut set structural importance

Practical interpretations are given, with application to design improvement and reliability centred maintenance (RCM). The suggested measures are compared to existing measures.

### **DEFINITIONS**

Consider a system with  $n$  components, and define

$X_i = 1$  (0) if component no  $i$  is (not) functioning at time  $t$ ,  $i = 1, 2, \dots, n$ .

The structure function is

$\phi(\underline{X}) = \phi(X_1, \dots, X_n) = 1$  (0) if the system is (not) functioning at time  $t$ .

Let  $p_i = P(X_i = 1)$ ,  $i=1, 2, \dots, n$ . If all components are independent ( $X_1, \dots, X_n$  are stochastically independent), there exists a function  $h$  such that

The probabilities  $p_i$  and  $P(\phi(\underline{x})=1)$  will be denoted the availability of component number  $i$  and of the system, respectively. The following notations will also be used:

$$(1_i, \underline{p}) = (p_1, \dots, p_{i-1}, 1, p_{i+1}, \dots, p_n)$$

$$(0_i, \underline{p}) = (p_1, \dots, p_{i-1}, 0, p_{i+1}, \dots, p_n)$$

$$(\cdot_i, \underline{p}) = (p_1, \dots, p_{i-1}, \cdot, p_{i+1}, \dots, p_n)$$

The notations  $(1_i, \underline{X})$  etc will be used in the same way.

## RELIABILITY IMPORTANCE

Birnbaum's (Birnbaum, 1969) measure of importance for component no  $i$  is defined as

$$\begin{aligned} I^B(i) &= \partial h(\underline{p}) / \partial p_i \\ &= P(\phi(1_i, \underline{X}) - \phi(0_i, \underline{X}) = 1) \\ &= P(\text{Component no } i \text{ is critical for the system}) \end{aligned}$$

Component no  $i$  is said to be critical for the system if the rest of the system is in such a state that the system is functioning if and only if component no  $i$  is functioning.

It can be shown that  $h(\underline{p})$  is linear in each  $p_i$  (see e.g. Høyland and Rausand, 1993). Hence, if  $p_i$  is changed by a quantity  $\Delta p_i$ , the change in system availability will be

$$\Delta h(\underline{p}) = I^B(i) \Delta p_i.$$

Criticality importance is defined as (see e.g. Høyland and Rausand, 1993):

$$I^{CR}(i) = P(\text{Component no } i \text{ is critical for the system and in a failed state, given that the system is in a failed state})$$

Consider a system in a failed state. Then,  $I^{CR}(i)$  is the probability that component no  $i$  is in a failed state and the system will function again once the component is restored.

The improvement potential (See i.e. Aven, 1992) is defined as the improvement in system availability if component no  $i$  is replaced with a perfect component:

$$I^A(i) = h(1_i, \underline{p}) - h(\underline{p}) = h(p_1, \dots, p_{i-1}, 1, p_{i+1}, \dots, p_n) - h(p_1, \dots, p_n).$$

The following simple relation exists between these three measures of importance:

$$I^A(i) = (1-p_i) I^B(i) = (1-h(\underline{p})) I^{CR}(i).$$

Considering the direct interpretation and applicability in RCM, it is surprising that the improvement potential has not been used more than what seems to be the case. Further, the improvement potential is proportional to the criticality importance, and gives a quantified fault-seeking list as a by-product.

For an overview of reliability importance measures, see e.g. Lambert (1975).

## RELIABILITY IMPORTANCE FOR CLASSES OF COMPONENTS

In many systems, more than one individual of one component type may be included. If the availability on one such component is improved, the same improvement will usually be carried out on all components of the same type. For example, two identical parallel branches of a subsystem may include the same component type. That is, one may be interested in the effect of changing the availability of a class of components in the system simultaneously.

Assume that the components are numbered such that component number  $1, \dots, r$  are of the same type, and that  $p_1 = \dots = p_r$ . The improvement potential for this class of components is natural to define as

$$I^A((1, \dots, r)) = h(1, \dots, 1, p_{r+1}, \dots, p_n) - h(p_1, \dots, p_r, p_{r+1}, \dots, p_n)$$

Further details, as well as generalizations the other reliability importance measures above, are given by Lydersen (1993).

## STRUCTURAL IMPORTANCE

### Birnbaum's Measure of Structural Importance

Measures of structural importance are only based on the structure of the components, and is not a function of component reliabilities. Birnbaum (1969) has suggested a measure as follows: A *critical path vector* for component no  $i$  is a state vector  $(1_i, \underline{x})$  such that

$$\phi(1_i, \underline{x}) = 1 \quad \text{and} \quad \phi(0_i, \underline{x}) = 0.$$

In other words,  $(1_i, \underline{x})$  is a critical path vector for component number  $i$  if and only if component number  $i$  is critical for the system. This is equivalent to

$$\phi(1_i, \underline{x}) - \phi(0_i, \underline{x}) = 1.$$

The total number of critical path vectors is

$$\eta_\phi(i) = \sum_{(\underline{x})} [\phi(1_i, \underline{x}) - \phi(0_i, \underline{x})].$$

There exist  $2^{n-1}$  states of the vector  $(\underline{x})$ , and Birnbaum's measure of structural importance is defined as

$$B_\phi(i) = \eta_\phi(i) / 2^{n-1}.$$

A high value of  $B_\phi(i)$  indicates a high importance. For a given system,  $B_\phi(i)$  may be calculated by computing each of the  $2^{n-1}$  terms in  $\eta_\phi(i)$ , or by using the identity  $B_\phi(i) = I^B(i)|_{p=1/2}$  (see e.g. Høyland and Rausand, 1993).



## Cut Set Structural Importance

A set  $K$  of components is said to be a cut set for the system if

$$X_i = 0 \text{ for all } i \in K \Rightarrow \phi(X) = 0.$$

A cut set is said to be minimal if it cannot be reduced without losing the status as a cut set.

Another measure of structural importance of component no  $i$  is the number of components in the smallest minimal cut set containing component no  $i$ :

$$L_\phi(i) = \min_{\{j: i \in K_j\}} |K_j|$$

A low value of  $L_\phi(i)$  indicates a high importance. For example, if the system contains cut sets of order 1, the components in these cut sets will automatically be most important. This measure has two advantages compared to Birnbaum's measure:

- The definition has a more direct interpretation and hence, is more easy to communicate to engineers with limited background in reliability theory.
- It is easier to calculate than  $B_\phi(i)$ .

As a special case, consider a system with only *disjoint* minimal cut sets. Such systems arise in many practical cases. For this special case, it is straightforward to show (Lydersen, 1993) that  $B_\phi(i)$  and  $L_\phi(i)$  give exactly the same ranking of the components.

$$B_\phi(i) = B_\phi(j) \Leftrightarrow L_\phi(i) = L_\phi(j) \quad \text{and} \quad B_\phi(i) > B_\phi(j) \Leftrightarrow L_\phi(i) > L_\phi(j)$$

However, the two measures do not always give the same ranking. Consider the system represented by the reliability block diagram in Figure 1.

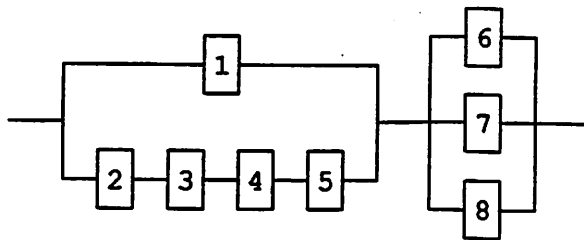


Figure 1. Example, reliability block diagram, structural importance.

In this case,

$$B_\phi(1) = 105/128 > B_\phi(6) = B_\phi(7) = B_\phi(8) = 17/128 > B_\phi(2) = B_\phi(3) = B_\phi(4) = B_\phi(5) = 7/128$$

$$L_\phi(1) = L_\phi(2) = L_\phi(3) = L_\phi(4) = L_\phi(5) = 2 < L_\phi(6) = L_\phi(7) = L_\phi(8) = 3$$

Hence, the two measures give opposite ranking of the component classes  $\{2,3,4,5\}$  and  $\{6,7,8\}$ . Further,  $L_\phi(i)$  does not differ between the classes  $\{1\}$  and  $\{2,3,4,5\}$ . In the next subsection, a refinement of  $L_\phi(i)$  to make this difference will be suggested.

### Cut Set Structural Importance and Reliability Importance

As already mentioned, if all components are independent and  $p_i = 1/2$ ,  $i=1,2,\dots,n$ , then  $B_\phi(i) = I^B(i)$ ,  $i=1,2,\dots,n$ . In this Section, a relation between cut set structural importance and the improvement potential is derived.

Using a notation common in quantitative fault tree analysis, let  $q = 1 - p$ , that is,  $q_i = 1 - p_i$ ,  $i=1,2,\dots,n$ , and let  $Q_0 = 1 - h(p) = 1 - h(1 - q) = g(q)$ . If all  $q_i \ll 1$ , say  $< 10^{-2}$ , then

$$Q_0 \approx \sum_{j=1}^k \prod_{i \in K_j} q_i$$

Further,

$$I^B(i) = \frac{\partial h(p)}{\partial p_i} = \frac{\partial Q_0}{\partial q_i} \approx \sum_{\{j : i \in K_j\}} \prod_{i \in K_j, i \neq i} q_i$$

and

$$I^A(i) = q_i I^B(i) \approx \sum_{\{j : i \in K_j\}} \prod_{i \in K_j} q_i$$

If all  $q_i = q$ , then

$$I^A(i) \approx m_i q^{L_\phi(i)}$$

where  $m_i$  is the number of minimal cut sets of order  $L_\phi(i)$  containing component number  $i$ . Taking the logarithms of both sides, we obtain

$$\log_{10}(I^A(i)) \approx \log_{10}(m_i) - L_\phi(i) \log_{10}\left(\frac{1}{q}\right)$$

Recall that this approximation is valid only if  $q \ll 1$ , say,  $q < 10^{-2}$ . In almost all practical cases with  $q \ll 1$ , the inequality  $m_i < 1/q$  will also hold, in fact, we will have

$$L_\phi(i_1) > L_\phi(i_2) \Rightarrow I^A(i_1) > I^A(i_2).$$

That is,  $L_\phi(i)$  gives a component ranking that is not in conflict with  $I^A(i)$ . Further, in these cases,

$$\{L_\phi(i_1) = L_\phi(i_2)\} \wedge \{m_{i_1} > m_{i_2}\} \Rightarrow I^A(i_1) > I^A(i_2)$$

The above implication suggests a refinement of the cut set structural importance measure may be suggested: If  $L_\phi(i_1) = L_\phi(i_2)$ , then component  $i_1$  is more important than  $i_2$  if  $m_{i_1} < m_{i_2}$ . In more general terms, define the cut set order vector for component number  $i$ :

$$\underline{C}_\phi(i) = (c_{i,1}, c_{i,2}, \dots, c_{i,n})$$

where  $c_{i,j}$  is the number of minimal cut sets of order  $j$  containing component number  $i$ . Component  $i_1$  is more important than  $i_2$  if  $\min\{j : c_{i_1,j} > 0\} < \min\{j : c_{i_2,j} > 0\}$ . If these are equal, then component  $i_1$  is more important than  $i_2$  if  $c_{i_1,d} > c_{i_2,d}$ , where

$d = \min\{j : c_{i_1,j} \neq c_{i_2,j}\}$ . This may be illustrated by revisiting the system in Figure 1. The

structural importance measures and the rankings are given in Table 1.

It may be beneficial to define a modified cut set importance measure in terms of a scalar instead of the cut set order vector  $\underline{C}_\phi(i)$ . This may be done by defining

**Table 1.** Example, structural importance measure for reliability block diagram in Figure 1.

Component number i	$B_p(i)$		$L_p(i)$		$C_p(i)$	
	Value	Rank	Value	Rank	Value	Rank
1	105/128	1	2	1	(0,1,0,0,0,0,0)	1
2	7/128	5	2	1	(0,4,0,0,0,0,0)	2
3	7/128	5	2	1	(0,4,0,0,0,0,0)	2
4	7/128	5	2	1	(0,4,0,0,0,0,0)	2
5	7/128	5	2	1	(0,4,0,0,0,0,0)	2
6	17/128	2	3	6	(0,0,1,0,0,0,0)	6
7	17/128	2	3	6	(0,0,1,0,0,0,0)	6
8	17/128	2	3	6	(0,0,1,0,0,0,0)	6

Rausand (1991) suggests the following way to rank minimal cut sets in a fault tree according to importance:

- i) The minimal cut sets of lowest order are most important.
- ii) If two minimal cut sets have the same order, the basic events are ranked as follows:
  1. Human error
  2. Active equipment failure
  3. Passive equipment failure

This ranking is based on the assumption that human errors have a larger probability than active equipment failures (equipment failing during operation), which again have a larger probability than passive equipment failures (passive equipment such as a storage tank or standby equipment). This categorization may also be used for a generalization of the component importance measure  $L_p(i)$  for components having the same value of  $L_p(i)$ .

## ACKNOWLEDGEMENT

I am grateful to my colleague Professor Marvin Rausand for comments and suggestions to this paper.

## REFERENCES

- Aven, T. A.: "Reliability and Risk Analysis". Elsevier, (1992).
- Birnbaum, Z. W.: "On the Importance of Different Components in a Multicomponent System in Multivariate Analysis - II". Ed. P. R. Krishnaiah, Academic Press, p 581 - 592. (1969)
- Høyland, A. and Rausand, M.: "Reliability Theory. Models and Statistical Methods." To be published by Wiley in 1993 or 1994.
- Lambert, H. E.: "Measure of Importance of Events and Cut Sets in Fault Trees". In "Reliability and Fault Tree Analysis. Theoretical and Applied Aspects of System Reliability and Safety Assessment", Ed. R. E. Barlow, J. B. Fussell, N. D. Singpurwalla, SIAM, Philadelphia (1975).
- Lydersen, S.: "Measures of Reliability Importance and RCM". Presentation at Society of Reliability Engineers Symposium, Malmö, Sweden, 25-26 November 1993.
- Rausand, M.: "Risikoenalyse. Veiledning til NS 5814" (Risk analysis. Guide to Norwegian Standard NS 5814. In Norwegian.) TAPIR, Trondheim, Norway (1991).

## **"INTEGRIT" - A PARAMETRIC RELIABILITY AND MAINTAINABILITY METHODOLOGY AND SAFETY RISK MANAGEMENT TOOL**

Richard Vote, Terry Barritt & Rex Blanchford

ELINTECH Ltd  
69 Breton House  
Barbican  
London EC2Y 8DQ England

### **CONCURRENT DESIGN EVALUATION**

Concurrent consideration of availability, reliability, maintenance and life cost strives for  
*Maximum Availability.*

*Maximised Safety and Integrity by design and procedural measures*

*Minimum through life costs with simple reliable systems*

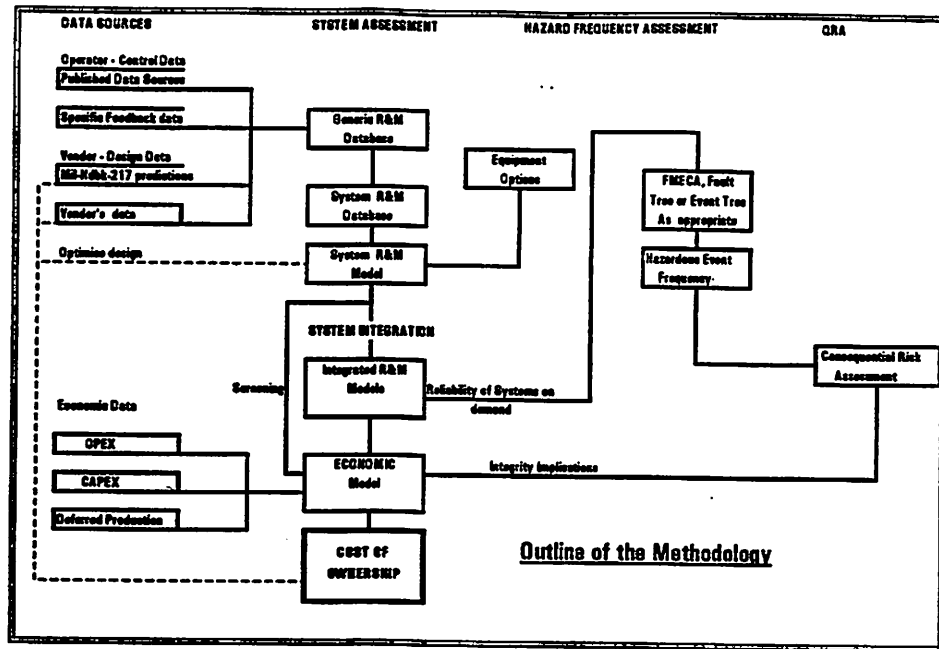
*Optimised maintainability, operability and logistics support.*

"Integrit" has been organically grown and is currently being used in major offshore, onshore petrochemical and air traffic control projects, being as adaptable as the spreadsheet program it is based on. "Integrit" is a methodology that has grown from simple evaluations to the complete structure covering all stages of design presented here, it is not a software program. This presentation provides an overview with spreadsheets shown as sample "pictures" in this paper, full size copies can be obtained from the authors.

Definitions of terminology and criteria are important in application to a complex project and similarly data gathering must be constrained to that sufficient to establish confidence for the engineering design rather than to provide unrestrained challenges to the mathematician!

Most reliability standards are geared to funded R&D programmes not "off the peg" designs however expectations of reliability from suppliers is becoming the norm. The users "stress" must also be accounted for in system design. QA for data is achieved through "Control" and "Design" assessments where manufacturer's estimates are compared with historical sources. Dialogue may then produce improvements as long as these are not limited by the state of the technological art or by costs.

In addition to failure rates, levels of reparability, test, diagnosis and restoration times, the life expectancy of the equipment and the maintenance activities necessary to preserve designed capability and performance; all form the "data base" for the assessments. Because the users operational conditions affect achieved Availability and Reliability and thus Safety, the analysis must account for these factors and introduce them into the calculations. The data bases therefore are split between the "Generic" and "System" influences.



In the *Generic Data Base* failure rates for each failure mode are apportioned to Covert and Overt effects. The Overt is further split into "Degraded" and "Failed/STR" modes and MTTR (Mean Time To Repair) is calculated.

GENERIC RELIABILITY DATA BASE						
TYPE CODE	ITEM DESCRIPTION	Failure mode Description	Failure rate FM/Hrs	Repair Time Hrs	Failure Rates per M/Hrs Apportioned to each effect	
					Covert	Overt
<b>The Generic Reliability Data Base</b> <b>Key to generic database layout</b> A code given to the type of equipment which refers to the same used in the model. Description of the item and its function. The failure modes listed for the item in the data source. Covert Failure - concealed except by test or full on demand Degraded Failure - Continued operation but not designed performance Total Failure - Covert Failure causing serious trip or cessation of function Total Failure Rate for Failure mode MTTR for Failure mode Covert failure rate F Rate - degraded F Rate - Failed						
OUTPUTS TO HIGHER MODELS SHOWN THUS						
WV	WING VALVE (OIL or GAS) < 24 lbs	Fail to Close	1.3	1.5	1.3	
		Fail to Open	2.5	1.5		2.5
		Unknown Critical	2.1	2	2.1	
		Delayed Operation	12	0.5	8	8
		Internal Leakage	2.8	3.5	2.8	
		External Leakage	2.2	3.5		2.2
		Unknown Degraded	2.8		2.8	2.8
		Faulty Indication	14	0.5	7	7
Total for Failure Rates and MTTR			38.5	1.8	21.8	10.8
						2.5

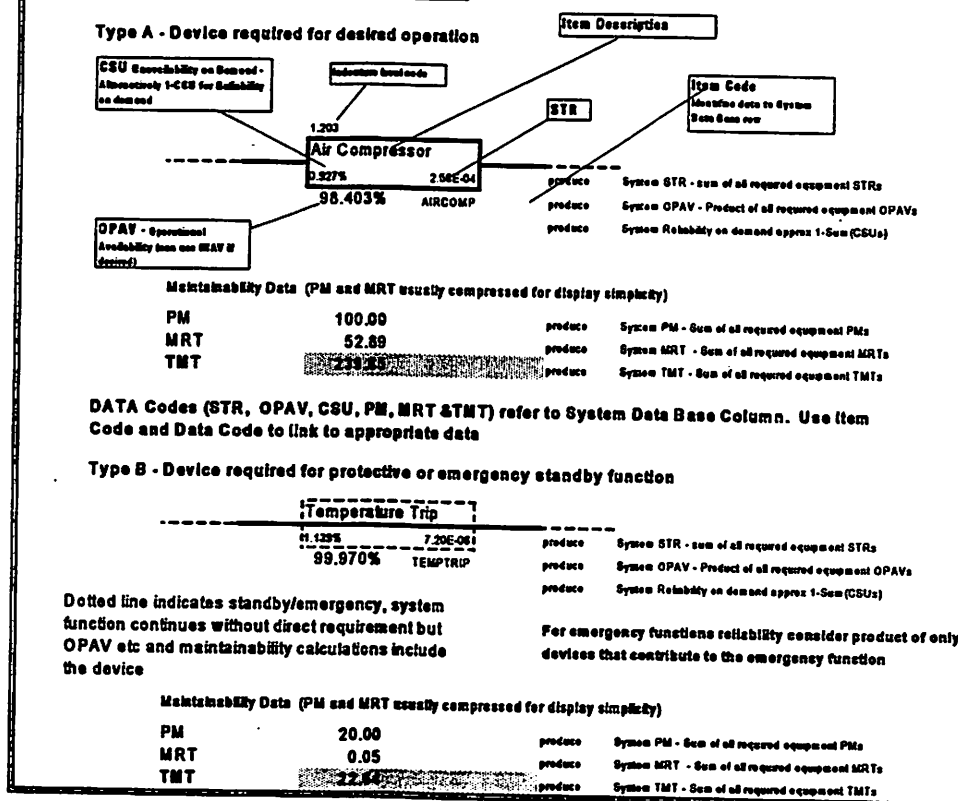
The *System Data Base* worksheets following the recommendations made by SINTEF for evaluation of Safety Critical System Reliability in the offshore industry, have been developed and extended to cover maintainability aspects using the techniques devised by the US and UK Defence and Aerospace Industries. These outputs are shown by shaded cells with the data underlined. Each output column has a *output code* and each row the *item code*, therefore the *data code* will be for example WVCSU identifying Critical Safety Unavailability of Wing Valves and is the NAME of the cell containing the data. Other outputs are similarly named.

This facilitates links to "higher" models and is the basis of "Integrit".

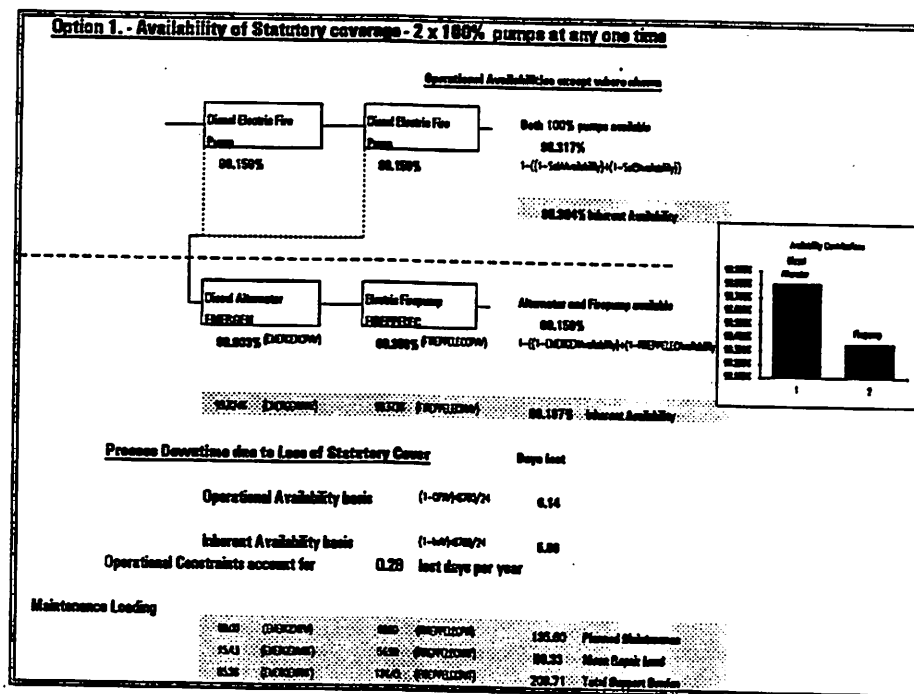
shaded cells indicate inputs, shaded and underlined cells indicate outputs. The outputs are identified by the Item Code with the appropriate suffix e.g. WVOPAV is the Operational Availability of a Wing Valve

The *System Models* are based on the Reliability Block Diagram, representing the system dependencies with redundancies and standby configurations producing.

#### Examples of System Block Diagram Construction



The example shown is typical (but does not reflect any particular installation or system). The availability of 2 x 100% sources is shown below with downtime and maintenance loading.



## ON-LINE VS. OFF-LINE MAINTENANCE IN NUCLEAR POWER PLANTS - INSIGHTS FROM A CYCLE-WIDE O&M COST MODEL

James R. Hewitt, Lawrence A. Bennett, Ronald L. Durling

Safety and Reliability Division  
ERIN Engineering and Research, Inc.  
2175 N. Calif. Blvd., Suite 625  
Walnut Creek, CA 94596

### OVERVIEW

This paper addresses a popular question among nuclear power plant outage managers:

*Is there a technical basis for performing certain maintenance tasks - tasks historically confined to outages - during power operation?*

The paper describes a quantitative model of cycle-wide operations and maintenance (O&M) costs. The results suggest on-line maintenance tends to reduce plant safety, and on that basis alone, may be regarded as unacceptable. However, it may be possible to develop a technical basis similar to that historically used in backfit analyses: that at some point, the cost of performing maintenance during shutdown exceeds the benefit gained by improving plant safety. The break-even point can be estimated with a fairly simple relationship between accident risk and the outage critical path time associated with work on that component.

### THE PROBLEM

Outage costs are one of the biggest variable O&M costs in a nuclear power plant. Of all the costs associated with an outage, one of the biggest is the cost of replacement power. (In many settings, power replacement costs exceed \$0.5M per day.) Hence, one of the most effective ways to minimize O&M costs is to minimize outage costs, which in turn, translates into minimizing outage duration. This, in brief, is the objective of outage planners.

Outage planners face a variety of constraints. Technical Specifications and other regulatory and self-imposed requirements limit the extent to which maintenance can



be performed on redundant systems. These tend to be rigid constraints; exceptions are rare. Another constraint is less rigid: the scope of work to be performed during the outage. Some work can only be performed during an outage (e.g., refuelling in light water reactors). Other work is optional, and some of that could conceivably be performed during power operation (e.g., standby diesel generator overhauls). When such work requires time on the outage critical path (the combination of tasks determining outage duration), it constrains the outage planners' ability to minimize outage duration. It is at this point that outage planners begin questioning whether such work could be performed during power operation.

Given recent trends in the economic and regulatory environment, such questions from outage planners are drawing increased attention. Historically, there has been little or no technical basis for the answers. The analytic problem, therefore, is to develop and exercise a cycle-wide O&M cost model to evaluate such questions.

## METHOD AND MODEL

The first step toward model-building is to define the evidence needed to decide between on-line or off-line maintenance. Such evidence must be acceptable to both outage planners and regulators. With no historical precedent, the best one can do is speculate about which decision criteria might really be acceptable. In that regard, consider the following possibilities:

- On-line maintenance reduces power replacement costs (by reducing outage critical path time), *and* it does not violate a strict interpretation of the operating license.
- On-line maintenance reduces power replacement costs, *and* does not cause plant risk to exceed a specified safety goal.
- On-line maintenance reduces power replacement costs, *and* it improves overall plant safety.
- On-line maintenance reduces power replacement costs, the cost difference exceeds the increased "expected cost" of plant accidents, *and* on-line maintenance does not cause plant risk to exceed a specified safety goal.

The first two decision criteria might satisfy outage planners, but probably not regulators. From the latter's perspective, plant safety depends on more than compliance with regulations and safety goals; it also depends on a safety conscious culture, which aggressively seeks ways to maximize plant safety.

The third criterion is extremely stringent, and should satisfy both outage planners and regulators. It has no practical value, however, because there are no maintenance actions meeting this criterion. For any tasks which might be performed during power operation, one can imagine a safer condition during an outage (perhaps near the end of a very long outage, with fuel removed from the RPV and all other equipment available).

Of all these decision criteria, the fourth is the most likely to satisfy both outage planners and regulators, *and* have potential for a practical application. The requirement to offset the increased expected cost of plant accidents is similar to the rationale historically used in backfit analyses. This criterion is also consistent with a

safety-conscious culture; it allows a utility to strive for a rational balance between safety and costs.

The following assumptions help simplify the analytic model for this criterion:

1. The major determinant of variable O&M costs is the outage duration. By ignoring other variable costs, the model tends to err on the side of safety, rather than economics.
2. A change in maintenance practices may change the expected frequency of fuel damage accidents during both power operations and shutdown, but not the expected magnitude of radionuclide releases or off-site doses associated with those accidents. This assumption allows for a much simpler model. It should be applied with care because it is not generally conservative.
3. An acceptable estimate of a cost/dose conversion factor is \$1,000/man-rem, the same value used by the NRC in prioritizing generic safety issues.
4. By saving time on the outage critical path, on-line maintenance will tend to increase the time spent in power operation, and decrease the time spent in outages.

These assumptions lead to the following relationships between the effects of maintenance tasks and variable O&M costs:

$$\Delta C_{SD} = C_{RP} \cdot \Delta D_{OUTAGE} + C_{DOSE} \cdot \left[ (1 - A) \cdot \sum_j \Delta f_j d_j \right]$$

$$\Delta C_P = C_{DOSE} \cdot \left[ A \cdot \sum_i \Delta f_i d_i \right]$$

where:

$C_{SD}$	=	Outage cost
$C_P$	=	Cost of expected offsite doses due to at-power accidents
$C_{RP}$	=	Cost of replacement power
$D_{OUTAGE}$	=	Change in outage duration
$C_{DOSE}$	=	Cost/dose conversion factor
$A$	=	Plant availability factor
$f$	=	Frequency of core damage events
$d$	=	Dose/event conversion factor
$i, j$	=	Subscripts denoting events for power operation and shutdown, respectively.

With these relationships, one can determine the best time to schedule maintenance by finding the least-cost alternative, subject to the constraint of meeting safety goals.

## RESULTS

This modeling approach leads to a fairly simple relationship between three parameters:

- the time a maintenance task spends on the outage critical path,
- plant accident risk, given the maintenance unavailability of the affected components, and
- the safety goal for core damage accidents.

The time a maintenance task spends on the outage critical path has a direct effect on the costs of the outage. These costs include costs associated with replacement power as well as personnel costs. However, there is a more complicated relationship between the critical path time and the core damage frequency during the outage. During shutdown operations, the risk of component maintenance is dependent upon several factors, such as the number of redundant trains remaining in service, the water volume present in the reactor coolant system (RCS), and the decay heat load. The change in the at-power plant accident risk tends to be strictly a function of the ratio of the new component unavailability to the original unavailability.

If the expected cost increase of an at-power accident does not exceed the cost reduction associated with performing the maintenance during power operations, on-line maintenance might be justified, as long as an acceptable safety goal has not been exceeded. For example, utility personnel at a representative plant wish to move emergency diesel generator (EDG) maintenance activities from an upcoming outage to a seven day period of full-power operations. It was found that performing this EDG maintenance on-line increased the at-power core damage frequency (CDF) from  $4.67\text{E-}05/\text{year}$  to  $5.18\text{E-}05/\text{year}$ . This increase of  $5.10\text{E-}06/\text{year}$  in the at-power CDF provides the first step in estimating the resultant public health risk increase. The second step requires an estimate of the offsite effects of such an event. A coarse estimate of a dose conversion factor is  $1\text{E}8 \text{ rem/event}^1$ . Assuming an availability factor of 0.70 and a cost/dose conversion factor of  $\$1000/\text{rem}$ , the increased cost of expected offsite doses as a result of performing on-line maintenance is  $\$357,000$ .

On-line EDG maintenance does not have as its only effect an increased cost due to increased public risk. Removing these activities from the outage critical path provides the benefit of reducing the length of the outage and possibly reducing the shutdown CDF. In this case, the EDG maintenance activities had been planned for a time when the refueling cavity was flooded. This maximized the time to RCS boiling, thus reducing the risk of having one EDG out of service. Because of this, the shutdown CDF did not noticeably change when these maintenance activities were removed from the planned outage. Therefore, given a replacement power cost of  $\$200,000$  per day and neglecting any cost savings associated with a nominally reduced shutdown CDF, a two-day reduction of the outage as a result of this change will satisfy the decision criteria outlined above.

## CONCLUSION

The preceding model demonstrates how competing costs might be computed. The demonstration is limited to a problem with one degree of freedom: a decision about when to perform a single maintenance task, assuming all other maintenance tasks are

fixed. Realistically, outage planners have a problem with  $n$ -degrees of freedom: every maintenance task can be rescheduled within an outage, as well as several that could conceivably be performed on-line. This "real world" problem is amenable to an optimization framework, e.g., linear programming.

A simple one-to-one relationship between the at-power cost increase and the shutdown cost reduction may not be acceptable to regulators. The key to using an optimization model is to establish the appropriate weighting factors in the objective function and constraints. The risks and cost conversion factors presented in this paper comprise most of the information needed to establish those weights. Hence, in addition to providing insights about one selected case study, this paper can be considered a stepping stone to a more sophisticated level of outage scheduling technology: a technique for designing short outages without compromising safety.

## REFERENCE

1. "Handbook for Value-Impact Assessments," NUREG/CR-3568 (PNL-4646), December, 1983.

## **A USER-FRIENDLY PROGRAM FOR SYSTEM AND COMPONENT AVAILABILITY MONITORING AND ITS POTENTIAL APPLICATION IN MAINTENANCE RULE IMPLEMENTATION**

**Thomas A. Petersen**

**David M. Kapinus**

**NUS  
1411 Opus Place, Suite 103  
Downers Grove, IL 60515**

**Commonwealth Edison Company  
1400 Opus Place, Suite 300  
Downers Grove, IL 60515**

### **INTRODUCTION**

The availabilities of nuclear power plant systems and components are becoming more and more important from a financial, personnel safety, nuclear safety and regulatory requirements standpoint. As a result, it is evident that a comprehensive, yet simple and user-friendly program for system and component tracking and monitoring is needed to assist in effectively managing the various and many required systems and components with their large numbers of associated availability records.

Based on the need for an availability monitoring tool, a user-friendly computer software program for system and component availability monitoring has been developed that calculates, displays and monitors selected component and system availabilities. This is a Windows™ based (Graphical User Interface) program that utilizes a system flow diagram for the data input screen (refer to Figure 1 for illustration). This screen also provides a visual representation of availability values and limits for the individual components and associated systems. This program is designed to be customized to the user's plant-specific system and component selections and configurations.

### **BACKGROUND**

Over the many years of commercial nuclear power electric generation, the focus of utility resources has changes several times from power plant construction/schedules, to nuclear safety, to now currently, cost effectiveness of operations. Technical Specification compliance has always been a major driver in ensuring nuclear safety. As of recently, the Maintenance Rule (10 CFR 50.65), is soon to become another major factor

(implementation by July, 1996) in maintaining nuclear safety via proper maintenance of nuclear plant equipment.

The Maintenance Rule furthermore specifies that monitoring or preventive maintenance activities must be balanced against the objective of minimizing the unavailability of plant equipment, since unavailable equipment affects the capabilities of plant safety functions (therefore increasing risk). Based on this, NRC Regulatory Guide 1.160, "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants", recommends that, for example, plant-specific emergency diesel generator reliability and *unavailability* should be monitored as goals under 10 CFR 50.65 or established as performance criteria under the plant's preventive maintenance program. This Regulatory Guide further recommends that when performance criteria is not met, that goals should be established and performance monitoring be continued, but consistent with an appropriate balance between emergency diesel generator reliability and *unavailability*.

Whether nuclear safety program initiatives are driven by Technical Specifications, the Maintenance Rule, power generation capacity, personnel safety, one major common link in ensuring safety is the ability to monitor system and component availabilities (or unavailabilities). It is additionally important to monitor availabilities properly (collection and analysis of data), since unavailability causes and effects can significantly impact plant operations and costs.

## SOFTWARE REQUIREMENTS SPECIFICATION

The availability monitoring program was designed with the common 80386 IBM compatible personal computer (PC) in mind, since it was expected that most users would have at least this type of PC. A faster computer, however, will speed the screen access time. The other necessary hardware includes one 3 1/2' high density diskette drive, 640 KB of memory, 2 MB hard disk storage (for program without data entered), VGA or SVGA graphics card and monitor, mouse and HP LaserJet IIP or better printer.

The required software to run the program is MS-DOS 5.0 or later version and Microsoft Windows™.

The desired program attributes for the project were:

- Graphical User Interface (e.g., system flow diagram illustration)
- User friendly, simple to input and retrieve data
- Compliance with availability monitoring recommendations of Regulatory Guide 1.160
- Flexible, able to be customized to users needs and system configurations
- Data base records available for sorting, viewing and editing
- Output for trending and graphics
- Data base compatible with external programs
- Compatibility with networks
- Modularized design to enable easy upgrades and to import or calculate reliability data, risk data, importance measure, and cost measure.
- Design to enable automated collection of pertinent data including equipment outages

- Minimize impact/changes to existing plant programs, procedures and processes
- Design per appropriate Quality Control standards
- Cost effective

Based on the above required program attributes and software/hardware requirements, it was determined at that time that the source code software that best fit the program design and was most efficient for the software developer, was to use a program called Toolbook™ (by Asymetrix Corporation).

The criteria for tracking (inputting) system and component availability data is based, for example, on the out-of-service periods for maintenance and testing of the component or system. Specifically modeled into the program are allowed unavailabilities for: corrective maintenance, preventive maintenance, system configuration, testing, inspection, and predictive maintenance. Availability tracking data can also be based on additional criteria such as direct and/or indirect support system inoperabilities or as defined by the end user. Figure 2 provides an illustration of a sample equipment out-of-service input form that would typically be used by the system engineer in inputting, monitoring and hypothesizing the impacts of equipment unavailabilities.

The program can track all inputted out-of-service intervals and out-of-service causes (including percent reactor derating) for the selected components. The program also then provides user-specified color-coded administrative and goal limits for components, subsystems and systems. These color-indicated goals are then overlaid on the system flow diagram screen on each component, subsystem and system. On screen, these components, subsystems and systems then change color as they become less available according to their inputted unavailability data, calculated results, and relation to the pre-established availability goals. The availability calculation is then based the a user-specified interval.

## **PROGRAM IMPLEMENTATION**

This program has many end uses pertaining to the monitoring of availability data including Maintenance Rule implementation. This program can be utilized for trending of performance criteria pursuant to implementation of 10 CFR 50.65, "Monitoring the Effectiveness of Maintenance at Nuclear Power Plants". This "Maintenance Rule" requires utilities to determine a performance criteria for systems, structures, and components, (SSC's) within the scope of the rule.

One criterion chosen by many utilities for determining SSC performance is system and/or component unavailability. By modeling the critical components of a system and monitoring the time those components are out of service (or unavailable), an indicator of the time a system is capable of performing its function is established. The function modeled may be of safety significance or electrical generation capacity factor as it is affected by the availability of key equipment.

By comparing the time a component is capable of performing its function (availability), to established goals, where such goals may be based on risk or electrical generation capacity, the decision on how to allocate corrective and preventive maintenance resources can be enhanced. As a result of performing these goal comparisons, overall plant risk will be minimized while maintaining maximum electrical generation capacity.

This program can be easily applied to Maintenance Rule requirements. NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants", provides that monitoring the availability parameter for systems and trains with respect to their goals will provide a basis on where improvements are needed and also confirm where corrective actions have been effective. This NUMARC Guideline furthermore recommends that individual train performance (such as its availability performance) be compared to the other train.

The modeled system is displayed with symbols commonly used for components such as pumps, valves, etc. Availabilities for individual components, groups of components, and the total system are automatically computed and displayed. By the use of pull down menus, the user can easily transfer between data entry screens and the system display screen. In addition, by inputting hypothetical data and transferring to the system display, the effect on system availability of upcoming planned equipment outages can be assessed by observing the resultant calculated availability values and goal color changes indicated on the system flow diagram screen. This type of analysis can be utilized in adjusting the preventive maintenance, inspection, and testing activities to achieve system availability goals.

Although the responsibility for maintaining system specific data may rest with one person, the desire to produce reports or examine current availability data may involve many different users at a site. By utilizing an existing computer network, this program can be adapted for such use. While providing specific users with input authority to ensure data integrity, other users, such as maintenance planners, work schedulers, or operators can view the data and produce desired reports.

## CONCLUSION

As described in this paper, this software program is designed for monitoring the availability of components and systems and can perform this function well. The program can also be customized to each plant's specific monitoring needs. Ultimately, this program is capable of providing valuable information that can be utilized for improving plant performance and reducing overall plant operating costs.



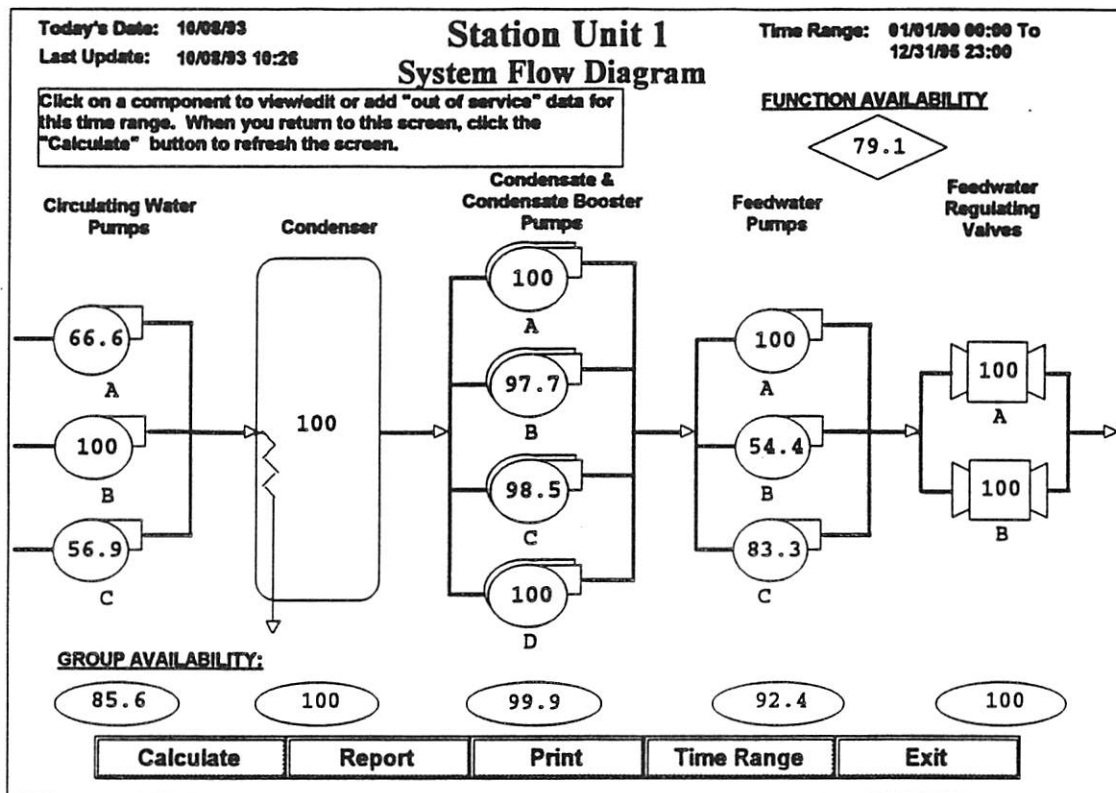


Figure 1. The System Flow Diagram screen is the main screen from which the user inputs and retrieves availability data. This screen displays the calculated resultant availability values for the individual components, subsystems (groups) and the entire system (function). A component is selected (point and click), then the program takes the user to the input screen to enter or view/edit out-of-service data.

Today's Date: 10/11/93 13:51  
Entry Date: 10/11/93 13:51

## Station Unit 1 Equipment Out of Service Form

Time Range: 01/01/90 00:00 To 12/31/94 23:00

Group: Condensate & Condensate Booster Pumps  
Component ID: Pump A - CCBA

Date/Time(Out of Service): 05/04/92 08:00  
Date/Time(Back in Service): 06/04/92 17:00  
Cumulative Out of Service Hours: 753  
Actual / Hypothetical: ☐ A ☒ H  
Reason for Out of Service\*: ☒ CM ☐ PM ☐ TS ☐ SY ☐ IN ☐ PD  
Reactor Derated: ☐ Y ☒ N Total Derated Percent:   
Comments: Shaft Failure

\* CM:Corrective Maintenance, PM:Preventive Maintenance, SY:System Configuration, TS:Testing, IN:Inspection, PD:Predictive Maintenance

Figure 2. The Equipment Out-of-Service screen allows the user to enter, view or edit out-of-service data for the selected component.

**089 Seismic Risk Analysis**  
***Chair: D.A. Moore, Primatech***

**The Experimental Breeder Reactor II Seismic Probabilistic Risk Assessment**  
***J. Roglans, D.J. Hill (ANL)***

**Seismic Risk Management Using Earthquake Injury Epidemiology**  
***P.J. Amico, T.A. Haley, S.J. Krill (SAIC)***

## **THE EXPERIMENTAL BREEDER REACTOR II SEISMIC PROBABILISTIC RISK ASSESSMENT**

Jordi Roglans, David J. Hill

Reactor Analysis Division  
Argonne National Laboratory  
Argonne, IL 60439

### **INTRODUCTION**

The Experimental Breeder Reactor II (EBR-II) is a US Department of Energy (DOE) Category A research reactor located at Argonne National Laboratory (ANL)-West in Idaho. EBR-II is a 62.5 MW-thermal Liquid Metal Reactor (LMR) that started operation in 1964 and it is currently being used as a testbed in the Integral Fast Reactor (IFR) Program. ANL has completed a Level 1 Probabilistic Risk Assessment (PRA) for EBR-II. The Level 1 PRA for internal events and most external events was completed in June 1991 [1]. The seismic PRA for EBR-II has recently been completed.

The EBR-II reactor building contains the reactor, the primary system, and the decay heat removal systems. The reactor vessel, which contains the core, and the primary system, consisting of two primary pumps and an intermediate heat exchanger, are immersed in the sodium-filled primary tank, which is suspended by six hangers from a beam support structure. Three systems or functions in EBR-II were identified as the most significant from the standpoint of risk of seismic-induced fuel damage: (1) the reactor shutdown system, (2) the structural integrity of the passive decay heat removal systems, and (3) the integrity of major structures, like the primary tank containing the reactor that could threaten both the reactivity control and decay heat removal functions. As part of the seismic PRA, efforts were concentrated in studying these three functions or systems. The passive safety response of EBR-II reactor - both passive reactivity shutdown and passive decay heat removal, demonstrated in a series of tests in 1986 [2] - was explicitly accounted for in the seismic PRA as it had been included in the internal events assessment.

### **PLANT SEISMIC RESPONSE MODELING**

Using the logic models developed for the internal events PRA, a seismic event tree was generated (Fig. 1). The event tree contains the relevant systems or structures that must perform their functions during a seismic event, namely, preservation of the structural integrity of the primary systems, the response of the shutdown system, and the continued

04-APR-93

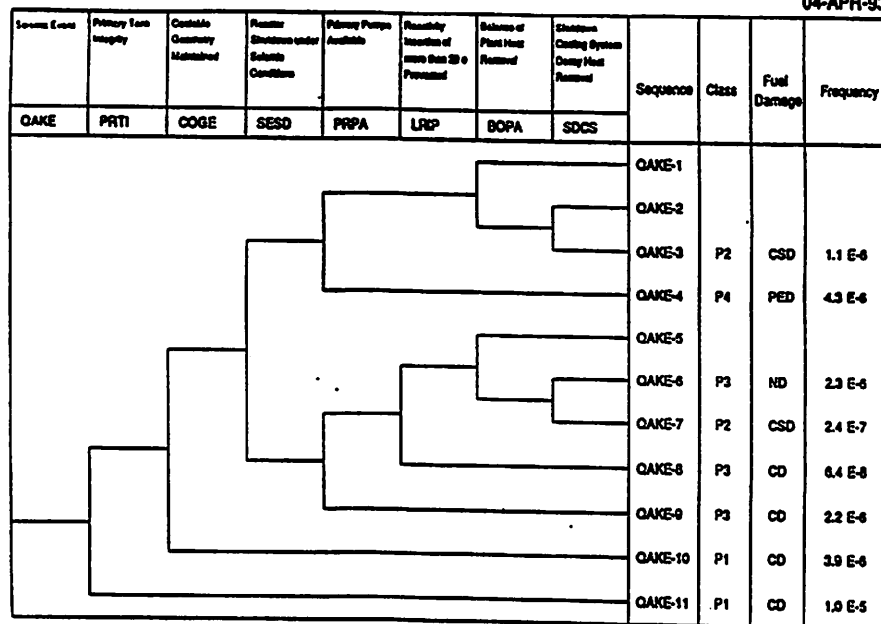


Figure 1. Seismic Event Trees

availability of adequate core cooling.

Fault trees were therefore developed to model both system and structural failures. The fault trees contain both seismic and non-seismic failures of the individual components involved in the system, as well as possible human errors. The probabilities for the non-seismic failures and human errors were obtained from the internal events analysis. For the seismic-induced failures, walkdowns were conducted to identify component vulnerabilities. Based on the observations of the walkdowns and the knowledge gained from the internal events models, the components requiring detailed seismic capacity analysis were selected. Components of secondary importance were assigned screening fragility values, based on the methodology of the Seismic Margins program [3].

For the components selected for detailed analysis, a two-step process was followed, consisting of a deterministic analysis performed at ANL and a fragility estimation provided by R. Kennedy. Following the usual methodology, fragilities were expressed with three parameters: median fragility, randomness, and uncertainty, and the chosen ground motion parameter, in agreement with the hazard curves, was the peak ground acceleration (PGA).

## SEISMIC ANALYSIS OF COMPONENTS AND STRUCTURES

### Major Structures

The most important structure analyzed was the primary tank. The primary tank in EBR-II is suspended from a beam structure by six hangers resting on a set of rollers to allow for thermal expansion. The first failure mode analyzed was the possibility of displacing rollers from under the hangers, resulting in a drop of several inches of the primary tank. Inspection and analysis showed that sufficient clearance would not exist for the rollers to withdraw from their position. The next failure mode analyzed was the weak

axis bending failure of the tank hangers. This failure was the limiting failure for the primary tank, with an estimated median fragility of 0.7g (Fig. 2).

Other structural failures studied included the fuel storage basket inside the primary tank, the reactor building, and the oscillation of the bottom core support plate. The storage basket and the reactor building were found to be rugged, and their estimated fragility well above that of the primary tank failure.

The vibration of the core support plate was analyzed for its effect on reactivity. A reactivity insertion would occur if the core moved with respect to the control rods, which are supported from the top of the primary tank. Although the reactivity insertion would be oscillatory, it was assumed that a net positive reactivity insertion would occur. Due to the EBR-II feedbacks, reactivity insertion events of less than 0.2  $\beta$  do not lead to fuel damage. The ground acceleration capable of inserting 0.2  $\beta$  was estimated at 0.4g.

### Reactor Shutdown System

Protection against the effects of earthquakes has been built into the Reactor Shutdown system at EBR-II by inclusion of a set of three seismic detectors. These detectors are set at a nominal value of 0.005g, with the Technical Specification Limit of 0.01g. The failure of the detection system was included in the fault tree model, along with the mechanical failure to scram. Although the shutdown system includes two mechanically independent subsystems (control and safety rods), only the control rods were accounted for in estimating the scram reliability under seismic conditions, given the susceptibility of the safety rods to slight misalignments caused by seismic ground motions.

Nine control rods are driven from the top of the primary tank, with control rod drivelines that penetrate the primary tank and reach the core through guide tubes in the reactor vessel cover. The rod drive mechanism is located above the cover of the primary tank. A detailed structural model was developed to predict the scram times under different peak ground accelerations [4]. The control rods are driven by gravity but an air assist piston is also provided. Even when ignoring the downforce generated by the air pistons, the control rod scram times were not found to increase significantly with the ground acceleration. It was estimated that the High Confidence of Low Probability (HCLPF) to scram in approximately the Technical Specification limit of 0.45 sec was 0.4g.

Another mechanical failure that could impair the scram function is the failure of the reactor vessel cover. The reactor vessel cover is lifted during fuel transfer operations. During reactor operation, the cover is secured by three cover locks. Seismic conditions can induce the movement of the vessel cover or the failure of one of the locks. If the cover is not securely locked against the vessel, it can tilt and jam the control rod drives. The fragility estimate for the vessel cover tilting indicates a median value around 1.2g.

A key issue for the reliability of the shutdown system is the existence of the very sensitive seismic detection system and trip. Taking into consideration the delay between the seismic P-waves and the more damaging S-waves, the use of the low-setpoint seismic trip will ensure that the scram takes place under very moderate seismic conditions.

### Primary Pumps System

Under seismic conditions, a loss of electrical power is expected, and therefore the EBR-II primary pumps will be deenergized. For protected (successful scram) sequences, operation of the primary pumps is not necessary to prevent fuel damage. The coastdown of the primary pumps is important to ensure a smooth transition to natural circulation. For unprotected (unsuccessful scram) sequences, a failure of the primary pump system results in a Loss of Flow (LOF) transient that leads to some degree of fuel damage, depending on the duration of the pump coastdown. The two primary pumps in EBR-II are driven by a

motor-generator set coupled by a clutch.

The internal events PRA showed that unprotected double pump LOFs lead to different degrees of fuel damage depending on the nature of the pump trip. There are three possible pump coastdowns in EBR-II, depending on the type of trip, i.e., motor, clutch or generator trip. For protected sequences, none of the trips led to fuel damage. Under seismic conditions, however, the coastdowns become faster. This degradation occurs because the primary pumps have a hydrostatic bearing that is less stable when horizontal accelerations cause the shaft to impact against the journal. The shaft impacts accelerate the coastdown. The degradation of the hydrostatic bearing was modelled, and the altered coastdowns were analyzed for different ground motion levels. The results indicate that severe core damage (CD) would occur for unprotected LOF transients at all ground accelerations for clutch and generator trips, and above 0.5g for motor trips. For protected double pump LOF transients, possible experimental fuel damage (PED) would occur at accelerations above 0.8g for generator trips, while motor or clutch trips would not result in any fuel damage for ground accelerations up to 1.5g.

Although the remaining components in the primary pumps system were also modelled in the fault tree, the degradation of the hydrostatic bearing was the dominant event, since the coastdown time becomes a key parameter given that the double pump LOF is highly probable even at low accelerations because of loss of electrical power supplies.

### Shutdown Cooling System

The two EBR-II shutdown coolers are passive systems. Liquid NaK naturally circulates through the shutdown cooling piping and to the shutdown cooler box located outside the reactor building. The shutdown cooler box is a natural draft air heat exchanger with chimney. When decay heat removal must be initiated, two dampers are required to open in the shutdown cooler box allowing air to be drawn over the heat exchanger and increasing the heat rejection. The dampers are fail-safe and easily opened manually and therefore readily recoverable. Total failure of the decay heat removal function leads to a gradual heat up of the primary tank that has been defined as core structural damage (CSD) in the internal events PRA [1].

The different structural components of the system were analyzed for seismic induced failures. Detailed analysis showed that only the structural failures of the cooler box or piping have any significant contribution to the unavailability of the decay heat removal system after a seismic event. The most fragile component was found to be the cooler box, with an estimated median fragility of about 1.5g.

### Other Systems

Other system failures were analyzed for their relevance in the accident sequences. For example, the argon cover gas systems were studied for their potential to pressurize the primary tank. Pressurization of the tank could occur if the pressure regulation system failed and the pressure release system were blocked due to seismic induced failures.

Failure of the secondary piping was included in the models because of its potential to start liquid metal fires that could affect the decay heat removal functions. Unavailability of the secondary by itself does not contribute to the risk of fuel damage.

The steam generators are not in the reactor building, and thus steam generator failures cannot directly affect the primary systems. Unavailability of the heat sink is not a significant contribution to risk in EBR-II. Steam generator failures, however, are included in the seismic PRA for their potential impact on the primary system. A sodium-steam reaction can create a pressure wave that could propagate to the intermediate heat exchanger (IHX). If the pressure wave failed the IHX, natural circulation through the core

might be impaired. The use of duplex tubes in the steam generators and the additional failures required to propagate a sufficiently large pressure wave to the IHX make this failure mechanism only a moderate contributor to the loss of the core coolable geometry.

### Hazard Curves

Site-specific hazard curves were developed for EBR-II by Risk Engineering, Inc. The hazard curves were developed from USGS data for the site (anchor point), from attenuation models, and from the results obtained in an EPRI study for 57 other plants (uncertainty in the curves). The resulting hazard curves show a significant spread, in particular at high ground accelerations. The curves were extended to a PGA of 1.5g. The concept of a maximum credible earthquake that had been used in some of the early seismic PRAs was not applied in the EBR-II site hazard curves.

## RESULTS AND DISCUSSION

Using the logic models developed, the plant-level fragility was estimated for each seismic accident sequence, for each bin (fuel damage class), and for the total fuel damage due to seismic events. The plant-level fragilities were then convoluted with the hazard curves developed for the EBR-II site to estimate the annual frequency of plant failure.

The overall results of the seismic PRA indicate a 90% range for the expected annual probability of fuel damage (minor or severe) between  $2.5 \times 10^{-7}$  and  $10^{-4} \text{ yr}^{-1}$ , with an estimated mean value of  $1.7 \times 10^{-5} \text{ yr}^{-1}$  (median estimate of  $3.9 \times 10^{-6}$ ).

The dominant seismic failure was found to be that of the primary tank hangers. Indeed, the primary tank failure dominates the seismic risk profile, since it can also affect the reactor shutdown and the shutdown cooling systems. Another significant contribution to the seismic risk is due to the altered primary pump coastdowns caused by the degradation of the pumps hydrostatic bearings.

The reactor shutdown system and the shutdown cooling system were found to be very rugged. For the reactor shutdown system, a very sensitive seismic detection system and a control rod driveline of high seismic capacity combine in a scram reliability that is not significantly degraded under seismic conditions.

The estimated seismic risk of fuel damage fares well when compared with that of commercial or other Class A DOE reactors, although a direct comparison is not truly appropriate because of the different site seismicity. Comparing the EBR-II seismic risk with that due to internal events [1], the seismic risk is an order of magnitude higher than the internal events contribution and a factor of 5 higher than the risk due to fires.

This comparatively high damage frequency is largely driven by the uncertainty in the hazard curves. With the EBR-II hazard curves, it would require a plant with an overall median fragility of 1.3g to make the estimated damage frequency comparable with the internal events. Examining the results in terms of plant-level fragility rather than annual failure frequency, provides a better insight into the seismic capacity and response of EBR-II, showing a seismically rugged plant. The overall plant-level fragility (Fig. 3) shows a median capacity approximately at a PGA of 0.55g, with a HCLPF of about 0.3g, which is around the current seismic design criteria for modern facilities.

Most of the fuel damage that results from the seismic sequences is of the extensive core damage type (CD), which is the type of damage expected after the failure of the primary tank hangers. The contribution of the tank failure to the total fragility can be seen by comparing Figures 2 and 3. This contrasts with the type of predominant damage in the internal events, which tended to be less extensive.

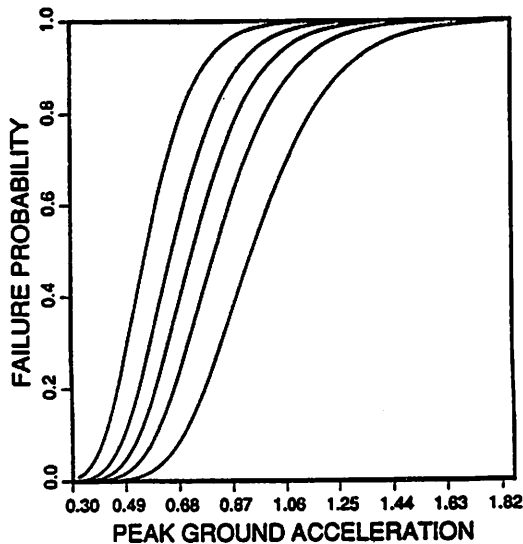


Figure 2. Primary Tank Hanger Failure Fragility Curves

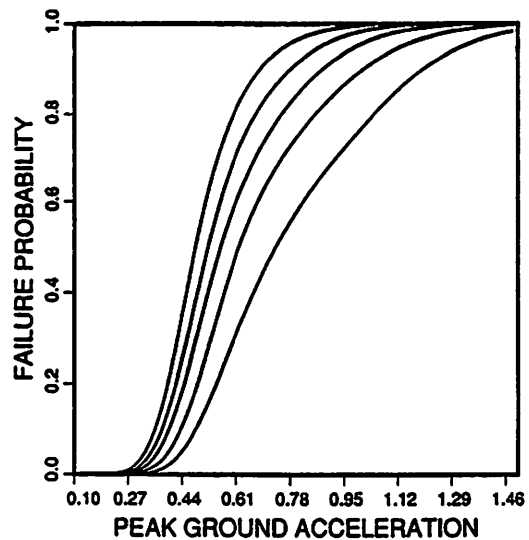


Figure 3. Plant-Level Fragility Curves for Fuel Damage

No structural or procedural improvements at EBR-II have been identified that could significantly reduce the seismic risk. Modest gains can be made by improving anchorage and support systems.

The results of the EBR-II seismic PRA indicate that a LMR reactor based on the EBR-II design can be built with a high seismic capacity and be structurally simple. Key factors in achieving a design with a high degree of protection against fuel damage are the reactivity feedback characteristics, the reliability of the shutdown system, and the passive decay heat removal systems. Lack of dependence on human actions and power supplies enhances the reliability of the safety systems.

## REFERENCES

1. D.J. Hill, W.A. Ragland, J. Roglans, EBR-II Probabilistic Risk Assessment: Summary and Insights, *in: Proceedings of the International Topical Meeting on Probabilistic Safety Assessment*, Clearwater Beach, FL, January 1993, G. Apostolakis, ed., American Nuclear Society, La Grange Park, IL (1993).
2. H.P. Planchon, et al., Implications of the EBR-II Inherent Safety Demonstration Test, *Nucl. Engrg. Des.* 101:75 (1987).
3. Electric Power Research Institute, "A Methodology for Assessment of Nuclear Power Plant Seismic Margin", NP-6041, EPRI, Palo Alto, CA, 1988.
4. J. Roglans, C.Y. Wang, D.J. Hill, Scram Reliability under Seismic Conditions at the Experimental Breeder Reactor II, *in: Proceedings of the 12th International Conference on Structural Mechanics in Reactor Technology*, Kussmaul, ed., Stuttgart, Germany (1993).



## **SEISMIC RISK MANAGEMENT USING EARTHQUAKE INJURY EPIDEMIOLOGY**

Paul J. Amico, Timothy A. Haley, and Stephen J. Krill, Jr.

Science Applications International Corporation  
20201 Century Boulevard  
Germantown, Maryland 20874

### **INTRODUCTION**

The issue of public health and safety consequences following an earthquake around a major nuclear facility has traditionally concentrated solely on those potential fatalities resulting from the radiological release. However, in developing a sound risk management philosophy for handling the seismic component, it is essential to consider the public health and safety consequences directly from the earthquake itself. In this paper, the attempt has been made to compare the direct public consequences due to building damage from a major earthquake in the Denver area with the consequences of a seismically-induced radiological release from a nearby nuclear facility (Building 707 at Rocky Flats). This comparison makes use of a relatively new field of study, earthquake injury epidemiology, which correlates earthquake intensity to building damage using field data from past earthquakes to formulate models of potential public health and safety consequences.

### **GENERAL APPROACH**

In developing the approach for this study, it was obligatory to remember that the goal (from a risk management perspective) was to answer whether the number of casualties from the seismic event itself greatly exceeded those from the radiological release. Consequently, "accurate" casualty estimates were not required as long as the bounding analysis sufficiently justified the goal. In support of this, the assumptions were made to maximize (i.e., established an upper bound for) the estimate of radiological casualties and to minimize (i.e., established a lower bound for) the seismically-induced casualties. This approach served to minimize the degree to which the estimate of seismic-induced casualties might exceed the radiological casualties.

The maximization of radiological casualties was accomplished by the accident analysis in the Building 707 Facility Safety Analysis Report (FSAR).<sup>1</sup> For example, in typical FSAR fashion, building failure was assumed to occur when the calculated stress levels exceeded conservatively established structural limits, in a configuration that maximizes: (a) the amount of radiological material available for release, (b) the availability of release paths, and (c) the fraction of radiological material released in respirable form (based on experimental data). The FSAR assumption of the structural stress levels for building failure also served to minimize in part the estimate of seismically-induced casualties because it resulted in the use of a lower intensity earthquake for estimating those casualties.

The remaining aspects of developing this estimate were a combination of other such assumptions combined with best estimate values where appropriate, justifiable, and necessary to support the conclusions. Further discussion of this part of the approach, which represents the risk management innovation proposed by this paper, is the subject of the ensuing sections.

### **EARTHQUAKE STRENGTH RESULTING IN BUILDING COLLAPSE**

The first step in the analysis was to define the earthquake strength at Rocky Flats that results in substantial collapse of Building 707 with a resultant radiological release. According to the FSAR, Building 707 has a seismic capacity resulting in total damage at 0.26g peak ground acceleration,<sup>1</sup> (where total damage was defined as approximately 50% of the wall panels being dislodged). A review of the FSAR concluded that the 0.26g estimate was too high for total damage to Building 707, so a new seismic analysis was performed.<sup>2</sup> This updated analysis predicted that total damage would occur at greater than 0.21g and less than 0.26g. For the purpose of this study, a 0.24g peak ground acceleration was assumed as the earthquake resulting in total damage of Building 707.<sup>a</sup>

In order to assess the public consequences from this earthquake, the unit of measure of the earthquake was converted from acceleration to approximate intensity, because the available health and safety studies on earthquakes effects put the damage assessment in this unit. For this study, the Modified Mercalli Intensity (MMI) scale was used. The conversion was accomplished using seismic characterization data provided in NUREG/CR-5250, which assembled several correlations relating site intensity and site acceleration.<sup>3</sup> The results of the correlation ranged from a calculated intensity of 7.4<sup>b</sup>, essentially a borderline MMI VII/VIII earthquake, to an intensity of 8.7, which more closely paralleled a MMI IX earthquake. The other correlations were all approximately MMI VIII. From these results, it was reasonable to assume that an MMI VIII earthquake at Rocky Flats could be used to represent the 0.24g earthquake that could cause total damage of Building 707.

---

<sup>a</sup> The analysis was also performed for 0.26g and 0.21g. The results were not particularly sensitive to these small changes in acceleration, thus making the assumption of 0.24g versus using 0.26g or 0.21g for total building damage insignificant to the conclusions.

<sup>b</sup> The correlation calculations result in a numerical value for intensity, which is then converted to the traditional Roman numeral designation by assuming that 6.5 to 7.5 is MMI VII, 7.5 to 8.5 is MMI VIII, etcetera.

The second step in the analysis was to determine the intensity at Denver, Boulder, and Golden in order to assess the impact of the earthquake on these nearby population centers. This was done by reviewing historical data on those earthquakes affecting the area that were at least Richter magnitude 5 or MMI VI.

As shown in Table 1, eight earthquakes were identified with either a Richter magnitude equal to or greater than 5 or an intensity equal to or greater than MMI VI affecting Rocky Flats and the three population centers<sup>4</sup>. From this evidence, it was concluded that the intensity of an earthquake affecting Rocky Flats would be essentially the same at Denver, Boulder, and Golden, making it reasonable to assume that the postulated MMI VIII earthquake that collapses Building 707 would result in an equal intensity of MMI VIII at the three population centers. This was a conservative assumption because cases where the acceleration at the population centers was greater than Rocky Flats (4 cases at Denver, 2 cases at Boulder, and 4 cases at Golden) were ignored, which would have increased the level of predicted damage at these centers. By comparison, in only two cases (one at Boulder and one at Denver) were the intensities less than Rocky Flats.

Table 1. Local Intensities Observed for Selected Earthquakes.

<u>Earthquake</u>	<u>Observed Intensity At:</u>			
	<u>Rocky Flats</u>	<u>Denver</u>	<u>Boulder</u>	<u>Golden</u>
Nov. 8, 1882	VI	VI	VI	V
Dec. 4, 1962	V	V	V	V
Dec. 5, 1962	IV	V	IV	V
Jan. 5, 1966	NF <sup>*</sup>	V	NF <sup>*</sup>	IV
Apr. 10, 1967	V	V	VI	VI
Apr. 27, 1967	<V	V	<V	<V
Aug. 9, 1967	VI	VI	V	VI
Nov. 27, 1967	V	VI	VI	VI

<sup>\*</sup>Not Felt

## BUILDING DAMAGE AND CASUALTY ESTIMATION

Using the earthquake damage database at Cambridge University, Coburn developed collapse probabilities for different building types in shallow-depth, near-field earthquakes.<sup>5</sup> The probabilities were for those buildings that were expected to be severely damaged (i.e., total collapse) given certain intensity levels. The correlations in this model also allowed Coburn to develop casualty rates for various building types based upon the percent of building stock severely damaged, which are expressed in terms of the percent of people present in those buildings who are killed. In a similar study, Tiedemann developed estimates as a function of MMI for casualties from all

types of building damage, including partial collapse, non-structural failure, and falling objects.<sup>6</sup> The results of these two studies formed the basis for the casualty estimates for the MMI VIII earthquake at Rocky Flats.

Restrictions on space do not allow for the detailed presentation of the results of each step in this analysis, so only the final casualty rates are presented. In determining an overall casualty rate for the three population centers around Rocky Flats, the foundation rested upon the distribution of the population amongst the various building types. Table 2 presents a range of casualties for each one percent of the population resident in each particular building type at the time of the earthquake. Using the 1988 U.S. Census Bureau estimate of 1,858,000 as the population of the Denver-Boulder-Longmount County area, each one percent of the population would be equivalent to 18,580 persons. The fraction of people who would be killed given their presence in a particular building type was based on earthquake injury epidemiology studies of various earthquakes. Except where noted, the estimates were based on the consolidated study by Tiedemann.<sup>6</sup>

Since the purpose of this study was not necessarily to calculate an estimate of casualties but rather to determine the relative contribution of the casualties induced directly by the earthquake versus those caused by the seismically-induced radiological release from Building 707, the approach taken was to consider some simple scenarios of population distribution amongst the various building types. This established the order-of-magnitude range of potential casualties from the earthquake and allowed possible insights to be developed.

**Table 2. Deaths Per One Percent of Population By Building Type.**

Building Type	Deaths Per One Percent of Denver Area Population Located In Each Building Type at the Time of MMI VII Earthquake
Unreinforced Masonry Adobe/Rubble Brick	4,600 to 11,000 900 to 3,700
Wood Frame	<200 (from Coburn)
Reinforced Concrete 0.025g Design 0.06g Design	50 to 750 7 to 50
Steel Frame	7 to 750 (est.)

## ANALYSIS AND RESULTS<sup>c</sup>

As was shown above, a definite correlation existed between building damage and occupant casualties. Wide-scale building destruction, especially with regard to total collapse, generally results in an enormous number of casualties. The damage models, which were based on the consequences of recent major earthquakes, predict

<sup>c</sup> The analysis and results presented in this section and the resulting conclusions discussed in the following section are those of the authors, based on an integrated assessment and application of all the available information documented in the references. They do not necessarily coincide with the individual opinions of the authors of those references.

that a MMI VIII earthquake would destroy a significant number of unreinforced masonry structures and would cause modest damage to other building types in the affected region.

Keeping in mind that the purpose of this study was to compare potential radiological versus seismic-induced casualties during an earthquake (as opposed to getting as "accurate" assessment of either), a few sensitivity calculations were performed to see what can be learned. As an initial estimate, every individual was assumed to be located in a reinforced concrete (RC) building<sup>d</sup> designed for seismic loads of 0.06g, a clearly optimistic assumption given that the population of such buildings in the affected area was likely to be only a subset of the overall population of buildings and certainly many people could be expected to reside in other building types. In addition, the casualties were assumed to be at the lower end of the predicted range of the Tiedemann model (Table 2). This was a bounding assumption because the 0.06g buildings represent the lowest casualty rate from the earthquake. This case would maximize the relative contribution of the radiological release from Building 707 to total casualties. Even with these assumptions, over 700 fatalities were projected to occur in the Denver area, (7 deaths per each one percent of the population). If a more central estimate of the death rate for 0.06g RC buildings was taken, the result would be on the order of 2,500 deaths (25 deaths per one percent of population). Next, the effect of some percentage of the population being located in building types that are more susceptible to casualties was considered. For every one percent of the population located in 0.025g RC buildings instead of 0.06g RC buildings, there would be an increase in casualties on the order of 400. Likewise, for every one percent of the population located in brick or adobe structures instead of 0.06g RC, there would be an increase in casualties of over 2000 (for brick) and over 7,000 (for adobe). Thus, the results indicated that the casualties would almost certainly be in the hundreds and could easily range into the thousands.

How did this compare with casualties from the seismically-induced radiological release from Building 707? As previously stated, the FSAR Review Team<sup>2</sup> performed a bounding assessment for a number of severe seismically-induced radiological releases. Based on the risk numbers and release frequencies given, the greatest number of off-site casualties (given the maximum release has occurred) was about 4 latent cancer fatalities. As compared to the casualties discussed above, this was two orders of magnitude lower than the conservative lower bound estimate of direct seismically-induced casualties.

## CONCLUSIONS

The difference in the casualties from the radiological release versus those from the earthquake itself was quite dramatic. Even given the uncertainties involved and the fact that no detailed assessment of the actual building stock or the distribution of the populace within that stock was performed, it was clear that the greater Denver area could expect hundreds of fatalities, and more likely thousands, from building damage following a MMI VIII earthquake at Rocky Flats. This compared with less than ten fatalities from radiological release from the concurrent collapse of Building

---

<sup>d</sup> Certainly some individuals would be out of doors, but they are not immune from death (e.g., falling objects). In fact, Coburn concludes<sup>3</sup> that consideration of other causes of death following earthquake (e.g., fires, landslides, etc.) in addition to building collapse adds another one-third to the casualty estimate (based on earthquakes over the period 1950-1989).

707. It was considered extremely unlikely that the casualty estimates could be off by the orders of magnitude required to make the earthquake and radiological casualties comparable. Thus, the conclusion is clear: the likely global effect of the seismic event directly on the affected population is large when compared to the rather narrow effect of an associated radiological release from Building 707 induced by the earthquake. From a risk management perspective, neither shutting down nor performing further seismic upgrades on that building would have any measurable or meaningful effect on the risk to the public from large seismic events. This would be true until substantial improvement was made to the capacity of the existing building stock, which constitutes the primary seismic risk to the public.

While this study addressed the specific issue of radiological risk versus earthquake risk in a specific situation, the type of study performed here could show similar results for a broad range of hazardous facilities. While the conclusion in this case was obvious, in certain instances the results may not be as clear, making it necessary to refine the assessment to address omissions in this study (e.g., building population, distribution demographics, lifeline survivability, etc.), which require a greater expenditure of effort.\* However, what this study confirmed was that such an analysis has a marked value if, as was shown here, seismic risk reduction efforts are being misdirected toward areas of negligible effectiveness.

## REFERENCES

1. Building 707 Final Safety Analysis Report, Rockwell International, North American Space Operations, Rocky Flats Plant, June 1987.
2. Rocky Flats Plant Building 707 FSAR Review, prepared by Stone & Webster Engineering Corporation for EG&G Rocky Flats, May 21, 1991.
3. D.L. Bernreuter, J.B. Savy, R.W. Mensing, J.C. Chen, Seismic Hazard Characterization of 69 Nuclear Plant Sites East of the Rocky Mountains, NUREG/CR-5250, January 1989.
4. R. M. Kirkham, W.P. Rogers, "Colorado Earthquake Data and Interpretation 1867 - 1985," Colorado Geological Survey Bulletin No. 46, Colorado Geological Survey, Department of Natural Resources, State of Colorado, Denver Colorado, 1985.
5. Coburn, A.W., A. Pomonis, and S. Sakali, "Assessing Strategies to Reduce Fatalities in Earthquakes," International Workshop on Earthquake Injury Epidemiology for Mitigation and Response, The Johns Hopkins University, Baltimore, MD, July 10-12, 1989.
6. Tiedemann, H., "Casualties as a Function of Building Quality and Earthquake Intensity," International Workshop on Earthquake Injury Epidemiology for Mitigation and Response, The Johns Hopkins University, Baltimore, MD, July 10-12, 1989.

---

\* For example, what would we have done if our lower bound seismic casualty estimate and the radiological casualty estimate had been about the same? The clear conclusion would be gone, and we would have had to evaluate some of the other parameters to determine if a case could be made that the lower bound estimate was overly optimistic given the real conditions that existed, such as the actual building population and design quality.

## **090 Risk Based Regulation (II)**

***Chair: G. Apostolakis, UCLA***

### **Regulatory Decision Making by Decision Analysis**

***J. Holmberg, U. Pulkkinen (Tech. Res. Ctr. Finland); L. Reiman, R. Virolainen  
(Finnish Ctr. for Radiat. & Nucl. Saf.)***

### **Application of Risk-Based Prioritization to QA Requirements**

***F.J. Rahn, W. Parkinson (EPRI); G.D. Bouchev (SAIC); M. Meisner (Entergy  
Operations)***

## REGULATORY DECISION MAKING BY DECISION ANALYSIS

Jan Holmberg,<sup>1</sup> Urho Pulkkinen,<sup>1</sup> Lasse Reiman,<sup>2</sup> Reino Virolainen<sup>2</sup>

<sup>1</sup>Technical Research Centre of Finland (VTT)  
Laboratory of Electrical and Automation Engineering  
P.O.Box 34, FIN-02151 Espoo, Finland

<sup>2</sup>Finnish Centre for Radiation and Nuclear Safety  
P.O.Box 268, FIN-00101 Helsinki, Finland

## INTRODUCTION

A regulatory decision making includes selections of methods to control power company's operating policy. An important decision making criteria for the regulatory decision maker is how well the selected control policy enhances safety culture. Decision analysis aims to model the subjective assessments of the decision maker and, thus, to help the decision maker to understand the considered problem.

Technical Research Centre of Finland (VTT) has studied with the Finnish Centre for Radiation and Nuclear Safety (STUK) the applicability of decision analysis to nuclear safety related problems at the regulatory body. Decision models and analysis have been presented to inspectors of STUK who deal with operational safety of nuclear power plants. The role of probabilistic safety assessment (PSA) in decision making was also discussed (Holmberg and Pulkkinen 1993).

Normally, the formulation of the contents of the regulatory requirements has several steps where three type of persons are involved: 1) decision maker, 2) referendary, who presents the subject to the decision maker, and 3) technical expert(s), who prepare(s) the subject to the referendary. In practice, the decision making process includes internal discussions and meetings as well as possibly some communication with the power company before the final decision is made.

In this study, inspectors from STUK exercised with two occurred and solved problems using decision analysis. The use of previously solved problems may bias the results of the decision analysis, but the inspectors also got feedback to the earlier decision making processes. The first case was related to a common cause failure phenomenon in solenoid valves controlling pneumatic valves important to safety of the plant. The latter problem was to evaluate design changes of external electric grid connections after a fire incident had revealed weaknesses in the separation of electric system. In both cases, the decision analysis



was carried out in several sessions in which decision makers, technical experts as well as experts of decision analysis participated. This paper presents the first case and discusses the applicability of the decision analysis on regulatory decision making.

## DECISION ANALYSIS

Decision analysis is a set of methods of systems analysis and operations research which are applied in supporting extensive decisions. The problem is decomposed into components, each of which is subjected to evaluation by the decision maker. The individual components are then recomposed to give overall insights and recommendations on the original problem (see e.g. Bunn 1984, French 1986).

The decision analysis is a co-operation between the decision maker, the decision analyst and the experts. The decision maker is a single person or a group of persons who have to solve a decision problem. The role of decision analyst is to familiarize the decision maker and the experts with the decision analytic method applied and to make sure that all necessary information is available. The experts give information about specific problems on the analysis. The main phases of the decision analytic process are: 1) the structuring of the problem, 2) the construction of the preference model, 3) sensitivity analyses.

During the structuring of the problem, the problem is characterized, and decision options as well as objectives are identified. The background material is collected and some additional analyses may have to be performed. Uncertain factors as well as dependences between the elements of the problem are identified. The structuring is the most valuable part of the analysis. In a multi-objective approach, the structuring should result in a decision table which has objectives or criteria as columns and decision options as rows. The elements of the decision table describe how the options fulfil various criteria.

The preference model is used to prioritize the decision options. The elements of a preference model are decision options  $a_1, \dots, a_n$ , and attributes  $x_1, \dots, x_m$  measuring the achievement of the objectives. A decision option  $a_i$  results certain level of achievement of objectives which is a point of the multi-attribute consequence space  $(x_1(a_i), \dots, x_m(a_i))$ . Consequences can be certain or uncertain. A preference model maps the points of the consequence space to numerical scores to be used in the comparison of the options. In a value function model, consequences are certain. Influence of the uncertainties on preferences can be modelled by utility functions (von Neumann and Morgenstern 1947).

A value function is a real-valued function expressing the preference over attributes (Fishburn 1964). Real-valued function  $v(x)$  satisfying the condition

$$\begin{aligned} v(x) > v(y) &\rightarrow x \succ y, \\ v(x) = v(y) &\rightarrow x \sim y, \end{aligned} \quad (1)$$

where  $x$  and  $y$  are compared elements of the consequence space, can be used to order the attribute values in a preference order. " $\succ$ " denotes strict preference and " $\sim$ " denotes indifference between the elements. Multi-attribute value functions are used to represent multi-objective decision making problems. Sometimes, it is easier to deal explicitly with multiple objectives because of the difficulties to convert them to pure monetary values. The computationally easiest form of the multi-attribute value function is the additive function

$$v(x_1, \dots, x_m) = k_1 v_1(x_1) + \dots + k_m v_m(x_m), \quad (2)$$

where  $k_i$ s are the weights of the single-attribute functions. A sufficient condition for an additive decomposition of the multi-attribute value function is mutual preferential independence of the attributes. Assuming that the conditions for an additive multi-attribute

function hold, the weights are assessed by making trade-offs between attributes. After that, the best option is found by maximizing the value function

In the sensitivity studies, the decision problem is examined by the decision model. The purpose is to find the sensitivity of the results with respect to input parameters.

## **EXERCISE CASE**

### **Problem description**

The exercise problem is related to detected delayed actuation of solenoid valves of the hydraulic reactor scram system at both units of the TVO (Teollisuuden Voima Oy) nuclear power plant in 1992. The cause for the deteriorated performance of the solenoid valves was unknown so that the phenomenon could be considered a common cause failure destructive detrimental for the safety of the plant. The starting point for the case was that the power company informed the regulatory body about the situation and proposed a strategy to solve or control the problem. The problem of the regulatory body was to judge whether to allow continued operation or to require more detailed investigations. In reality, the regulatory body required an inspection of failed valves of TVO II unit during the next weekend.

### **The course of decision analysis**

The decision analysis was carried out in several sessions in which decision makers, technical experts as well as experts of decision analysis participated. The purpose was to create one decision model reflecting opinion of all participants. The mutual acceptance and understanding in each phase of decision analysis were obtained in discussions without using any formal methods to guide the discussion. In the first session, decision analysis techniques were presented and the subject of the first case was defined. Before the second session, the representatives of the regulatory body were asked to identify decision options and criteria relevant to the case. During the following session, the options and criteria were defined more specifically, and a decision table (see Table 1) describing how the options meet the criteria was filled. Based on the decision table, a multi-attribute value function was constructed in the third session. The objectives achievements were measured by attributes and the weighing of the criteria was performed by asking trade-offs. The model was then manipulated by a spreadsheet application designed for additive multi-attribute value functions. In the fourth session the results of the analysis were presented and discussed. The second exercise was carried out in a similar fashion.

**Decision options.** Four decision options were identified shown in Table 1. The first option means that the power operation is continued and the test interval of the valves is shortened. In the meantime, the power company and the vendors of the plant as well as of the valves try to find out the cause of the phenomenon by other means but not by inspecting the deteriorated valves. In the second option, some of the deteriorated valves are inspected to identify the causes of the faults. It means that one of the units has to be shut down to ensure safe replacements of the valves. Power operation can be then continued, but the valves must be investigated immediately. The third option is the same as the second one except that investigations does not have to be done immediately. A time limit of one month is assumed. Due to time, the company can better schedule the shut down and investigations. In the fourth option, shut down of both units, the situation is considered so severe that power operation cannot be allowed till the investigations provide results. The contents of the investigations are assumed to be same as in the second and third options.

Table 1. Decision table of the case 1.

Criteria	Decision options			
	1. No extra investigations	2. Immediate investigations	3. Investigations within one month	4. Shut down of both units
Risk of external release	+1 %, half a year, two units	+1 %, one week, two units	+1 %, one month, two units	+0 %
Core damage risk	+1 %, half a year, two units	+1 %, one week, two units	+1 %, one month, two units	+0 %
Shut down risk	0 shut down	1 shut down immediately	1 shut down within a prescribed time, not necessarily an extra shut down	2 shut downs immediately
Identification of failure mechanism	depends on the effectiveness of tests	depends on the effectiveness of investigations and tests	same as option 2 but more time to plan the investigations	depends on the effectiveness of investigations
Safety culture	implies that solenoid valves are not important to safety, closest to the internal probab. guide	shows awareness of the importance of solenoid valves and hydraulic scram system	same as option 2, acknowledges the importance of careful preparations	in practice a nearly impossible option, in-consequently stringent
Economical losses	no losses	1 day production	1 day production, not necessarily extra losses	2x7 days production losses

**Decision criteria.** Six decision criteria corresponding rows in Table 1 were identified. The conditional probability of an external release in a core damage as well as the core damage frequency increase temporarily, and each decision option results in different periods of increased risk. The decision options cause various number of extra shut downs which increase temporarily the risk of core damage and a shut down is a thermal transient loading the components in the primary circuit. The options differ also in their ability to discover the cause of the failure mechanism. Safety culture includes that the decisions of the regulatory body should be consistent and support the development of safety culture in utility, too. The consistency can be assessed by comparing this problem to the treatment of other problems and to regulatory guides. A STUK guideline used for internal purposes states a maximal allowed core damage probability increase till the next scheduled plant shutdown. In this case, the risk increase was assessed to be so small that the power operation could be allowed till the next refuelling outage. During a shut down of one or two units, the electricity has to be produced by other power plants in Finland or it can be imported. Although the economical consequences do not directly concern the regulatory body, this criterion can be included in the model.

The decision model was a multi-attribute value function. The risk of external release was measured by days in operation with increased risk. Correspondingly, one day in the core damage risk attribute means one day of operation of a unit which has 1 % higher core damage frequency. The shut down criterion was measured by the number of anticipated extra shut downs. The ability to identify the failure mechanism was measured by a subjective scale. The interpretation of the scale can be derived from the trade-offs. The

safety culture was counted by how many days earlier the shut down of a unit is performed than the probabilistic guide would have allowed. The economical losses were measured by days lost of production per unit. Each single-attribute value function was assumed to be linear.

The weights of the criteria were asked by trade-offs. One shut down was used as a reference yardstick because it was easy to interpret. Besides, the risk of a shut down has been evaluated. Respective core damage probability increase is obtained, if the plant is operated 150 days with 1 % higher risk frequency. Other trade-offs were determined by asking equally preferred changes in attribute levels compared to one additional shut down. By this way, the ratio of the attribute weights were obtained.

## Results

Figure 1 presents a bar diagram of the results. The higher a bar is in the diagram, the more an attribute supports the decision option. In each attribute column, the decision option worst with respect to the attribute receives zero points. The last row represents final scores which are sums of attribute specific scores.

The decision options "Investigations within one month" and "Immediate investigations" are clearly the best options. They are very much alike, and the critical judgement is how much the identification methods improve if some time is allowed for the power company to prepare the investigations than to require the power company to start the investigations immediately. The option "No extra investigations" is weighed down by low scores from external release risk, core damage risk and identification criteria. The option "Shut down of both units" is the worst one because it is unfavorable with respect to production losses, identification of failure mechanism and shut down risks.

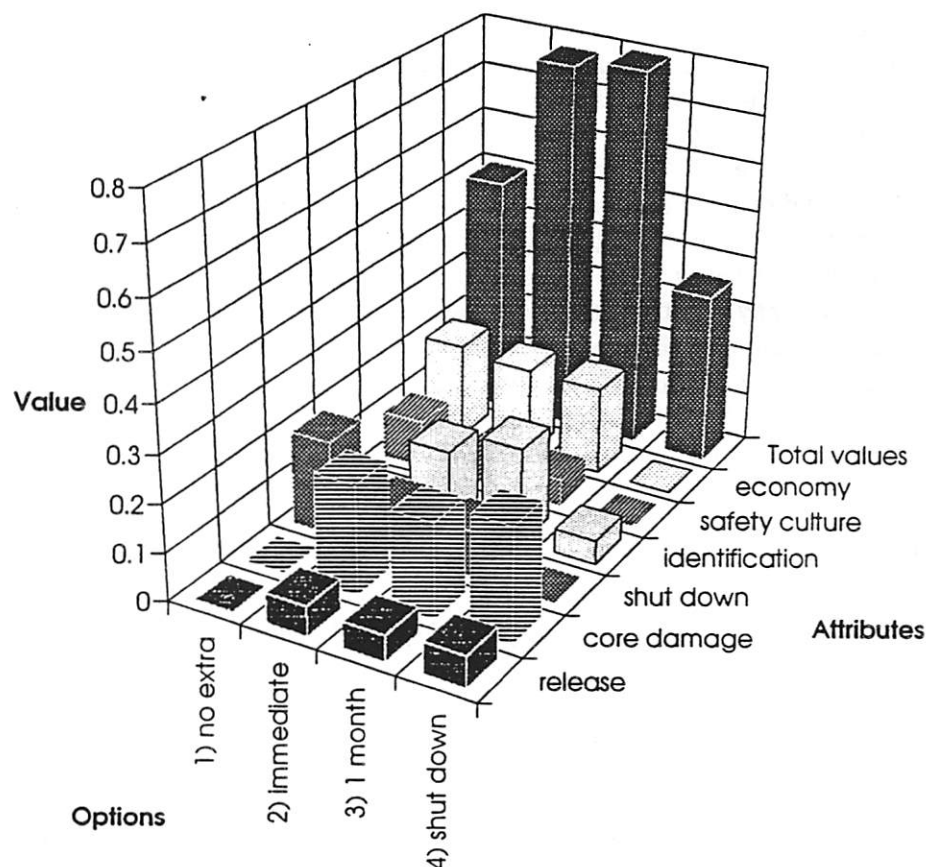


Figure 1. The final scores of the case 1.

## DISCUSSION

A communication process, alike decision analysis, helps to clarify and to verify the fundamentals of the authority work even if it is not applied as a regular approach. It improves the consistency in the decision making. An analysis is particularly needed when the problem is not clear and the best solution is not obvious. The problem of applying decision analysis in regulatory decision making is that the decision options usually include future options which are more effective than minimal solutions to the original problem. Additional reports or proposals can be required from the power company to solve the problem. Therefore the emphasis in the analysis turned out to be in the specification of objectives, after which it was meaningful to discuss decision options. The discussions during the structuring of the problem and the processing of the weights for multi-attribute function were, perhaps, the most educating part of the exercise. In that purpose, decision analysis can be an advancement to the normal practice, because it increases co-operation and information exchange.

To establish decision analysis as a standard approach in regulatory decision making, the authorities should enhance the discussion on the objectives of the regulatory decision making. During the course of such discussion, the legal or institutional position of the authority should be taken into account. A result of this kind of discussion could be a consistent hierarchy of objectives, which could be used as a basis for the identification of the decision attributes in every application of decision analysis.

The case studies were solved during several sessions, which were quite time-consuming. Much of time was used in identification of the attributes, i.e., in structuring of the problem. In practical work, the decision analysis should be made in shorter time. We expect that education of the inspectors and more experience on additional exercises or real cases will make the approach more effective.

The PSA results and analyses were essential parts of the decision models in the exercise cases. This is natural since one of the main objectives of regulatory decision making is to reduce risk. The combination of decision analytical thinking with the PSA is one way to well established and balanced risk based operational criteria or technical specifications. The PSA of level 1 is not, however, sufficient but the results from source terms and radioactive releases are needed. The uncertainties of PSA results can be, in principle, taking into account in the decision models.

Although the case studies revealed the potential of decision analysis in regulatory decisions, we may expect that this approach is even more suitable for the power companies. In their decisions the economical and risk aspects interact more clearly than in those of regulator. Furthermore, if both the authority and the power company apply decision analysis, then both sides understand more explicitly the objectives of each other, and, without doubt, the quality of decisions and discussions would be better.

## REFERENCES

- Bunn, D.W., 1984, "Applied Decision Analysis," McGraw-Hill, New York.
- Fishburn, P.C., 1964, "Decision and value theory," John Wiley, New York.
- French, S., 1986, "Decision Theory: An Introduction to the Mathematics of Rationality," John Wiley, New York.
- Holmberg, J., and Pulkkinen, U., 1993, Regulatory decision making by decision analysis, report RISKI(93)8, Technical Research Centre of Finland, Espoo.
- von Neumann, J., and Morgenstern, O., 1947, "Theory of Games and Economic Behaviour," 2nd ed. Princeton University Press, Princeton, New Jersey.

## **APPLICATION OF RISK-BASED PRIORITIZATION TO QA REQUIREMENTS**

**F. J. Rahn,<sup>1</sup> W. Parkinson and G. D. Bouchey,<sup>2</sup> and M. Meisner<sup>3</sup>**

<sup>1</sup>Electric Power Research Institute  
Palo Alto, California 94301

<sup>2</sup>Science Applications International Corporation  
Los Altos, California 94022

<sup>3</sup>Entergy Operations, Inc.  
Port Gibson, Mississippi 39150

### **INTRODUCTION**

U.S. nuclear plant operating and maintenance cost have averaged \$85.1/KWe-yr (1992 constant dollars). According to an Electric Power Research Institute (EPRI) study performed by United Engineers and Constructors<sup>1</sup>, roughly 57% of this cost is incurred in areas whose expense could be substantially reduced by applying Risk-Based Prioritization technology. Varying cost reduction potentials apply: the largest are for areas like regulatory assurance and QA/QC where as much as 50% of the current costs could be eliminated, smaller percentage cost reductions (up to 25%) are achievable in such areas as training, technical support staff, and maintenance administration. EPRI is addressing ways of applying PRA methods to the following areas to make these O&M cost savings a reality: technical specifications improvements, on-line/off-line maintenance, Appendix R requirements, QA/QC requirements, EQ requirements, component aging, and safety/commercial grade equipment. Several EPRI pilot projects are now complete which demonstrate the cost savings possible.<sup>2,3</sup> With full Nuclear Regulatory Commission (NRC) acceptance of industry's risk-based prioritization techniques, O&M cost reductions of between \$12-18/KWe-yr are feasible. This corresponds to savings of \$12-18 Million per year for a 1000 MWe unit. Substantial savings are possible even without full NRC acceptance through changes implemented under 10CFR50.54 and 50.59.

## UTILITY NEEDS

Operating nuclear power generation facilities face increased pressure from customers and regulatory agencies to improve cost effectiveness of operations. Some costs are not allowed for inclusion in the current rate base and represent an operating loss to the utility. State regulators often use operating and maintenance cost comparisons for competing technologies, such as existing fossil and cogeneration facilities. Occasionally utilities are offered 'incentive' rates by Public Utility Commissions which are tied directly to plant performance. In contrast to these pressures are the requirements of nuclear industry organizations and the NRC to improve the 'quality' of operations. Both the nuclear industry organizations and NRC sometimes use conflicting parameters to judge the effectiveness of operations, and often issue guidelines and/or regulations that significantly impact operational costs. Some nuclear facilities, such as ENTERGY's Grand Gulf station, are convinced that the majority of excess cost is due to misapplication of and over commitment to regulation rather than the regulation itself. Until recently no tools existed to clearly distinguish between those facility programs and processes necessary to preserve safety and those which added little value due to over commitment or poor regulation.

As Individual Plant Examinations<sup>4</sup> (IPEs) are completed and submitted to NRC for review, numerous additional opportunities exist for the application of PRA methodology and plant specific results to address risk impact for regulations. The Atomic Energy Act and 10CFR50 have always recognized that the NRC regulatory process and licensee response to NRC regulations should be proportional to risk of any system, structure or component (SSC) in the plant. It has only been recently with the completion of the IPE process that the tools existed to quantify individual SSC risk. Therein lies a new approach that allows utilities to meet strict compliance to NRC regulations in a way that incorporates risk proportionality, that is, a graded response is possible that accounts for contribution to risk and enables a plant to meet the regulations in a much more cost effective way.

## RANKING OPPORTUNITIES FOR 10CFR50, APPENDIX B

To identify the major cost drivers related to non-safety significant Appendix B requirements, a broad scope effort was started at ENTERGY's Grand Gulf nuclear station in the first quarter of 1993. The object was to apply PRA techniques that could be applied, in combination with deterministic techniques and operational insights, to selected areas to reduce costs while maintaining or reducing the level of risk. The overall approach to the QA burden reduction effort consisted of the following elements:

- Develop a screening technique to rank opportunities for risk-based QA program improvement,
- Develop ways to grade according to safety significance the QA program controls applied to structures systems and components (SSCs),
- Develop means to assess the impact of QA practices on safety and reliability,
- Perform a case study at Grand Gulf to pilot these techniques, and

- Work with Nuclear Management and Resources Council (NUMARC) to ensure both the proper coordination within the nuclear industry and proper interface with the Nuclear Regulatory Commission (NRC).

Because of the different approaches used to implement 10CFR50, Appendix B throughout the industry and the fact that QA impacts almost every aspect of plant operation, a screening approach was developed to identify the most attractive opportunities for risk-based QA program improvements. The goal for the screening approach were:

- It should be quick and inexpensive,
- It should identify cost reduction opportunities with the greatest savings potential, and
- It should provide the information needed for reliable decisions (i.e., highly ranked items should have a high likelihood of success in both the regulatory and financial context).

NUMARC, through its Regulatory Threshold Working Group, has provided useful guidance to the project throughout its inception and performance stages. The results of the Grand Gulf work is currently being made generic to other nuclear plants.

### APPLICATION TO GRAND GULF NUCLEAR STATION

A case study<sup>5</sup> was performed at Grand Gulf Nuclear Station to demonstrate the approach. The engineering design and plant modification process was chosen for analysis to identify potential opportunities to reduce costs associated with 10CFR50, Appendix B implementation without impacting plant safety margins. The results of the Grand Gulf

Table 1(a). Utility changes to the QA process not requiring NRC approval.

List of Opportunities	Risk Profile		
	Safety	Economic	Regulatory
Reduce number and scope of design changes	2	3	2
Reduce design verification effort	3	3	2
Graded corrective action process	3	3	3
Reduce number and types of QA records	3	2	2
Restructure document control process	3	3	2
Personnel certification for repetitive tasks	3	3	1
M&TE calibration based on performance data	2	2	2
Simplify specialty review checklists	3	3	3
Streamline review of design packages	3	3	3
Reduce procurement to obsolete specifications	3	3	3



case study are summarized on Table 1, which summarizes the evaluation of the major opportunities related to the implementation approach, potential risk impacts and projected cost savings. Opportunities are listed in two implementation categories; i.e., those that can be implemented by Grand Gulf without NRC approval (i.e., through 10CFR50.54 and 50.59) and those that probably require an NRC submittal and NRC acceptance prior to implementation. Within these two categories, the items are in rank order with those having the greatest estimated cost savings potential (for Grand Gulf) listed first.

Table 1 also summarizes the level of confidence that a proposed change can be implemented in a fashion that is either safety neutral or a net improvement in safety. The higher the value in the risk profile column, the greater confidence that it will not degrade overall safety.

**Table 1(b). Utility changes to the QA process requiring NRC approval\*.**

List of Opportunities	Risk Profile		
	Safety	Economic	Regulatory
Graded procurement of safety equipment	2	2	2
Increased sharing of procurement resources	3	3	3
Commercial grade dedication process	2	2	1
Less prescriptive audit scope/frequency	3	3	3
Graded QA inspection	2	2	2
Peer inspection by crafts	2	2	2
Reduce vendor audits and surveys	2	2	2
Reduce material traceability	1	0	1

**Risk Profile Key:** 3 = Very Certain 2 = Moderately Certain 1 = Not Very Certain  
0 = Probably Some Risk Impact

\*Note that a portion of the potential savings may be possible in many of these cases without NRC approval.

## CONCLUSION

The results of the Grand Gulf case study verified that large O&M costs savings are possible without degrading safety. A single example from the list is the design verification costs associated with QA. Grand Gulf, like many utilities, does not "grade" the extent of design verification based upon complexity or risk sensitivity. This increases the cost of design and reduces engineering schedule responsiveness. A graded approach would legitimize and standardize verification implementation because it would define decision factors, provide ranked approaches as well as support application of statistical process

control performance indicators/management actions to maintain a more consistent design product quality.

The changes possible in the design process would include provisions to screen design changes for impact on risk-sensitive SCCs to apply (or eliminate) verification activities and to grade the verification activity performed for a given design change. In addition, the process change would introduce focused performance indicators to judge the adequacy of graded verification decisions and would provide the opportunity to continually improve design product quality. To judge the success of the changes, the following performance indicators should be tracked: design engineering schedule performance compared to target, design related field change notices that reflect a failure to provide sufficient quality, and manpower expended on a design change compared to target. Although quantification of the actual savings await the actual implementation of the changes to the design process, preliminary estimates are not inconsistent with the results of the UE&C study mentioned above.

Some of the improvement opportunities are plant specific. This was not unexpected, given other EPRI studies that suggest that the cost structure of licensing related O&M costs varies widely from utility to utility, even plant to plant. Other opportunities are more general Appendix B issues in that they may apply to many other plant processes and may have broad applicability across the nuclear utility industry.

## REFERENCES

1. Braun, C., E. J. Ziegler, and F. J. Rahn, "O&M Cost Reduction Due to the Application of Risk-Based Regulation - Top Level Estimate," ANS Annual Meeting, San Diego, CA, June 21, 1993.
2. Draft EPRI Report, "Application of PRA for the Development of the MOV Test Program Prescribed by Generic Letter 89-10," April, 1993.
3. Draft EPRI Report, "Risk-Based Regulation Project Service Water System Technical Specification Modification," March, 1993.
4. NRC Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities."
5. Preliminary EPRI Report, "Screening Methodology for Identification and Ranking of Opportunities for Risk-Based Application of 10CFR50, Appendix B," August, 1993.

**091 Management Issues**  
***Chair: D. Cunha, Northrop Corp.***

**"Risk Index" - A Proposed Concept**

***S. Chakraborty (Swiss Fed. Nucl. Saf. Insp.); C. Preyssl (European Space Agency)***

**The Quality Issues of Technologic Risk Assessment**

***B.O.Y. Lydell (RSA Technologies)***

## **"RISK INDEX" - A PROPOSED CONCEPT**

**S. Chakraborty<sup>1</sup>, C. Preyssl<sup>2</sup>**

**<sup>1</sup>Swiss Federal Nuclear Safety Inspectorate  
5232 Villigen-HSK  
Switzerland**

**<sup>2</sup>European Space Agency ESA  
2200 AG Noordwijk  
The Netherlands**

### **ABSTRACT**

This paper provides an overview of the theoretical concept for a proposed "risk index" method. This method provides a framework for different risk considerations and decision making under uncertainty. In the definition of the method uncertainties are treated explicitly and systematically. Risk results are displayed on an index scale.

### **INTRODUCTION**

Risk is not an empirical reality and therefore risk communication and risk based decision making are subject to major difficulties. Risk is in itself not a measurable quantity but it has quantifiable components like likelihood, consequence severity and uncertainties. There are other aspects of risk which will influence the risk consideration such as the utility of taking the risk. It is important to have a general approach supporting risk communication and risk based decision making. For this purpose and in order to consider risk with all its associated aspects a "risk index" method is proposed that fulfills a set of general requirements.

### **GENERAL REQUIREMENTS FOR RISK INDEX METHOD**

The following set of general requirements for a risk index method is established:

- \* the risk index method shall be simple, robust and easy to apply
- \* the risk index shall be based on a scientifically sound concept
- \* a systematic treatment of different types of uncertainties must be possible
- \* a discrimination between objective and subjective data must be possible
- \* the steps of the risk index method must be fully transparent to the professional user

- \* the risk index method shall provide a standard language for various groups of users and as such a decision support tool at the various levels of decision making
- \* the risk index method shall support meaningful risk comparisons only by stating its framework, limitations and usefulness.

## DEFINITION OF "RISK INDEX" METHOD

The risk index method is based on a probabilistic evaluation of scenarios. A scenario is defined as a sequence and combination of undesired events resulting in a consequence. Risk  $R$  posed by one or more scenarios is defined as a function  $r$  of three risk parameters  $S$ ,  $P$  and  $U$

$$R = r[S(C), P(C), U(S,F)]$$

$S$  denotes the consequence severity of the consequence  $C$ .  $P$  denotes the likelihood of occurrence.  $U$  denotes the associated uncertainties.

Uncertainty rises from several sources and can either refer to quantitative or to qualitative aspects of the risk. For example a likelihood can be uncertain due to effects of randomness while a consequence severity can be uncertain due to imprecision in the consequence. Uncertainty is represented using uncertainty bounds or distribution functions. In the risk definition uncertainty is an explicit risk parameter in order to account for "no information is important information". The higher the uncertainty in the unfavorable region the higher will be the risk.

The central idea of the risk index method is to assign the risk  $R$  an index  $I$ . This index summarizes all information including uncertainty about the risk. The conversion of  $R$  into  $I$  is performed in two steps.

In the first step both the consequence severity and likelihood are mapped into the "risk index" grid. This grid has basically two dimensions namely  $I(S)$  and  $I(P)$ .  $I(S)$  is the severity index and  $I(P)$  is the likelihood index. In order to represent a risk  $R$  in the grid the severity  $S$  has to be assigned a severity index  $I(S)$  and the likelihood  $P$  has to be assigned a likelihood index  $I(P)$ . The uncertainties associated with  $S$  and  $P$  are represented using uncertainty bounds or in a third dimension using distribution functions. Figure 1 provides an example.

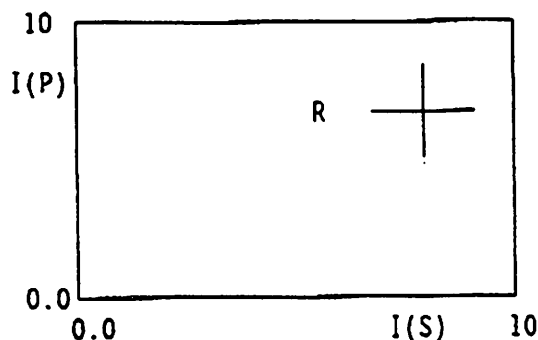


Fig. 1 Risk Index Grid

The transformation of S into I(S) has to be defined on a case by case basis due to the different qualitative and quantitative scales for the consequence severity.

The transformation of the likelihood P into I(P) can be of the general form

$$I(P) = 10 + \log[P(C)]$$

$$P(C) < Z \quad \text{or} \quad I(P) = 0.0$$

where Z is a cut off value.

When it is desirable to deal with point values rather than with distributions the concept of "potentiality" can be used. Potentiality is mathematical definition as follows:

$$Q(E) = Q' \cdot \exp\{0.5 \cdot [\ln(Q'/Q'')/1.645]^2\}$$

where

Q(E) ..... potentiality of event E  
 Q' ..... 50 % quantile of distribution of event E  
 Q'' ..... 95 % quantile of distribution of event E

The potentiality is more sensitive than the median to the location of mass in the upper part of the distribution, but not as sensitive as the mean to extreme tails. For a log normal distribution the potentiality equals the mean.

In the second step the risk R represented in the index grid is converted into the risk index I(R). Each location in the risk index grid is assigned a qualitative or quantitative expression on the risk index scale defined in figure 2. The numeric part of the scale ranges from 0.0 to 100 and the qualitative part of the scale ranges between "maximum risk" and "no risk".

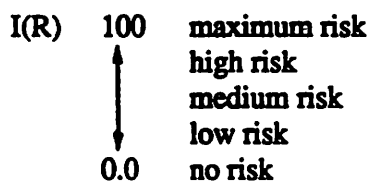


Fig. 2 Risk Index Scale

A possible formula for combining I(S) and I(P) into I(R) is

$$I(R) = I(S) \cdot I(P)$$

which corresponds to weighting the consequence severity with the associated likelihood.

In general the cumulation of risks is carried out before any conversion into indices. However uncertainty in the consequence severity of a risk may require the cumulation of associated weighted risk indices in order to obtain the risk index as a mean value. The weightings are implied by the uncertainty distribution of the consequence severity.

## PROCEDURAL STEPS OF RISK INDEX METHOD

The following steps during practical application of the risk index method can be defined:

- Step 1: Definition of Risk Consideration
- Step 2: Identification of Scenarios
- Step 3: Identification of Consequence Severities
- Step 4: Identification of Likelihoods
- Step 5: Determination of Risk Index
- Step 6: Use of Risk Indices in Risk Considerations

A simple example is provided below to illustrate the steps. Consider the risk assessment for "release of toxic gas from chemical plant". Three major scenarios are identified and investigated in detail in order to introduce risk reducing plant improvements. The consequences of the scenarios belong to different consequence severity categories, which are defined as follows:

- I Catastrophic loss of life on or off site
- II Serious detrimental health effects
- III Major severe material damage
- IV Negligible minor damage

The considered scenarios are:

	Scenario	Consequence	Severity
A	Total release due to tank explosion	Death of large number of people	I
B	Partial release due to pipe rupture	Illness of several people	II
C	Minor release due to leakage	Contamination of plant	IV

In the next step the annual frequency of occurrence of the scenarios is determined and the transformation into I(F) is performed.

Scenario	Potentiality	I(F)
A	2.7E-5	5.43
B	1.1E-6	4.04
C	1.0E-4	6

A quantitative scale for the consequence severity classes is established:

- I [7.5, 10]
- II [5, 7.5]
- III [2.5, 5]
- IV [0, 2.5]

In the next step the risks are displayed in the risk index grid in figure 3.

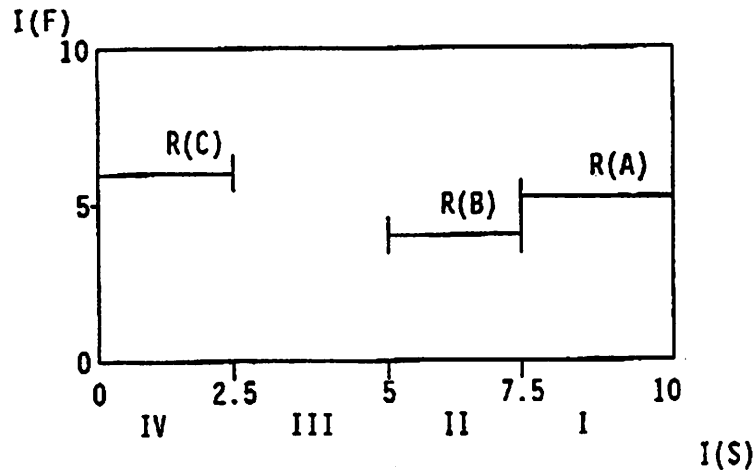


Figure 3. Example

The risk indices associated with the three scenarios is calculated by using the product and the mean operation. The results are

$$\begin{aligned} I[R(A)] &= 47 \\ I[R(B)] &= 25 \\ I[R(C)] &= 8 \end{aligned}$$

They can be displayed on the index scale of figure 2. The tank explosion scenario is found to be the main risk contributor.

## CONCLUSION

The concept of risk index is based on mapping measurable risk parameters into non physically measurable scales. In the risk index method emphasis is given to the coexistence, combination and correlation of qualitative and quantitative concepts.

The risk index method has the potential to reduce the chance of direct misinterpretation and misuse of probabilistic risk results and to improve the communication of risk results to management and - if applied carefully - to the public.

## REFERENCES

- C. Preyssl, et al. "Safety Risk Assessment for ESA Space Programs" ESA Symposium 'Space Product Assurance for Europe in the 1990', ESA SP-316, Noordwijk - The Netherlands, 1991
- C. Preyssl "Fuzzy Risk Analysis for Space Flight Systems" Int. Workshop on Fuzzy System Applications, Kyushu Institute of Technology, Iizuka - Japan, 1988



## **THE QUALITY ISSUES OF TECHNOLOGIC RISK ASSESSMENT**

**Bengt O.Y. Lydell**

**RSA Technologies  
Vista, CA 92083**

### **INTRODUCTION**

The technologic risk assessment discipline provides the analysis techniques and tools for objective quality assurance (QA) of the safety and reliability programs in place at industrial installations. In addition to its 'control function', risk assessment also provides engineering insights directly applicable to the design, operations and maintenance activities; i.e., this is the 'decision support function' of risk assessment. The risk assessment practitioner is using the qualitative and quantitative results of the 'control function' and 'decision support function' to communicate the potential hazards and operability problems throughout the life cycle of an installation.

One of the challenges of risk assessment is the need to maintain risk models in a cost-effective way, and to apply the models on a day-to-day basis. These needs can be fulfilled if the risk model is sufficiently detailed to allow for updates whenever there is a modification to plant design, operations (including procedures), and maintenance. An overriding issue in meeting the challenges is the concept of quality indicators of risk assessment. Unless a risk assessment meets certain quality requirements its ability to fulfill the control and decision support functions is in doubt. This paper defines the quality indicators of risk assessment, and how they are implemented and measured.

### **QUALITY INDICATORS OF RISK ASSESSMENT**

The quality of technologic risk assessment has been expressed as its 'fitness for use' as described by Suokas (1988). That is to what extent the risk assessment, including its boundaries, assumptions, data, models and results satisfy the explicitly formulated goals and requirements relating to the intended use of an assessment. The quality also implies that the best available techniques, analysis practices and documentation practices are adopted, provided they do not entail excessive costs.

Another expression of the quality is given by a three-tier descriptor defined by compliance - completeness - usefulness. The "compliance-factor" is concerned with whether an assessment meets industry standards and practices. It is also concerned with the ability of a risk assessment to demonstrate an industrial installation's compliance with the requirements of risk-based regulations. The "completeness-factor" is described in terms of number of incident scenarios that are addressed relative to the "true" number. Finally, the "usefulness-factor" addresses to what extent a risk assessment can be applied to solve (or address) practical risk management issues.

There is judgment involved in determining quality. While some aspects of it can be measured (e.g., the completeness factor), others will have to be determined by inference. Ultimately the determination of overall quality is given by the practical uses of an assessment, and the ease by which a risk model can be understood and applied to solve practical problems.

The one quality indicator that has received the most attention in the past is the *completeness factor* as demonstrated by Taylor (1991, 1992). One of the criticisms often directed at technologic risk assessment projects is that of incompleteness. Since a risk assessment never can be proven to be "complete" it will never be able to address the "true" risk. The underlying thought behind this criticism has a (theoretical) merit; i.e., risk assessments are invariably incomplete, and, even if believed to be complete, never can be proven to be so. However, it is not sufficient simply to accept a vague declaration of incompleteness. It is important to know (and understand) in what ways the particular risk assessment is incomplete, and to what extent an assessment can be trusted. The issue of completeness is particularly important if a risk assessment is to be used as a decision support function. Here an oversight would not only be an embarrassment for the analyst(s). It could, by concealing the need for safety measures, contribute to a future process-related incident. A worst case situation would be when upon completion of a detailed risk assessment a serious incident does occur that was not addressed (explicitly or implicitly) by the study.

The 'completeness factor' can be measured, say, by comparing the number of identified hazards with the number of known hazards as recorded by the incident data bases. Practically the 'completeness factor' is often addressed through the living risk assessment; i.e., the risk models are maintained regularly and modified as warranted by design changes or new operating experience. It is the availability of state-of-the-art, user-friendly computer aided risk models that have proved to be particularly effective in addressing the completeness of risk assessment.

Another approach to addressing the 'completeness factor' is drawn from insights from repetitive and consistent applications and to make adjustments and modifications as new insights are generated from the analytical process, and by comparing the risk assessment results. This approach has proven effective for the nuclear industry applications of risk assessment as demonstrated by Garrick (1984) and others.

The other two quality indicators are a lot more challenging to address within an ongoing risk assessment project. Clearly, it is not enough to have access to well qualified analysts and computer tools to ensure a high degree of 'compliance' and 'usefulness'. There are numerous examples of elaborate risk assessments, performed with a high degree of attention to details, that don't score very well when viewed from the compliance and usefulness perspectives.

A quality indicator for the *compliance factor* is given by a characterization of how well it has adopted the available industry standards, guidelines and practices for risk assessment in view of the unique design, engineering, operations and maintenance features of an industrial installation. Although considerable efforts have been directed to the development (especially) of guidelines for the practitioners, it must be recognized that some of these guidelines are specific only to one kind of industry applications. As an example, it would not be very effective to assume, without substantial modifications, that a nuclear industry-based guideline for how to analyze control room operator responses to plant upset conditions would be directly applicable to, say, refinery operations. No matter the technical approach chosen by a risk assessment project team, it is never sufficient to just refer to a specific guidance document and to automatically assume that such reference will help achieve the necessary quality requirements. During the early era (1975 - 1985) of applied technologic risk assessment it was not uncommon that the practitioners relied on achievement of compliance through inference via an extensive list of recognized references on risk data and techniques.

In practical terms, the 'compliance factor' can be addressed effectively and controlled through an internal and external peer review process as discussed by Okrent et al (1982) and Evans (1993). If the risk assessment results are "transparent" and can be traced back to the initial assumptions and model input data, and if the applicable standards, guidelines and practices have been applied (or adopted) in a consistent way, it can (normally) be concluded that the level of compliance is high.

An added complication to the determination of the 'compliance factor' is the effect a risk-based regulation can have on the performance of a probabilistic risk assessment. The risk-based regulations have emerged based on a premise that the best way of addressing the potential risks associated with the operation of industrial installations is to use probabilistic risk assessment. Thereby risk comparisons can be made by use of a consistent basis, and the uncertainties can be expressed clearly. Further, the risk assessment discipline allows for an independent "check" of the effectiveness of the traditional (deterministic) engineering approaches to plant safety.

While the development of the risk-based regulations is admirable and appropriate, it is equally important to question the technical clarity of the regulations and the interpretative leverage afforded the risk assessment practitioners. In other words, does a particular risk-based regulations encourage the most appropriate applications, and are the quality indicators of risk assessment addressed properly? It is a complex task to develop effective regulations. There needs to be a balance between the level of prescriptiveness and the level of 'encouraged interpretive allowance'. If a regulation is too prescriptive it may pre-empt the analytical process by the setting of expected or desired quantitative results.

It is often suggested that the most effective way of addressing the 'compliance factor' is to provide the practitioners with standardized tools for risk assessment. However, due to the evolving character of risk assessment it is unclear exactly how the standardization should be pursued, or whether it is a viable solution at all. It is noted that the acceptance criteria of risk-based regulations, the risk assessment techniques and the data go hand-in-hand, see Gjerstad (1992). In view of this observation some extremely valuable insights have been generated by national risk assessment programs where industry and regulators have worked together to establish comprehensive and up-to-date equipment reliability data bases and computer tools. By making available to the risk assessment practitioners a range of industry-sponsored comprehensive data bases and computer tools

a very high degree of uniformity has been achieved in how the risk assessments are performed. This uniformity allows for a consistent risk communication basis and risk comparisons.

One concept used to determine the 'usefulness factor' is the predictive validity of a risk assessment as introduced by Suokas (1988). The predictive validity concept illustrates how well the risk assessment addresses the objectives for which it is intended. Specifically, the concept illustrates the capability of an assessment to estimate the risks associated with the operation of a process. It can also mean the ability of an analysis to estimate the effect of a suggested safety improvement on the incident frequency or consequences. Hence, the 'usefulness factor' can be determined by how often a risk assessment is applied to answer engineering type and risk management type questions. Clearly, the usefulness is highly correlated with the level of detail and technical approach of the risk model development.

To measure the usefulness of a risk assessment one must characterize how often the risk model successfully is applied to support a regulatory case, design modification case, incident investigation case, etc. A frequent usage normally implies that the risk assessment products have been accepted and are easy to understand and communicate. Not only by the risk assessment practitioners, but by management and operations personnel.

## THE DETERMINATION OF QUALITY

With the overview of the risk assessment quality indicators as a background, a key question is whether it is essential (i.e., a must) to comply with all three indicators in the broadest sense for a risk study to be "fit for use"? By design, the risk assessment process is highly dynamic and subject to modifications and iterations as the analytical process progresses. Unfortunately, any one of the three indicators does not in itself ensure that the overall risk assessment product is totally fit for use.

Take for instance the 'completeness factor'. If we were to focus, say, all our resources on making sure that all possible hazards and operability problems are addressed in detail, doubts present themselves about the practical usefulness of this effort to address risk-impact of design modification. In a similar vein, if we were to prepare extremely detailed system fault trees but refrain from development of unit- or plant-specific equipment reliability parameters, the risk model may be ineffective in addressing specific risk management questions. In any risk assessment it is possible to stop the process of hazard identification at any level. Generally, the more detailed the analyses, the more opportunity for oversights due to "tunnel-vision".

A balance must be struck between the desired achievement of excellence in all three areas of risk assessment quality. The three quality indicators can be addressed in sufficient depth as long as there is a sustained management commitment to risk assessment and risk management. Ultimately the "fitness for use" is determined by the how a risk assessment project is planned.

The key question of the risk assessment planning effort is "who will perform the assessment?" The answer to the question is highly correlated with quality. In terms of results, insights and validity, two different groups of risk assessors can generate two very different products. The process of performing risk assessment is by definition a team

effort. Therefore, the way a risk assessment team is put together and organized to do its work has a strong influence on how the technical work is performed. To meet project objectives and to stay within budget it is necessary to first understand the limitations of the team itself.

Assuming a group of highly experienced practitioners, the most important aspect of having a successful team effort is good communications within the team and an ability to allow for job rotation. Because of project constraints and/or staff availability the project team does not always consist of a coherent group of professionals with similar experience levels. However, the novice risk assessor can have as positive/important role in a project as the highly experienced practitioner. The project manager must allow for the novice analyst to learn from the experience and to be part of the technology transfer that always should take place while developing a risk model. In fact, the novice can be extremely effective in ensuring that there is ongoing internal review of work products. It is a cost-effective way of addressing the 'compliance factor'.

## **SHARED RESPONSIBILITIES**

The quality concept of technological risk assessment can be formalized in a theoretical way through the three-tier descriptor of 'compliance - completeness - usefulness'. Ultimately it is the organization of the risk assessment project and the support it receives from upper management that determines what degrees of quality will be achieved. It is not just the data, the computer tools, or the project manager taken individually that determines the acceptability of the product. Risk assessment quality is determined by the totality of the features that constitute the risk assessment project and its future applications. An awareness of the quality indicators and their implications should be viewed as starting point for understanding and instilling quality in risk assessment.

During the past decade there have been numerous efforts towards risk-based regulations. The way these regulations have been implemented has had an important effect on how the quality issues are viewed and addressed by the practitioners. It can be argued that while some of the regulations have been poorly conceived and coordinated, there are also some extremely positive and valuable lessons that have been learned. An important aspect of risk assessment is the systematic and consistent application of a risk model within an overall risk management scheme. The sophisticated and informed risk-based regulation should focus on this notion and provide a framework for quality requirements.

Ultimately the risk assessment professional determines the "fitness for use" by performing the analyses in a responsible way and by employing tools and techniques in a most cost-effective way. Where the objectives of a risk assessment project is considered counter-productive to meeting any of the quality indicators, the necessary adjustments should be proposed and implemented. Throughout the risk assessment project there should be an effort to:

- Interact with project team members to ensure consistency and clarity of deliverables
- Analyze the risk assessment task procedures and analysis tools on a regular basis with intent of improvement
- Communicate with customers (users) of the risk assessment for the purpose of clear understanding of the requirements.

## REFERENCES

- Evans, M.G.K., 1993. Review of PRA - what guarantee of quality does this offer, *Proc. Probabilistic Safety Assessment International Topical Meeting*, American Nuclear Society, La Grange Park (Ill).
- Garrick, B.J., 1984. Recent case studies and advancements in probabilistic risk assessment, *Risk Analysis*, Vol. 4, No. 4, pp 267-280.
- Gjerstad, T., 1992. Safety evaluation of offshore installations and operations: the Norwegian experience, *Reliability of Offshore Operations: Proceedings of an International Workshop*, NIST Special Publication 833, National Institute of Standards, Gaithersburg (MD), pp 69-78.
- Okrent, D. et al, 1982. "On PRA Quality and Use," UCLA-ENG-8269, UCLA School of Engineering, Los Angeles (CA).
- Suokas, J., 1988. Evaluation of the quality of safety and risk analysis in the chemical industry, *Risk Analysis*, Vol. 8, No. 4., pp 581-591.
- Taylor, J.R., 1991. "Quality and Completeness of Risk Analyses. Vol. II: Computer Aided Hazard Identification," TA-91-35-1, Taylor Associates ApS, Glumsø (Denmark).
- Taylor, J.R., 1992. "Quality and Completeness of Risk Analyses. Vol. I: Hazard Identification," 2nd Edition, Taylor Associates ApS, Glumsø (Denmark).

**092 Industrial and Transportation Risks**

*Chair: D. Henneke, TENERA*

**The ARIPAR Project: Analysis of the Industrial and Transportation Risk Connected with the Ravenna Area**

*D. Egidi (Civil Protection, Emilia Romagna Region); F. Foraboschi, G. Spadoni (U. Bologna); A. Amendola (CEC-JRC)*

**Identification and Evaluation of Maritime Exposures**

*J.L. Borrello, M.J. Spansel (Adams & Reese)*

**A Decision Model of a Multi-Point Mooring of a Tanker with a Tug Assist**

*M.L. Eskijian (Calif. St. Lands Commis.)*

## **THE ARIPAR PROJECT: ANALYSIS OF THE INDUSTRIAL AND TRANSPORTATION RISK CONNECTED WITH THE RAVENNA AREA**

**Demetrio Egidi<sup>1</sup>, Franco P. Foraboschi<sup>2</sup>, Gigliola Spadoni<sup>2</sup>, Aniello Amendola<sup>3</sup>**

<sup>1</sup> Civil Protection of the Emilia Romagna Region, Bologna, Italy

<sup>2</sup> Chemical Eng. Department, University of Bologna, Italy

<sup>3</sup> CEC-JRC-ISEI, 21020 Ispra (VA), Italy

### **INTRODUCTION**

The paper describes the main outcomes from the ARIPAR project, aimed at the assessment of the risks connected with processing, storage and transportation of dangerous substances on the Ravenna industrial and harbour area.

The main objective of the project has been the assessment of the major sources of accident risks, in order

- to plan for urban development taking into account major accident hazards;
- to plan for the improvement of transport infrastructure (road, railways, shipping and pipelines) to diminish possible accident risks;
- and, to evaluate compatibility of new industrial developments with existing land use.

The project started in 1988 with the complete inventory of the different hazard sources: process and storage facilities, warehouses, transport ways and quantities of the single dangerous substance involved in each activity. It has been monitored by very representative scientific and technical committees, with the contribution of the involved industries and commercial organisations, as well as of the administrative and social parties. A consistent part of data collection, model development and calculations has been performed by the engineering companies SNAM Progetti, Niers and DAM. It has been concluded by the publication of the final report<sup>1</sup> in 1992.

### **PROJECT DESCRIPTION**

In the Ravenna area there are about 47 fixed installations, 9 of which with inventories of dangerous substances above the threshold for the safety notification according to the Seveso directive<sup>2</sup>. Main substances involved are chlorine, ammonia, acrylonitrile, various inorganic acids, LPG, high flammable liquids.



Around the harbour activities there is a movement of large quantities of dangerous substances transported by road (700,000 trucks/year with 13 million tonnes of goods, 6.4 % of which are constituted by hazardous substances. Just to give a figure, the only LPG quantity transported by road amounts to about 200,000 tonnes/year); by shipment in the channel port (3,500 ships/year for a total of 14 million tonnes of goods, 13% of which are constituted by hazardous substances); by railways (500,000 tonnes/year, 20% of which are constituted by hazardous substances); and by 16 oil or gas pipelines.

The data collection for the project has been the first example of a very comprehensive inventory of stored, processed and transported dangerous substances, having been done in Italy on an important industrial area. This was possible thanks to the collaboration of all institutions and industries involved which gave access to the data, even without a mandatory legal requirement.

The study has concerned all the hazard sources on the area including railways and transportation roads. The area on which accidents may have a significant impact is large about 220 square Km (Figure 1).

The second step has been the identification of accident scenarios (release and explosion events and their probabilities) for each hazard source. For the 9 plants for which obligations for safety reports existed, the accident scenarios considered in the reports have been assumed, some other few scenarios have been included after suggestion of the scientific and technical committees. For the other plants, as well as for pipelines it has been necessary to conduct a safety analysis to identify the possible accidents scenarios. A particular methodological effort has been required to model transportation accidents and especially accidents from ships entering and moving along the harbour channel (Figure 1).

This step has resulted in the identification of about 2,500 scenarios to be included in the quantitative risk assessment. At the same time the characteristics of the territory and the population (residential and not residential) as well as the meteorology of the area have been analysed.

Afterwards the individual risk contours and the group risk have been evaluated for each hazard source and for each single dangerous substance (i.e. chlorine, ammonia, etc.). Lastly the single risk curves have been composed in order to get overall area risk levels, taking also into account the possibility of Domino effects between installations on nearby sites (these however have been found to not contribute significantly to the overall risk). At this purpose new models and new computational tools have been developed, which enable to evaluate at the same time the risk contribution from transportation and fixed installation in connection with the population and the meteorological data of the area, including Domino effects. Via the developed software package it was possible to evaluate:

- the local risk contours (a characteristic of the location for a person permanently exposed to the risk);
- the individual risk contours (as above but taking into account the permanence time at a given location);
- the F-N diagrams; and
- the I-N diagrams (the number of people exposed at a certain risk).

## RESULTS OF THE RISK CALCULATIONS

Figure 1 shows the overall local risk contours (from all sources) on the whole area subjected to the study. Similar risk contours have been derived for each hazard source category: major fixed installations; other fixed installations; transportation by roads, by railways, by ships and by pipelines. Furthermore sensitivity analyses have been made

with respects to the most critical substances (because of either their intrinsic hazards or their quantitative relevance).

The limits of the paper do not allow to show the complete results: therefore examples of individual risk contours, and I/N diagrams are not presented. To show the sensitivity of the results to the single hazard categories, F/N diagrams are depicted in Figures 2 to 5, for the overall hazards sources, for the major installations, for road transportation and for railways accidents respectively.

## DISCUSSIONS OF THE RESULTS

Risk contours characterised by a frequency of about  $10^{-4}$  lethal events per year (indicated in the following simply as f/y) are found on the industrial area near to the harbour channel where there is a high concentration of fixed installations and transportation nodes. The Ravenna town area is characterised by risk contours values less/equal to  $10^{-6}$  f/y which are consistent with criteria set up by countries having adopted risk goals for their land use planning policy<sup>3</sup>.

The major contribution to individual risk in the town is deriving from road transportation and from the marshalling yard nearby the railways central station.

Some few relatively small inhabited areas have been identified for which the overall individual risk is about  $10^{-5}$  f/y. On the other hand from the I/N diagrams it could be ascertained that 93% of the population is exposed to an overall individual risk less than  $10^{-6}$  f/y.

By the analysis of the contributions of the single hazard sources with respects to their effects on the F/N diagrams (Figures 2 to 5) it could be assessed that

- up to  $N=100$  the major contribution to the risk arises from dangerous substances transportation by road;
- for  $N$  ranging between 100 and 1000, the contributions from road transport, fixed installations and railways (essentially marshalling yard) are equivalent;
- for  $N > 1000$  the contribution from the marshalling yard located too near to the town is dominating.

The single hazard sources which give the maximum contribution to the area risk resulted to be the fixed installations in which release of toxic materials is possible (in particular chlorine and ammonia); some well identified road sections characterised by a high frequency of trucks transporting dangerous substances; and, finally, the marshalling yard.

On the contrary pipelines and ship transport within the harbour channel do not give a relevant contribution to the overall risk.

Furthermore the results show that the contribution of accident hazards linked with the release of toxic substances is dominating with respects to accidents provoking fires and explosions without toxic releases. Finally the contribution to the overall risks from Domino effects involving different sites is negligible: however this last result might be affected by model simplifications introduced in the resolution of the subdivision of the study area to avoid prohibitive computational times.

## SOME CONCLUSIONS

Along the execution of the project, full awareness existed about the uncertainties linked with performing such kinds of studies<sup>4</sup>. However the results described in above have been found very useful to ranking hazards and to prioritise interventions.

Three results in particular have been found to be very important:

- the fixed installations are located sufficiently far from the Ravenna town, so that they do not contribute significantly to the risk in the town;
- the contribution of the 9 "Seveso" sites is dominating with respects to the total contribution to the risk from the resting 38 sites storing / processing dangerous substances. This confirms the distinction in the obligations put by the existing regulations with respects to the different categories of sites;
- the contribution to the overall risk from transport sources may dominate in certain cases as the transportation roads and/or the marshalling yards might be located nearer to inhabited areas. Therefore the existing regulations on transportation of dangerous goods is unsatisfactory.

The value of the project is not restricted to the quantitative results: an enormous amount of information concerning the activities involving dangerous substances are now available to the administration. From the study very useful information has been also extracted for the emergency plan of the whole area as privileged sources of accidents (including transportation), extension of their consequences (independently of the probability of occurrence), as well as particularly vulnerable areas have been identified.

The informatic structure of the model will allow the administration to update the risk situation and therefore to establish a decision tool for land use planning and control for future developments in the area.

The project has also to be considered as a pioneer study in Italy, which anticipate the requirements which are being introduced in the revision of the "Seveso" Directive concerning land use planning with respects to major accidents hazards and public participation in the related decisions.

Under the latter aspect, by the way in which all parties involved collaborated in the data acquisition and analysis, and by the way the information has been given to the public, the project has to be considered as mostly successful. Indeed the results have been presented to the public in Ravenna on April 1993. This was the first time that in Italy chemical risk figures have been publicly presented and discussed. The event had a good acceptance by the public. The reason for that was not only the quality of the scientific project, but even the fact that together with the results, proposals for a better risk control and for priority interventions both in the public sector and in the private one have been presented.

## REFERENCES

1. Report on the results of the ARIPAR project, Published by the Italian Civil Protection Department and by the Emilia-Romagna Region, Bologna, Italy, November 1992 (in Italian)
2. Council Directive of June 24, 1982 on the major-accident hazards of certain industrial activities (82/501/EEC). Official Journal of the European Communities L230, Vol. 25, August 5, 1982.
3. See for instance: C.J. van Kuijen "Risk Management in The Netherlands: A Quantitative Approach" in B. Segerstahl and G. Kroemer (eds.) Issues and Trends in Risk Analysis. IIASA, Laxenburg(A). WP-88- 34, pp.41-57.
4. A. Amendola, S. Contini and I. Ziomas: Uncertainties in chemical risk assessment: Results of a European benchmark exercise. The Journal of Hazardous Materials. 29 (1992) 347-363

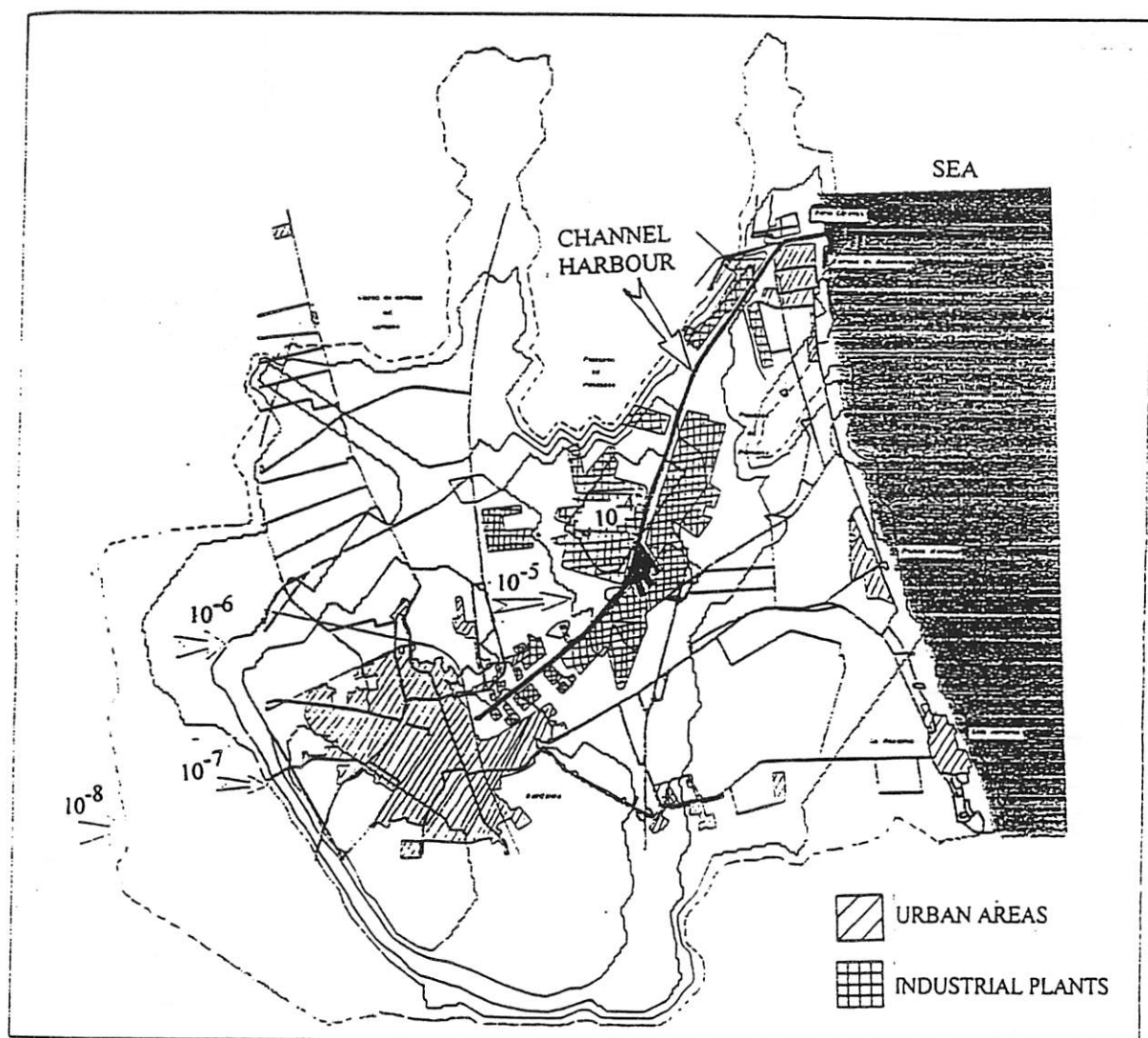
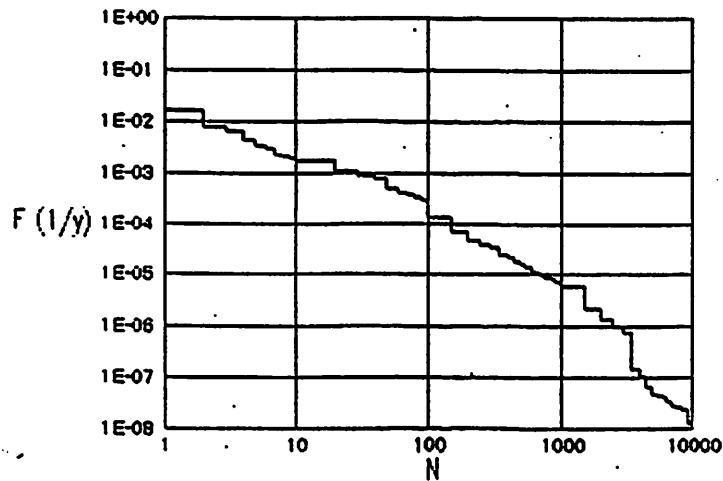
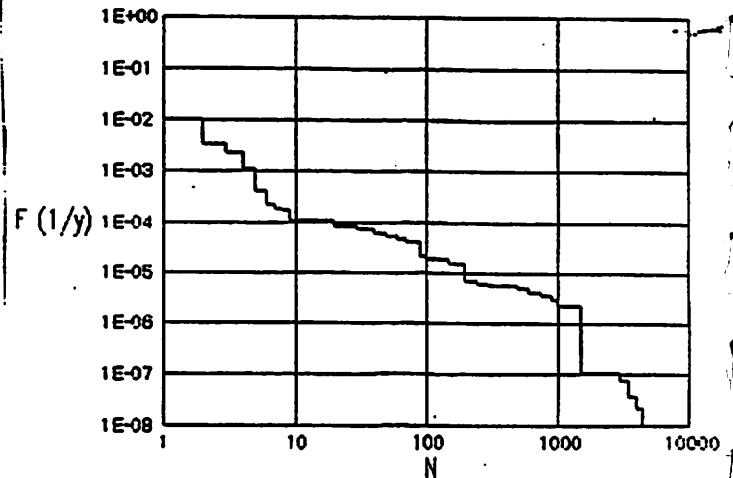


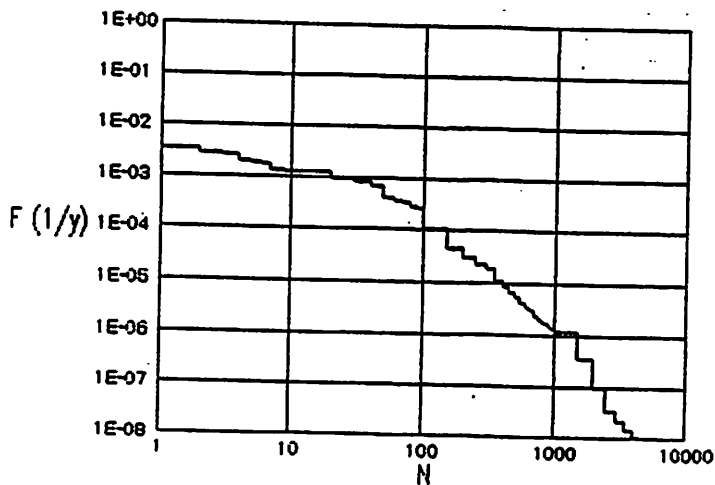
FIG.1: LOCAL RISK CONTOURS FROM ALL SOURCES



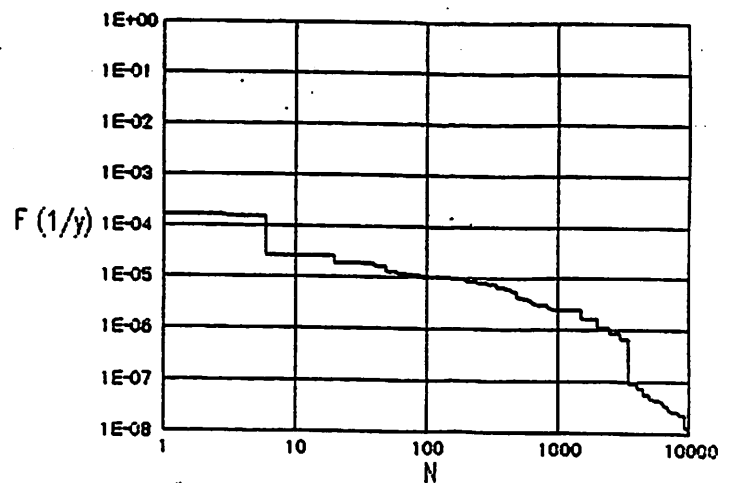
**FIGURE 2**  
**F-N DIAGRAM**  
**FROM ALL SOURCES**



**FIGURE 3**  
**F-N DIAGRAM**  
**FROM MAJOR INSTALLATIONS**



**FIGURE 4**  
**F-N DIAGRAM**  
**FROM TRANSPORTATION**  
**BY ROAD**



**FIGURE 5**  
**F-N DIAGRAM**  
**FROM TRANSPORTATION**  
**BY RAILWAYS**

## **IDENTIFICATION AND EVALUATION OF MARITIME EXPOSURES**

Joel L. Borrello and Mark J. Spansel

Adams and Reese  
Attorneys and Counselors at Law  
4500 One Shell Square  
New Orleans, LA 70139  
(504) 581-3234

### **I. INTRODUCTION**

Regardless of the industry or business, if its activities, even incidental, occur on, near or around navigable waters, then there is a likelihood that injury to persons, death and damage to property will be regulated by the maritime law of the United States, necessitating identification of these risks and evaluation of the corresponding exposures. Though the primary functions of a business may not be associated with navigable waters, secondary activities, including waterborne shipment of products, may create maritime liabilities. An awareness and understanding of these risks is essential for making decisions in the areas of prevention, budgeting, contract protection and insurance coverage.

### **II. REMEDIES AVAILABLE TO MARITIME WORKERS**

#### **A. General Maritime Law**

Those remedies generally recognized under the General Maritime Law are available for maritime tort, unseaworthiness, wages, maintenance and cure.

**1. Maritime Tort - Negligence.** The cause of action of maritime tort is based upon concepts of simple negligence or a breach of the duty to exercise ordinary care and becomes actionable when that negligence is a proximate cause of the resulting injury, death or property damage. Essentially, the claim is triggered if the accident occurred on navigable waters.

**2. Unseaworthiness - Strict Liability.** The warranty of seaworthiness, another theory of liability, is owed by a vessel owner or bareboat charterer to provide a vessel and appurtenances which are reasonably suited for their intended use. If an accident results from an unseaworthy condition, the vessel owner or bareboat charterer will be liable even though he may not have been negligent in bringing about that unseaworthy condition.

**3. Nature of Remedies.** When personal injury is associated with the maritime tort of negligence or unseaworthiness, the claimant is entitled to recover what are called by the law "general" and "special" damages. General damages include pain, suffering, fear, fright, humiliation, embarrassment and similar losses that are not subject to direct measurement. On the other hand, damages that can be objectively measured, such as property damage, medical expenses, loss of past wages and loss of future wage earning capacity are considered to be special damages. In the event of the death of a non-seaman, the survivors may also recover loss of support, services and society - including loss of love, affection, attention, companionship, care, comfort and protection. Provable damages will be recoverable in the case of property damage.

**4. Wages, Maintenance and Cure.** These remedies against the employer or shipowner are available only to seamen, who are injured or fall ill in the service of the vessel without regard to negligence, fault or unseaworthiness. In brief, a seaman is entitled to wages to the end of the voyage; maintenance in the form of a daily allowance; and, finally, cure or medical expenses related to the injury or illness.

#### **B. The Jones Act (46 USC Sec. 688, et seq.)**

In 1920, Congress enacted the Jones Act, which permitted seamen in the case of injury or their survivors in case of death, to sue the employer for damages based on negligence of that employer or fellow crewmembers. That negligence is actionable if it contributes "even the slightest" to the injury. When personal injury is involved, the seaman may recover from his employer all provable general and special damages. However, in the event of death, the survivors are limited to pecuniary loss, that is, the monetary value of the support and services which the beneficiaries would have received had the seaman lived.

#### **C. Death on the High Seas Act (46 USC 761, et seq.)**

Also in 1920, Congress enacted the Death on the High Seas Act to provide a remedy for deaths occurring more than three nautical miles from the shores of the United States, its territories or dependencies. The beneficiaries must prove negligence, unseaworthiness or strict liability that was a proximate cause of the death and will be limited to pecuniary loss.

#### **D. Longshore Act (33 USC Sec. 901, et seq.)**

The Longshore Act, which specifically excludes seamen, provides a workers' compensation remedy in lieu of general damages in the form of medical expenses and scheduled, weekly benefits against an employer for injury or death occurring in the course and scope of employment without regard to whether the employer or the employee was guilty of fault. These benefits are the exclusive remedy against the employer except in limited situations. Generally, this Act provides benefits which are significantly greater than those recognized under most state workers' compensation acts.

The Act covers those involved in maritime employment, including but not limited to any longshoreman or other person engaged in longshoring operations, and any harbor worker, including a ship repairman, shipbuilder or shipbreaker ("status" test), who are injured or killed on navigable waters of the United States or adjoining land areas, including but not limited to any adjoining pier, wharf, dry dock, terminal, building way, marine railway or adjacent area customarily used by the employer in loading, unloading, repairing, dismantling or building a vessel ("situs" test). By virtue of the Outer Continental Shelf Lands Act, the Longshore Act applies to accidents on fixed platforms on the Outer Continental Shelf.

Coverage of the Longshore Act can be triggered for workers, who otherwise are considered land-based personnel, but who are assigned to water-related activities. Take, for example, a construction foreman assigned to a project to build a sewerage treatment plant on a river. If that foreman is injured on a barge while directing the unloading of the barge, he will most likely be entitled to Longshore benefits from his employer.

#### **E. State Workers' Compensation Acts**

Some maritime workers are entitled to seek a workers' compensation remedy in lieu of general damages against their employers in connection with injury or death occurring in the course and scope of employment under state statutes. Fault is not relevant to most state workers' compensation remedies. Because the Longshore Act not only covers navigable waters, but also adjoining land areas, state workers' compensation acts may overlap with the Longshore Act, providing concurrent application. Normally, however, workers elect Longshore benefits because they are usually higher than the corresponding state remedy. Moreover, various states have extended their acts to accidents on fixed platforms offshore.

#### **F. State Tort Law**

Naturally, state tort law will apply to land-based accidents occurring within a state's territorial boundaries. Moreover, state tort law will apply to fixed platforms within a particular state's territorial waters. Additionally, by virtue of the Outer Continental Shelf Lands Act, enacted by Congress in the early 1950's, state tort law will govern occurrences on fixed platforms on the Outer Continental Shelf, immediately adjacent to the particular state. In each instance, general and special damages are recoverable.

#### **G. Generally No Double Recovery**

As a result of the preceding discussion, it is apparent that some of the causes of action and remedies reviewed overlap and others are mutually exclusive. In general, however, there is no double recovery of damages, though more than one theory of liability may apply. The exception is when the particular loss is also covered by a separate resource, such as a health care insurance policy not provided by the tortfeasor.

### **III. RELATIONSHIP BETWEEN STATUTORY REMEDIES AND THE GENERAL MARITIME LAW**

States may not enact laws which deprive parties of rights under the General Maritime Law or otherwise affect the uniform application of maritime law. On the other hand, according to the United States Supreme Court, federal statutes of Congress not only affect, but in general preempt, the application of the court-created General Maritime Law. Thus, in situations where the Jones Act or the Death on the High Seas Act are applicable, wrongful death remedies are limited to the pecuniary losses of support and services and not the extended benefits of loss of society or consortium.

### **IV. RELATIONSHIP BETWEEN JONES ACT AND LONGSHORE ACT**

The Jones Act and the Longshore Act are both federal statutes which provide remedies against employers for injury or death sustained by maritime workers. On the one hand, the Jones Act covers seaman; and, on the other hand, the Longshore Act governs maritime workers who are not seamen or members of the crew of the vessel.



## **V. INTERACTION BETWEEN LONGSHORE ACT AND STATE COMPENSATION ACTS**

As noted previously, because the Longshore Act's coverage extends to certain land areas adjoining water, its coverage may overlap with state workers' compensation acts. In those instances, receipt of benefits under one act does not preclude a claim under the other act, subject to a credit in favor of the employer to avoid double recovery. In most instances, though, injured workers will simply opt for the Longshore remedy for the reason that it will most often exceed state benefits.

## **VI. JONES ACT STATUS**

A seaman covered by the Jones Act is one who is more or less permanently assigned to a specific vessel or fleet of vessels under common ownership or control in navigation. The seaman's work must further the overall function of the vessel. It is not necessary that the worker be involved in the navigational movement of the vessel.

When faced with the term "seaman", one normally thinks of a member of a crew of a classic ship, plying the seas. In maritime law, the notion is not so limited. A jack-up drilling rig is a vessel and a driller on the drilling crew is considered a seaman. A barge on which a crawler crane was mounted has been determined to be a vessel and the crane operator a seaman. Thus, if an object or watercraft is capable of being used for transportation on navigable waters, then the personnel assigned to it may qualify for seaman's status, if they meet the test described above.

## **VII. PUNITIVE DAMAGES**

Punitive damages are recoverable under the General Maritime Law in cases of personal injury and property damage and are awarded as punishment in addition to compensatory damages, if the conduct of the defendant was egregious, such as willful, wanton or reckless behavior. If the defendant is a corporation, partnership or principal, then the act must be committed by one with managerial or policy-making authority. Should a claim under the Jones Act or Death on the High Seas Act be asserted, then punitive damages are considered non-pecuniary and, consequently, not recoverable by implication of a recent decision of the United States Supreme Court. To date, the United States Supreme Court has found punitive damages to be constitutional, within certain parameters.

## **VIII. PRODUCTS LIABILITY**

As a result of a decision by the United States Supreme Court several years ago, the General Maritime Law now includes the concept of strict liability on the part of maritime manufacturers. However, the product must cause personal injury or damage to property other than the product itself. There must be a defect in the product which creates an unreasonable risk of harm or is unusually dangerous in normal use. At the time of the damage, the product must in fact have been in normal use. It is essential that the loss be caused by a defect, which existed when it left the hands of the manufacturer. Not only does the products liability doctrine cover manufacturers, but also component manufacturers and those providing maritime services. Where the only damage is to the product itself, the rights of the parties are governed by contractual provisions, warranties, conditions and disclaimers.

## **IX. CONTRACTUAL INDEMNITY**

General Maritime Law permits allocation of responsibility for personal injury and property damage between parties by way of indemnity through contractual arrangements. It is also common for maritime contracts to state the insurance requirements for the contracting parties. These devices may be particularly important in the area of protection against maritime liability. However, some states prohibit or restrict the enforceability of certain indemnity provisions, particularly those that provide indemnification for the consequences of one's own negligence. Therefore, of prime importance is the resolution of whether the contract is maritime or non-maritime. In general, courts make this determination by examining whether the contract, activities and circumstances in question involve traditional maritime activity.

## **X. MARITIME INSURANCE**

Although maritime insurance is a subject matter that may warrant a presentation in itself, it is noteworthy here that the appropriate insurance for the maritime risks addressed above will protect against those losses. Most of the coverages are particularized and generally not provided under standard liability policies without specific tailoring. Even punitive damages under the General Maritime Law may be insured.

## **A DECISION MODEL OF A MULTI-POINT MOORING OF A TANKER WITH TUG ASSIST**

**M. L. Eskijian**

**California State Lands Commission  
200 Oceangate, Suite 1200  
Long Beach, California 90802**

### **INTRODUCTION**

The problem is to construct a decision model for the evaluation of whether or not a tug boat assist is recommended for the mooring operation of a tanker at a multi-point facility. For this study, a mooring master was interviewed, and a simplistic decision model was created using an influence diagram. The paper will first summarize the interview, and then discuss the model created using an influence diagram, and finally present some of the results of this study. The software used for this study is "INDIA" (INfluence DIAGram) by Decision Focus, Inc of Los Altos, California. It should be noted that this paper is not an endorsement of any particular software package, nor does it represent official policy of the California State Lands Commission.

Variables with simple probabilities include tanker size, current direction and magnitude, tug availability and tanker crew expertise and communication in English. The problem was to evaluate whether or not a tug should assist in the mooring process. Accident scenarios are postulated in terms of time loss and associated costs, independent of who pays. In this

simplistic example, losses are computed as the sum of all possible financial losses. The postulated damage is a time or mechanical delay, induced by a improper mooring, or the vessel running over the hose buoy-- possibly rupturing the line, causing damage to the vessel screw and putting the pipeline contents (shore to mooring) into the water. Structural damage to the propeller is an additional concern and the associated tanker time losses are included. Operational errors are translated into lost time in achieving the mooring. Oil in the water is not a postulated scenario for this problem.

## **THE INTERVIEW AND CONSTRUCTION OF THE DECISION MODEL**

The interview with a mooring master included details from the initial boarding of the tanker to the tie-down of all of the lines. The mooring master boards the vessel, inspects the topsides as he walks to the bridge, hands the captain a newspaper and shakes hands. Each step of the process is important to the overall understanding of the operation, and is greatly simplified to construct the influence diagram. The interview ended with the mooring lines connected, and unloading operations commencing.

Figure 1 presents the detailed INDIA influence diagram. Initial probabilistic nodes include the current conditions, vessel size and crew competence. These probabilistic nodes feed into other probability nodes, describing the tug, possible operational errors and mechanical failures. Tug availability is then considered, and deterministic cost evaluations are then calculated, resulting in the computation of the total cost. The model does not consider profit, but merely seeks to minimize the financial loss, independent of responsibility.

Based on the interview, the following probabilities have been assigned. The values are based on the judgement of the mooring master, and should not be considered qualitative, and serve as an example only. They illustrate the usefulness of the model; others should construct their own probabilities. A description of each node in the model follows:

1. **CURRENT CONDITIONS:** Current conditions can be slow, unfavorable or unpredictable. For this specific model, the current is the primary environmental load. For the unloading process, the vessel is at deep draft with a minimum sail area during mooring. The slow current condition is the normal operating condition; velocity is slow and direction is as expected. The unfavorable condition has also been included in the mooring design, but is less than ideal; direction and magnitude are not desirable, but acceptable and can be accommodated by the skill of the harbor master and vessel captain. The unpredictable current condition has been defined as uncertainty both in magnitude and direction; this condition could easily create problems and time delays in the mooring operations.

Description	Probability
Slow	0.90
Unfavorable	0.10
Unpredictable	0.05

2. **VESSEL SIZE:** The vessel size ranges from small, medium to large. The table of values is as follows:

Description	Probability
Small (less than 50,000 DWT)	0.75
Medium (capacity less than 72,000 DWT)	0.15
Large (capacity greater than 72,000 DWT)	0.10

The larger vessels require a tug, regardless of other conditions.

3. **CREW:** The level of crew competence is a final initial probability variable. For purposes of this model, three possible crew conditions were postulated:

Description	Probability
Competent	0.70
Acceptable	0.20
Unknown	0.10

The unknown crew is most likely foreign, and few of the crew can communicate in English. The acceptable crew has probably called on this port before, and the mooring master might have had problems with them in the past. The competent crew is most likely a "company vessel", and everyone is familiar with the captain and the vessel.

These three probabilistic nodes feed into other probabilistic nodes that define tug conditions/availability, and different types of errors that can result from crew and vessel accidents. This second tier of probabilistic nodes have been defined as follows:

4. **TUG 1:** This simple probabilistic node assigns a probability as to whether or not a tug would be assigned to the vessel, based on the environmental load conditions:

Description	YES	NO
Current Slow	0.02	0.98
Current unfavorable	0.50	0.50
Current unpredictable	0.90	0.10

5. **TUG 2:** This simple probabilistic node assigns a probability to whether or not a tug is required, based on vessel size. Large vessels will always require a tug:

Description	YES	NO
Small	0.10	0.90
Medium	0.50	0.50
Large	0.95	0.05

6. **TUG 3:** Based on the mooring master's perception of the crew's competence, a tug might be required:

Description	YES	NO
Competent Crew	0.05	0.95
Acceptable Crew	0.40	0.60
Unknown Crew	0.85	0.15

7. **OPERATIONAL ERRORS:** Based on the crew expertise, the following matrix of probabilities is constructed for various operational errors. The first type of error involves a communication failure, resulting in some sort of operational upset. The second type of error is a judgment error - information was correct, but the crew made an error in judgement. Coordination is the next type of operational error; someone didn't get the correct message, communicated from the harbor master to the vessel crew, or in response to the crew, the harbor master did not process some information, or whatever. The next type of error involves the crude oil cargo; operating temperatures, flowing temperatures, both real and reported are potential sources of operational errors. This list is not purported to be exhaustive, but could easily be modified to include a multitude of other possibilities:

Description	Comm.	Judgment	Coord.	Cargo	None
Competent crew	0.02	0.02	0.02	0.02	0.92
Acceptable crew	0.15	0.15	0.15	0.15	0.40
Unknown crew	0.20	0.20	0.20	0.20	0.20

This matrix illustrates the small probability of operational errors with a competent crew, and the relatively high probability with an unknown crew. These probabilities are not meant to be considered qualitative by others; they represent one harbor master's perception for one specific location.

8. **MECHANICAL FAILURES:** Closely coupled with the crew's capability is the mechanical condition of the vessel and its equipment required to moor the vessel. The

following matrix of probabilities was constructed:

Description	Winch Lines	Anchor Windlass	Pump Failure	Power Loss	Chain Foul-up	NONE
Competent crew	0.02	0.02	0.02	0.02	0.01	0.91
Acceptable crew	0.10	0.10	0.10	0.10	0.10	0.50
Unknown crew	0.15	0.15	0.15	0.15	0.15	0.25

The mooring lines could be inadequate, or poorly set, or the winch fails, or whatever. The anchor windlass might not let out the line fast enough, or malfunction in some fashion. The pumps used to unload the crude oil could malfunction. A very severe problem would be a failure of the vessel's power. But perhaps the most severe problem would be that the vessel tangle its propeller in the chain used to lift the loading hose from the seafloor. For the competent crew, a 91 percent probability of none of the above will happen, but for a unknown crew, there is only a 25 percent that all will go well during the mooring/unloading operations.

**9. TUG AVAILABILITY:** If a tug is required, a simple probability node is used to determine a specific type/cost of tug:

	Tractor	Twin	Single	None
Tug Required (YES)	0.80	0.15	0.05	0.0
Tug Not Required (NO)	0.0	0.0	0.0	1.0

This node is used pending the decision to use a tug.

**10. COST OF TUG ASSIST:** The deterministic cost of operating the tug is included in this node. Depending on the selected tug, the cost is computed:

	Cost
Tractor	\$5,000.
Twin Screw	4,000.
Single Screw	2,000.
None	0.

**11. COST OF LOST TIME:** In order to determine the cost of lost time, the approximate value of \$20,000. per day has been used. Small US-flagged tankers are approximately \$20,000/day, large tankers are about \$25,000./day. Foreign-flagged vessels are less expensive, ranging from 15 to 25 thousand a day. For purposes of this

example, a mean value of \$20,000/day has been used, and the following table of approximate time loss values (in days):

Operational Errors (Time loss in days)					
	Comm.	Judgement	Coordination	Cargo	None
Time Loss	0.25	0.50	0.50	1.50	0.0
Cost	\$5,000.	10,000.	10,000.	30,000.	0.0

**12. COST OF MECHANICAL FAILURES:** The final deterministic node for assessing the cost of a failure includes all of the mechanical problems that could be encountered. This list is not meant to be exhaustive, and the costs are only approximate:

Winch	Anchor	Pumps	Power Loss	Foul-up	NONE
\$45,000.	50,000.	60,000.	100,000.	500,000.	0.0

A foul-up with the chain from the hose/spar buoy is an expensive accident, and has a very low probability of occurrence. All of the mechanical problems are fairly costly, compared to the operational errors.

**13. TOTAL COST:** Total cost is computed as the sum of all three of the deterministic nodes, including tug assist, lost time and mechanical failures. For this simplistic model, no additional cost of mopping up spilled oil has been included, only the direct costs associated with the berthing of the vessel.

## MODEL RESULTS

At least two different analyses can be performed with this INDIA decision model. The first is to calculate the resultant probability versus cost curve, resulting from the normal execution of the program. Figure 2 provides the resultant cumulative probability curve, plotting dollars (cost) versus cumulative probability. As can be clearly seen from the initial step function behavior, there is a very high probability that no cost (financial loss) will be incurred.

A second use of the model is to perform a series of sensitivity analyses. There are three (3) initial probability nodes, without any successors, that can be separately processed to perform sensitivity analyses. The INDIA program will use one of these initial probability nodes, and calculate its influence on the final result. For example, using the "current conditions" (node 1) results in the cost versus current plot of Figure 3. Figure 4 provides sensitivity results for vessel size versus cost. Larger vessels require tug support, and tug support reduces the probability of an accident. Figure 5 provides results for the crew competence versus cost.



Clearly, the crew is the critical element, and having an unknown crew (no experience at this location, unknown crew to the harbor pilot) is the most critical element.

Having both the overall model results and the sensitivity results from the three independent, initial probability nodes yields significant insight. First, the sensitivity analysis indicates that the results are most sensitive to the crew competence. Thus, the study provides important information to regulators as to which parameter should be most carefully monitored. Vessel size and current uncertainty are not as important in the determination of the final resultant costs. The overall model results indicate that there is a high probability that no costs, or no errors will be encountered most of the time, and if a mishap occurs, it will be relatively inexpensive. There is a less than 20 percent chance that a mishap will result, with a major financial impact.

This type of model can be easily constructed in a few hours, and the same type of steps and procedures can be applied to a broad range of decision analyses. The primary goal of this paper is to illustrate how easily an influence diagram can be created, and the types of insight and understanding that can be obtained.

## REFERENCES

Clemen, Robert T. "Making Hard Decisions: An Introduction to Decision Analysis", PWS-Kent Publishing Company, Boston, MA 1991.

"Management of Human Error in Operations of Marine Systems", Final Joint Industry Project Report, by W. H. Miller and R. G. Bea, Report No. HOE- 93-1, March 1993, Department of Naval Architecture & Offshore Engineering, University of California, Berkeley.

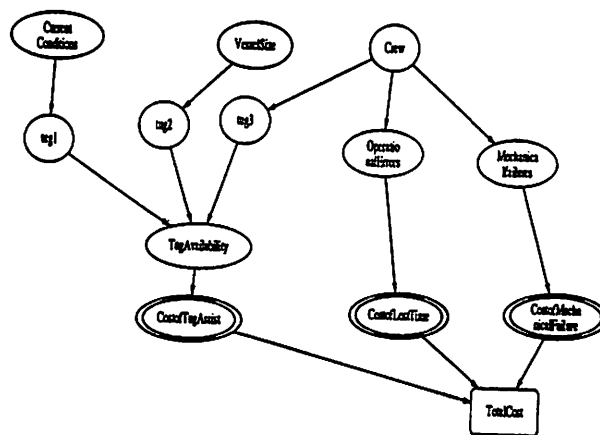


FIGURE 1. Overall Influence Diagram (INDIA) of the Decision Model

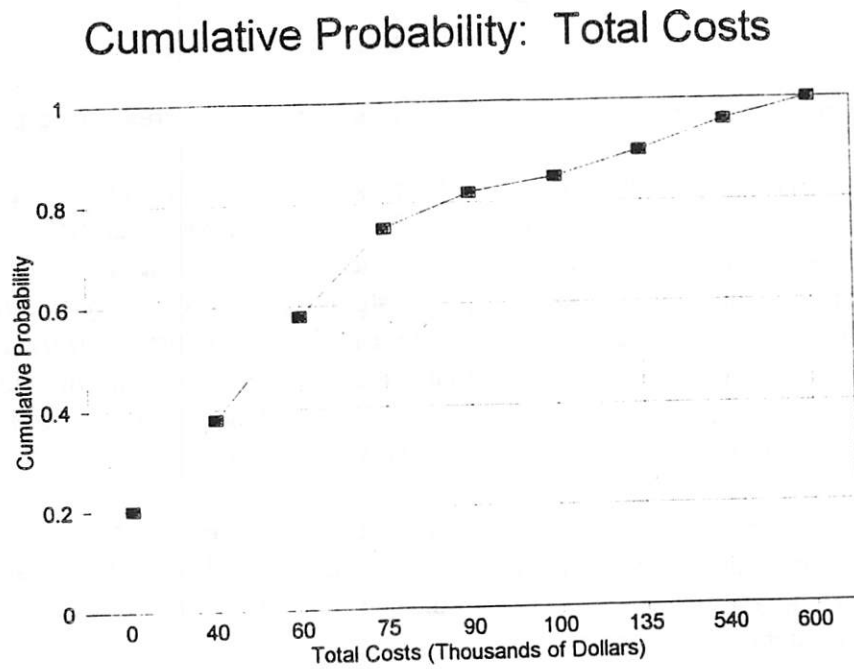


FIGURE 2. Cumulative Probability versus Total Cost

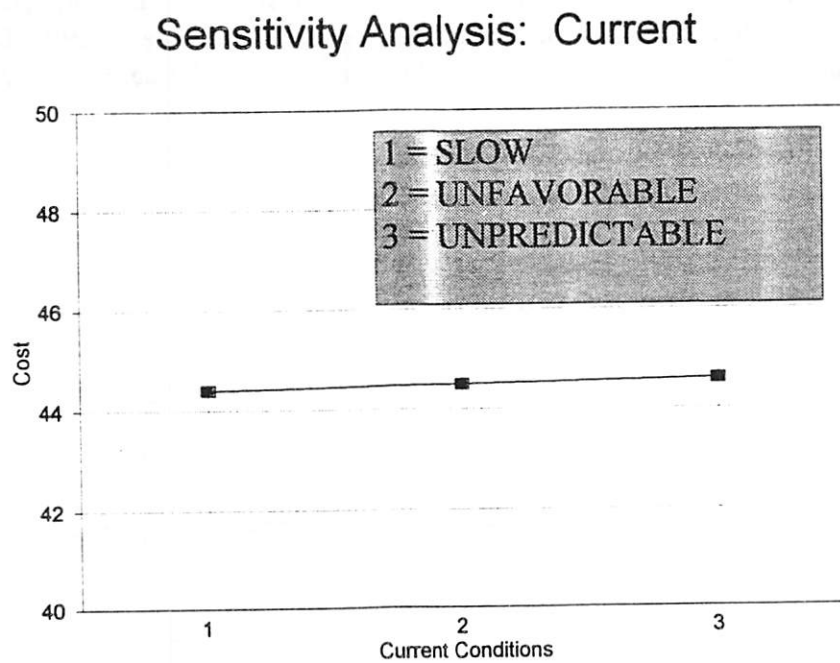


FIGURE 3. Sensitivity Analysis: Current versus Total Cost

### Sensitivity Analysis: Vessel Size

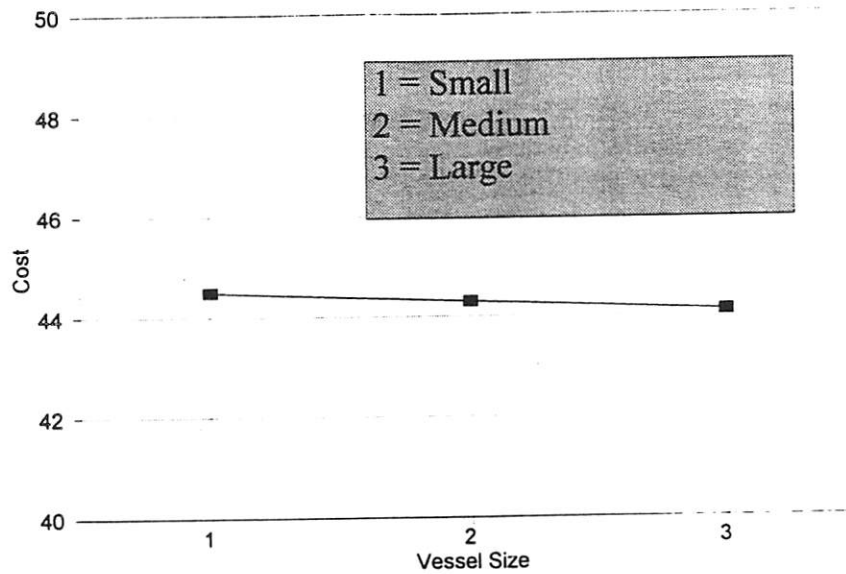


FIGURE 4. Sensitivity Analysis: Vessel Size versus Total Cost

### Sensitivity Analysis: Crew Competence

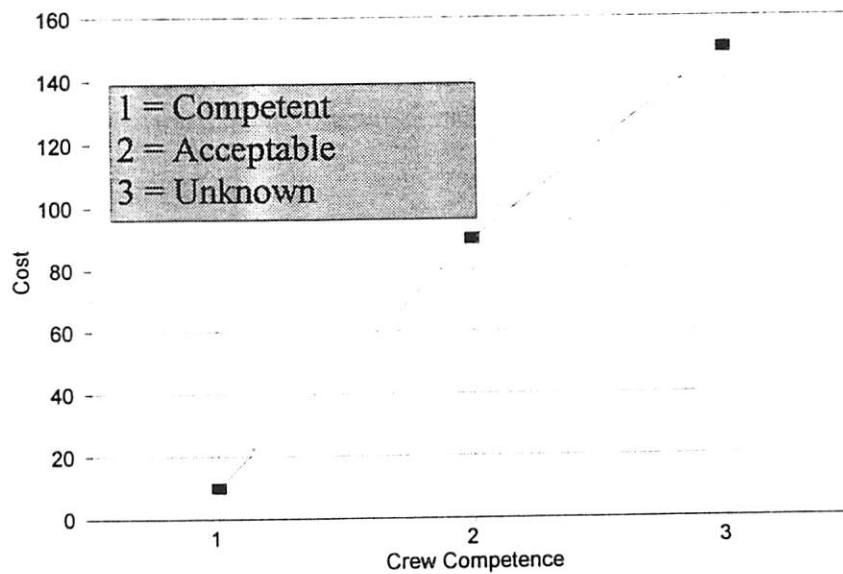


FIGURE 5. Sensitivity Analysis: Crew Competence versus Total Cost

**093 Time Dependence of Equipment Failure Rates--  
Models, Data, and Impacts on System Modeling**  
*Chair: D. Bley, PLG*

**On a Class of Dependent Failures**

*I. A. Papazoglou (National Center for Scientific Research, Greece)*

**Statistical Treatment of Time and Demand-Related Failures in the Nordic Reliability Data  
Book (T-Book)**

*K. Porn (Studsvik Eco & Safe)*

**Derivation of Time Dependent Component Unavailability Models and Application to  
Nordic PSAs**

*M. Knochenhauer (Logistoca Consult.); G. Johanson (Ind. Process Safety)*

## ON A CLASS OF DEPENDENT FAILURES

Ioannis A. Papazoglou

Institute of Nuclear Technology-Radiation Protection  
National Center for Scientific Research "Demokritos".  
Aghia Paraskevi, 153-10, Greece

### INTRODUCTION

The objective of this paper is to present the capabilities of Markov models in modeling a wide range of dependent failures important in RAM analyses. Reliability analyses of systems begin with the establishment of logic models such as event trees, fault trees and cause-consequence graphs. These models are not only essential for the qualitative identification of the reliability characteristics of a system (e.g. cut sets) but they can be also quantified for obtaining quantified reliability performance measures like failure probability, mean time to failure and so on. This quantification is adequate as long as the stochastic characteristics of the components are *static* or when they do not depend on the state of other components or of the system. When, however, the stochastic behavior of the components exhibits a dynamic behavior and in particular when this dynamic behavior is due to a dependence of its stochastic characteristics on the state of other components and/or the state of the system which change with time, then the static logic models should be complemented by special techniques for the quantitative evaluation of various reliability measures. Markovian analysis is especially suited for modeling dynamic dependences affecting both the failure and the repair characteristics of components. This paper, however, addresses only failure dependences.

Dynamic dependences affecting the failure rates are present in the case of components operating under cold or warm standby, when sharing common loads and the failure rate depends on the level of the load undertaken by each component, and finally a special class of common mode and common cause failures. It is demonstrated that when the latter class of dependent failures characterizes the components of a parallel system, an  $N+1$  parallel system is not always better than an  $N$  parallel system.

## THE TWO-COMPONENT SYSTEM PARADIGM

The theory of Markov processes<sup>1</sup>, the application to reliability analysis<sup>2,3</sup>, and methods for analysis of large systems<sup>4,5</sup>, are given in the literature. Here the discussion will be confined on a two component system to demonstrate the capabilities of Markov models in modeling dependences that affect the failure characteristics of components.

Let us consider a two-component parallel system consisting of components A and B. with the state transition diagram given in Fig. 1.

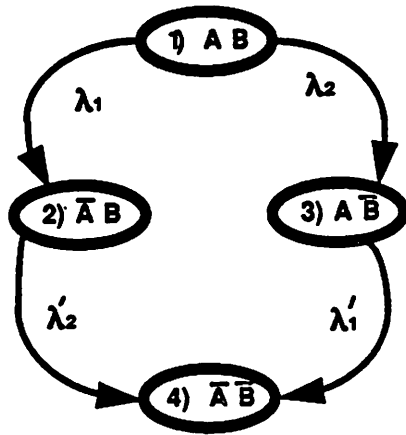


Fig. 1. State transition diagram for a 2-component system.

There are four states for the system, states 1, 2, and 3 being operating states and state 4 being a failed state. Transitions from state 1 to state 2 and from state 2 to state 4 are caused by failure of component A while transitions from state 1 to state 3 and from state 2 to state 4 are caused by failure component B. State transitions {1→2} and {3→4} although caused by the failure of the same component are not necessarily occurring at the same rate. This is because failure of component A when the system is in state 1 occurs while component B is operating while the same failure when the system is in state 3 occurs while component B is failed. Operation of component B might affect positively or negatively the operation of

component A and hence the corresponding failure rates are not necessarily the same ( $\lambda_1 \neq \lambda'_1$ ). Similar remarks can be made about component B ( $\lambda_2 \neq \lambda'_2$ ).

Solving the model of Fig. 1 for the state probability of state 4, which is the failure probability of the system,  $F(t)$ , and setting for mathematical simplicity  $\lambda'_1 = \lambda'_2 = \lambda_3$ , yields

$$F(t) = 1 - \frac{\lambda_2}{\lambda_3 - (\lambda_1 + \lambda_2)} \exp[-(\lambda_1 + \lambda_2)t] + \frac{\lambda_1 + \lambda_2}{\lambda_3 - (\lambda_1 + \lambda_2)} \exp[-\lambda_3 t] \quad (1)$$

Specific cases where such dependences can be manifested include the following:

### Cold Standby Redundancy

In cold standby the non operating component is not subject to any stress and hence it cannot fail. Assuming that the failure rate of the operating component is  $\lambda$  and the at time zero component A is operating eq. (1) yields ( $\lambda_2 = 0$ ,  $\lambda_3 = \lambda_1 = \lambda$ )

$$F(t) = 1 - (1 + \lambda t) \exp[-\lambda t] \quad (2)$$

### Warm Standby Redundancy

In warm standby the non operating component is assumed to fail at a reduced rate than that of on-line operation. Again assuming that component A is operating at time zero and setting  $\lambda_1 = \lambda_3 = \lambda$  with  $\lambda_2 < \lambda$  eq. (1) yields

$$F(t) = 1 - \left(1 + \frac{\lambda}{\lambda_2}\right) \exp[-\lambda t] + \frac{\lambda}{\lambda_2} \exp[-(\lambda + \lambda_2)t] \quad (3)$$

### Components sharing Common Loads

If the failure of a component depends on the "load" under which is operating then failure of components sharing a common load increase the load on the remaining operating components with a corresponding increase in the failure rate. In the two-component system when both components are operating each is assuming 50% of the load while when one of the two fails the remaining assumes 100% of the load. In this case,  $\lambda_1 = \lambda_2 = \lambda$  with  $\lambda_3 > \lambda$ , and eq (1) yields

$$F(t) = 1 - \frac{2\lambda}{2\lambda - \lambda_3} \exp[-\lambda_3 t] + \frac{\lambda_3}{\lambda_3 - 2\lambda} \exp[-2\lambda t] \quad (4)$$

### Static Logic Model Solution

A static model like a fault tree or an event tree would evaluate the failure probability of two-component system as

$$U(t) = Pr\{\bar{A} \cdot \bar{B}\} = Pr\{\bar{A}\} \cdot Pr\{\bar{B} / \bar{A}\} \quad (5)$$

None of the equations (1) through (4) can be deduced from eq (5). For example, eq. (5) can only bracket the correct solution provided by eq. (2) between

$$U_1(t) = 1 - 2 \exp(-\lambda t) + \exp(-2\lambda t) \quad (6)$$

if the standby is considered hot ( $\lambda_2 = \lambda$ ), and

$$U_2(t) = [1 - \exp(-\lambda t)] [1 - \exp(-\lambda_2 t)] \quad (7)$$

if it is assumed that component B always exhibits a reduced failure rate  $\lambda_2$ .

### SYMPATHETIC FAILURES

The concept of dependent failures of redundant components sharing the same load can be extended to include an interesting class of common failures. Traditionally dependent failures are treated in reliability analyses under the terms "common cause" or "common mode" failures. Various models have been developed for handling these dependent failures<sup>6,7</sup> (see also references in section three of 6). All these models, however, are based explicitly or implicitly on the assumption that given a group of N components connected in parallel, there is a common event that simultaneously may cause the failure of all N components. Differences are then focused on the modeling of this common event and its relationship with the failure rate of each component. All the models, nevertheless, eventually propose an upper limit for the reliability of the redundant system controlled by the rate of occurrence of the common cause of failure. As a consequence a system with N+1 redundant components will be always more reliable than a system with N components.

There exists, however, another very important class of dependences that reduce the reliability of redundant systems. It includes all situations in which the failure of one component can cause the failure of other redundant components of the system. An example of such dependences was given above in the case of components sharing a common load. There are situations in which the increase of the failure rate of the remaining components following the shock of a single component failure is so high that, for all practical purposes the remaining components fail instantly. This kind of failure can be called "sympathetic".

Sympathetic failures occur when the failure of a component creates phenomena generating stresses that challenge the strength of the remaining operating components. For example, the failure of a generating station in an interconnected network, challenges the frequency stability of the whole network and could result in a blackout. Similar phenomena can occur in redundant transmission lines, diesel generators, channels of various logic circuits, redundant legs of fluid systems, structural supports etc. A valve can fail and spray with water the electrical controls of nearby valves. Sympathetic failures can also happen indirectly through human errors. For example, a failure in one of a number of redundant components may trigger a repair action which may be inadvertently applied to an operating component causing its unavailability. Such failures have been actually observed.<sup>8</sup>

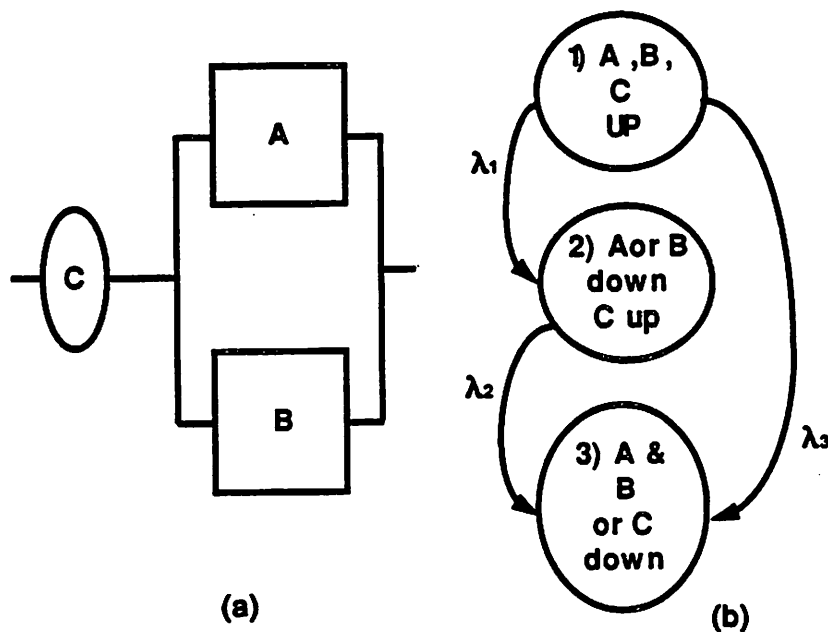


Fig. 2. Two-component redundant system subject to external common cause failures: (a) Block diagram; (b) Corresponding state transition diagram.

Common cause failures can be incorporated in Markovian as in other models by assuming a dummy component connected in series with the redundant components (see Fig. 2a). Whenever component C fails — whenever the common cause event occurs — the system fails. The common cause event may occur when either both or only

one component is operating. This model can be extended in systems comprising N parallel components.

Sympathetic failures can be incorporated in Markov models as follows. The state transition diagram of the two-component system of Fig. 2a is presented in Fig. 2b. There are three merged states: a) the first state corresponds to the state where both components A and B are operating and the external common shock has not occurred; b) the second state contains states with either component A or B has



failed and the common external shock has not occurred; c) the third state contains all the states that include the occurrence of the external event or that both components A and B have failed. Assuming that the external shock follows the "β-factor" model<sup>6</sup>, and that this is the only dependence in the system the failure rates in the state transition diagram become:

$$\lambda_1 = (1 - \beta)\lambda, \quad \lambda_2 = \lambda, \quad \lambda_3 = \beta\lambda \quad (8)$$

Incorporation of the sympathetic failures is possible by assuming that a portion ( $\omega$ ) of the individual component failure will cause the failure of the other component too. Or in other words that the individual failure of one component, say A, will cause the failure of the other component with probability  $\omega$ , while it will not affect the other component with probability  $(1 - \omega)$ . In that case the transition rates in the transition diagram of Fig. 2b become

$$\lambda_1 = (1 - \beta)(1 - \omega)\lambda, \quad \lambda_2 = \lambda, \quad \lambda_3 = \beta\lambda + (1 - \beta)\omega\lambda \quad (9)$$

These considerations can be generalized to an N-component system with a transition diagram consisting of N+1 states. State 1 contains all N components operating and the external event has not occurred, state I contains (N+1-I) operating components and the external event not having occurred, and state N+1 contains either no operating component or the external event having occurred. The transition rates  $\alpha_{ij}$  between any two states I and J are then given by

$$\alpha_{ij} = \begin{cases} (N+1-I)(1-\beta)(1-\omega)\lambda & \text{if } J = I+1 \\ (N+1-I)[\beta + (1-\beta)\omega]\lambda & \text{if } J = N+1 \\ 0 & \text{otherwise} \end{cases} \quad (10)$$

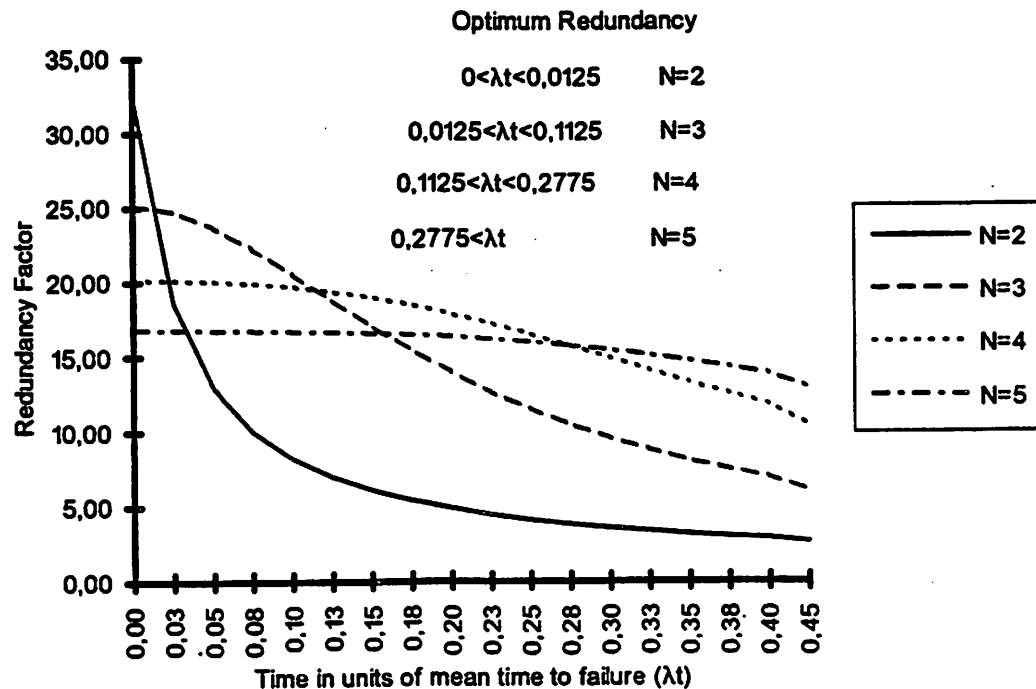
where  $\lambda$  is the total failure rate of a single component.

Solution of the model implied by eq (10) yields for an m-out of -n parallel system a failure probability of

$$F_n^m(t) = 1 - \left( \sum_{j=0}^{n-m} \binom{n}{j} \left\{ (1-\omega)[1 - \exp[-(1-\omega)\lambda t]] \right\}^j \left\{ \exp[-(1-\omega)\lambda t] \right\}^{n-j} \right) \exp(-\beta\lambda t) \quad (11)$$

The importance of sympathetic failures lies in the fact that in their presence an (N+1)-component system is not necessarily more reliable than an N-component parallel system. Indeed this is demonstrated in Fig. 3 where the ratio of  $F_1^1(t)$  over  $F_n^1(t)$  —the failure probability of a single component over the failure probability of an 1-out-of-n system— is plotted as a function of the composite variable  $(\lambda t)$  for various values of n. It is noteworthy that an 1-out-of-5 parallel system is not always better than an 1-out-of-4 system and so on. The choice of the optimum degree of redundancy depends on the mission time and of course on the specific values of the parameters  $\lambda$  and  $\omega$ .

**Acknowledgement:** The author wishes to thank Dr. Sati Mitra for suggesting the term "sympathetic" failures while they were both working at the U.S. Brookhaven National Laboratory.



**Fig. 3.** Redundancy factor ( $= F_2^1(t) / F_1^1(t)$ ) versus time for various redundant systems.  
 $\beta = 0.01 \quad \omega = 0.01$

## REFERENCES

1. Howard, R. : Dynamic Probabilistic Systems , Vol I & II, Wiley (1971)
2. Lees, F. : Loss Prevention in the Process Industries , Vol 1, Butterworths, Guilford, UK, 1986, Chapter 7.
3. Henley, E. and Kumamoto, H. : Reliability Engineering and Risk Assessment, Prentice-Hall Inc., (1981).
4. Papazoglou, I.A. and Gyftopoulos, E.P. : Markovian Reliability Analysis Under Uncertainty with an Application on the Shutdown System of the Clinch River Breeder Reactor , *Nuclear Science and Engineering* 1980, 73,1
5. Papazoglou, I.A. and Gyftopoulos, E.P. : *IEEE Trans. Reliability* 1977, R-26, 232
6. Mosleh, A., Flemming, K. N., Pazy, G. W., Worledge, D.H., Rasmuson, D.M., "Procedures for Treating Common Cause Failures in Safety and Reliability Studies" EPRI Report NP-5613 and NUREG/CR-4780, 1988
7. Paula, H.M., and Pazy, G.W., "A Cause-Defence Approach to the Understanding and Analysis of Common Cause Failures", NUREG/CR-5460, 1990.
8. Teichman, T., and Papazoglou, I.A., "On the Statistical Relation Between Single and Multiple Component Failures", American Nuclear Society, Transactions-43, November 1982.

## STATISTICAL TREATMENT OF TIME- AND DEMAND-RELATED FAILURES IN THE NORDIC RELIABILITY DATA BOOK (T-BOOK)

Kurt Pörn

Studsvik Eco & Safety  
S-611 82 NYKÖPING  
Sweden

### INTRODUCTION

Since the beginning of 1980's a Reliability Data Handbook (T-book) for components in nuclear power plants of Swedish design has been in use. The main objective of this T-book is to provide failure data for the reliability calculations that are done as parts of the obligatory safety analyses of nuclear power plants. The third version<sup>1</sup> was issued 1992 and was based on operational statistics covering the operation of twelve Swedish and two Finnish nuclear power plants from their commercial start up to and inclusive 1987 - about 110 reactor-years. This amount of experience will be increased by 70 reactor-years in the next edition, to be issued in the middle of 1994.

The operational statistics is primarily based on evaluation of failure reports recorded into the central data bank ATV<sup>2</sup> (nowadays called TUD) and Licensee Event Reports delivered to the Swedish Nuclear Power Inspectorate, as well as information provided by the operation and maintenance staff at each plant. Before the statistical evaluation these raw data are carefully examined with respect to the correctness and consistency. The failures are also classified as being either critical or noncritical. A failure is called *critical* if it stops the function of the component or leads to repair. Only critical failures are considered and included in the T-book.

For the determination of reliability parameters the components are divided into rather homogeneous groups based on their type, operating mode, size and capacity. Nevertheless, there are certainly factors such as environmental, operating and maintenance conditions that make it unrealistic to assume complete homogeneity within the groups with regard to reliability. The similarities, however, are considered so significant that the groupwise treatment is deemed beneficial from the statistical point of view. Thus, in the formulation of the empirical Bayes problem, each component is assumed to be an individual, but related to the other units within the group. The problem is then solved by a hierarchical and robust Bayesian approach.

In previous versions of the T-book the failure modes considered were of two kinds: time-related, for which failure rate  $\lambda$  is of concern and demand-related failures, characterized by failure probability per demand,  $q$ . For the latter group of failure modes one has found, by specific analyses, that the failure mechanisms that are active during the stand-by time very often dominate over the ones at the demand occasion. This phenomenon should motivate the use of a  $\lambda_s$  (failure rate during stand-by) rather than of  $q$ . In reality, there is of course both types of failures. An unavailability model, which takes both types into account, is the so called " $q+\lambda t$ -model".

In the last edition of the T-book<sup>1</sup> this 2D model is used for groups of periodically tested components where different testing intervals have been applied and where the number of demands is relatively well known. In these cases it is possible, by sensitive and appropriate statistical inference methods, to estimate both parameters  $q$  and  $\lambda$  and their uncertainties. After a short presentation of the basic features of the statistical method used in the T-book, this paper describes the  $q+\lambda t$ -model in more detail.

## BASIC STATISTICAL APPROACH IN THE T-BOOK

In parallel with the successive editions of the T-book there has been continuous efforts to improve the methods for the statistical inference required. The statistical reasoning behind the earlier versions of the T-book can be classified as a parametric empirical Bayes (PEB) method. For mathematical convenience, gamma distributions  $g(\lambda|\alpha, \beta)$  were chosen as potential a priori distributions. Then, a unique member of this distribution family was selected by estimating the secondary parameters  $\alpha$  and  $\beta$  on the basis of available operational data. The estimation was made by the use of traditional, frequency-based methods like maximum likelihood and various moment matching methods. The inconsistency hidden in this mixture of Bayesian reasoning and frequency methods as well as the difficulties encountered in the estimation of the secondary parameters led to the development work that has been described by Pörn<sup>3</sup> and has been applied in edition 3 of the T-book.

One important feature of the new approach is the expanded class of potential uncertainty distributions for  $\lambda$ . The expansion is achieved by contaminating the gamma distribution with a "non-informative" part

$$p(\lambda|\theta) = (1-c) \cdot g(\lambda|\alpha, \beta) + c \cdot f(\lambda), \quad (1)$$

where the secondary parameter  $\theta$  stands for  $(\alpha, \beta, c)$ , of which  $c$  denotes the mixing coefficient between the informative distribution  $g(\lambda|\alpha, \beta)$  and the non-informative part  $f(\lambda)$ . The addition of  $f(\lambda)$  just emphasizes the total uncertainty in the tail areas of the distributions, the specification of which is extremely difficult even if a substantial amount of observations were available.

With regard to the quantities  $\theta$ ,  $\lambda$  and the observations  $x$  we assume that the hyperparameter  $\theta$  has a density  $p(\theta)$ , that the component specific parameters  $\{\lambda_i\}$ , given  $\theta$ , are iid with  $p(\lambda|\theta)$ , and given  $\theta$  and  $\{\lambda_i\}$ , that the observed number of failures  $\{x_i\}$  are independent having density  $p(x_i|\lambda_i)$ , independent of  $\theta$  and all  $\lambda$ 's other than  $\lambda_i$ .

Now, because there is uncertainty about which distribution in the expanded class above is most appropriate for the description of our knowledge about  $\lambda$ , the hyperparameter too is uncertain and handled by Bayes' method. Thus, instead of selecting a specific distribution out

of the class, a non-informative a priori distribution  $p(\theta)$  is assigned to  $\theta$  and a posterior distribution  $p(\theta|x)$  is determined based on the observations  $x$ . The distribution  $p(\theta)$ , non-informative according to the *principle of data translated likelihood*<sup>4</sup>, is mathematically derived<sup>3</sup> and approximated with

$$p(\alpha, \beta, c) \propto \left[ \alpha(\alpha + \beta / t_a) \right]^{-1/2} \beta^{-1} c^{-1/2} \quad (2)$$

where the average operation time of the components might be a reasonable choice of  $t_a$ .

Having estimated the uncertainty concerning the hyperparameter  $\theta$  one returns to the uncertainty around the primary parameter  $\lambda$  by the *law of total probability*

$$p(\lambda|x) = \int p(\lambda|\theta) \cdot p(\theta|x) d\theta \quad (3)$$

This generic uncertainty distribution of  $\lambda$ , displayed in the T-book in the form of mean value and some percentiles, is used as a prior distribution in the determination of component and plant specific posterior distributions. The plant specific distributions are discussed in a separate section of this paper.

The *contaminated Bayes' empirical Bayes' method* (CBEB) outlined above has been found to be a consistent, robust and practicable solution to the statistical inference problems in the T-book applications. The distributions provided by the CBEB method are significantly broader than the distributions generated by the earlier PEB approach, where much of the statistical uncertainty is neglected.

## MIXTURE OF TIME- AND DEMAND-RELATED FAILURES

In earlier versions of the T-book the failure modes considered are of two different kinds: time-related, for which failure rate  $\lambda$  is of concern (e.g. spurious stop, spurious opening, short circuit) and demand-related failures, characterized by failure probability per demand,  $q$  (e.g. failure to close, failure to start). For the latter group of components one has found, by specific analyses, that the failure mechanisms that are active during the stand-by time dominate very often over the mechanisms occurring just at the demand occasion. This phenomenon should motivate the use of a  $\lambda_s$  (failure rate during stand-by) rather than of  $q$ . Further, the estimation of  $q$  requires data about the number of demands, consisting of periodical tests and real activations. For some component groups such information is not easy to retrieve. On the other hand, the total stand-by time is always relatively easy to obtain. Therefore, we think it will be an advantage in many cases to treat the  $q$ -failure modes as  $\lambda_s$ -failures. There is also another reason for such a move. The variability of  $q$  for certain groups of components is caused more by variations of the activation interval within the group than by other environmental conditions. By using  $\lambda_s$  this source of variation is eliminated.

Above we made a complete move from  $q$ - to  $\lambda_s$ -failures. In reality, there is of course both types of failures. Therefore a model, which takes both types into account, has to include two primary parameters,  $\lambda_s$  mentioned above and  $q_0$  representing the probability of failure caused by failure mechanisms occurring at the demand occasion. If we, for the sake of simplicity, use the signs  $\lambda$  and  $q$  to denote these unknown quantities, the unavailability  $u(t)$  of such a component at time  $t$  since the last activation can be written

$$u(t) = q + (1 - q) \cdot (1 - e^{-\lambda t}) \quad (4)$$

For sufficiently small values of  $\lambda t$  this unavailability can be approximated by

$$u(t) = q + \lambda t, \quad (5)$$

after which the model is usually named "q +  $\lambda t$ -model".

Now, if the component is activated regularly, with interval T (between the tests) and n times in total suffering x failures, the likelihood can be written (using  $q' = 1 - q$ )

$$p(x|q, \lambda) = [1 - q'e^{-\lambda T}]^x \cdot (q'e^{-\lambda T})^{n-x} \quad (6)$$

The likelihood (6) is applicable to components which have rather few real demands compared with the periodically recurrent tests.

Going to the second stage of a twostage approach, we presuppose a hyperparameter,  $\theta = (\alpha, \beta, a)$ , such that for given  $\theta$  we have

$$p(\lambda|\theta) = g(\lambda|\alpha, \beta) \quad (7)$$

and

$$p(q|\theta) = aq^{a-1} \quad (8)$$

Thus the uncertainties of the primary parameters are tentatively described by classes of distributions that are conjugate with respect to the Poisson parameter  $\lambda$  and the binomial parameter  $q$ .

For given  $\theta$ ,  $q$  and  $\lambda$  are assumed independent on each other, which means that  $p(q, \lambda|\theta)$  can be written as the product of the two densities above. For the sake of simplicity, we have not prescribed any contamination part like the one we introduced in case of only one primary parameter  $\lambda$ . To include contamination, but to avoid an increased number of hyperparameters one could presume a fixed contamination. Utilizing the assumption of independence between  $q$  and  $\lambda$  (for given  $\theta$ ), and the distributions (7) and (8), the likelihood function  $p(x|\theta)$  can be written

$$p(x|\theta) = \sum_{i=0}^x (-1)^i \binom{x}{i} a \frac{\Gamma(a) \Gamma(n - x + i + 1)}{\Gamma(a + n - x + i + 1)} \left[ \frac{\beta}{(n - x + i) \cdot T + \beta} \right]^\alpha \quad (9)$$

Thus we have an explicit expression for the likelihood, for one observed component, in terms of the hyperparameters. For a set of components, the corresponding likelihood is simply the product of likelihoods in (9) with varying values of  $n$ ,  $T$  and  $x$ . Then the final solution rests on the choice of a prior distribution for the hyperparameters.

By the same type of reasoning as in the derivation of the distribution (2) in the 1D case the hyperparameters  $\alpha$ ,  $\beta$  and  $a$  are assigned the non-informative distribution

$$p(\alpha, \beta, a) \propto \left[ \alpha(\alpha + \beta / t_a) \right]^{-1/2} \beta^{-1} a^{-1} \quad (10)$$

Thus there is no difference in the distribution of  $\alpha$  and  $\beta$ , while the new parameter  $a$  is given the a priori distribution  $p(a) = a^{-1}$ , or equivalently, that  $\log(a)$  has a uniform distribution, in accordance with the principle of data translated likelihood.

The "q+ $\lambda$ t-model" does not presume that these two types of failure are distinguished in the empirical data, which in many cases would be very difficult to do. However, for the sake of verification the failure types of some specific component groups have been studied<sup>5</sup> with regard to their time dependence. Then the validity of the pure statistical approach of the 2D "q+ $\lambda$ t-model" has shown to be surprisingly good.

## PLANT SPECIFIC DISTRIBUTIONS

In addition to the generic distributions in the 1D and 2D case outlined above the T-book also provides plant specific uncertainty distributions. The components at a given plant - which are a part of the total statistical material - are still assumed to be individuals, even if they can be expected to be more homogeneous than the generic group as a whole. The plant specific distributions are derived as uniformly weighted posterior distributions, where the latter distributions are based on component specific data and the generic distribution as a priori distribution. It is to be emphasized that a plant specific distribution still describes the uncertainty concerning the failure rate of an individual component - a component that is "typical" for the given plant.

In the 2D case, the plant specific values are characteristics of distributions for  $\lambda$  that are conditioned by a q-value equal to its mean  $E(q)$ . Most of the information about q is obtained from failure statistics representing different testing intervals. By examples it has been shown that the posterior distribution of q is influenced very little by component specific data, which also could be expected as a component represents only one test interval. The same is also valid for plant specific materials, because these very often are quite homogeneous with regard to the test interval. From the generic distribution  $p(q, \lambda | x)$  the mean value  $E(q)$  can be calculated, and conditioned on this mean value the plant specific distributions of  $\lambda$  are displayed in the T-book.

This choice of presentation mode was also dictated by the difficulty to conveniently display multidimensional distributions. In the next edition of the T-book we will supplement the tables with integral values of component unavailability as a function of test intervals, where the uncertainty of q and  $\lambda$  have been utilized through the law of total probability. Such integral values can then become of direct use in the so called *integrated uncertainty analysis*<sup>6</sup>.

If the amount of plant specific data is rather restricted compared with the overall data, the procedure outlined above will result in a plant specific distribution that is rather close to the generic one. Therefore, plant specific distributions can always be chosen for plant specific analyses. Technically, the uncertainty distributions in the T-book, both generic and plant specific ones, can be used as a priori distributions in component specific analyses. Further, if the distributions are stored on a computer medium, they can easily be used in uncertainty analysis where total failure probabilities are needed.

## CONCLUSIONS

The T-book, the handbook of reliability data of components in Nordic nuclear power plants, the statistical approach of which is discussed in this paper, has the purpose to provide

probability distributions  $p(\lambda)$  to describe the uncertainty concerning the failure rate  $\lambda$  of individual components. Likewise, in cases of component groups with different test intervals, the T-book provides characteristics of the 2D distribution  $p(q, \lambda)$ , where  $q$  denotes the probability of failures with demand-related causes. This "q+ $\lambda$ t-model" has shown to be of great interest in the community of nuclear safety analysts, especially in studies of test interval optimization. The distributions have been estimated on the basis of operating data that are systematically collected into a common database from all nuclear power plants in Sweden and two BWRs in Finland.

The concept and treatment of uncertainty in the T-book is founded on a complete Bayesian reasoning. A central feature of the Bayes empirical Bayes method (BEB) described above - and applied to both 1D and 2D probability models - is that it applies to groups of components, where the individual units are not necessarily identical with respect to the model parameters. Instead the relation between the units is expressed by a tentative distribution for the individual failure rates and, in the 2D case, also for the individual demand-related failure probabilities. The choice of this uncertainty distribution, partly describing the population variability, is such that the distribution is flexible enough, that it stresses the uncertainty in areas with little support from empirical evidence, and finally, that the distribution is mathematically tractable.

The method as a whole has been found to be a consistent and practicable solution to the statistical inference problems encountered in probabilistic safety assessment. In the construction of the model more attention has been paid to a relevant description of the uncertainty itself, rather than to any specific point estimate of the parameters. One consequence of this is the robustness of the method, by which we mean its sensitivity to extreme cases, so called outliers.

### Acknowledgements

The author is indebted to the Swedish Nuclear Power Inspectorate for the financial support both of the study described in this paper, and of the work required for the preparation of its presentation.

### REFERENCES

1. T-book. Reliability Data of Components in Nordic Nuclear Power Plants. 3rd ed.. Prepared by the ATV-Office and Studsvik AB. The ATV Office, Vattenfall AB, Vällingby, (1992)
2. K. Ekberg, M. Andersson and J-P. Berto. The ATV-System and Its Use, in: Vol.1, ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, (1985)
3. K. Pörn, On Empirical Bayesian Inference Applied to Poisson Probability Models, PhD Thesis, *Dissertation No. 234*, Linköping University, Sweden, (1990)
4. G.E.P. Box and G.C. Tiao, Bayesian Inference in Statistical Analysis, Addison-Wesley, Reading, Mass., (1973)
5. S-O. Andersson, Analysis of raw data for the T-book with regard to time dependence (in Swedish), Report Vattenfall PT-28/93, Vattenfall AB, Vällingby, (1993)
6. K. Pörn and K. Shen, On the Integrated Uncertainty Analysis in Probabilistic Safety Assessment, in: Safety and Reliability '92, ed. K.E. Petersen and B. Rasmussen, ESRA Conference Series, Elsevier Applied Science, (1992)



## **DERIVATION OF TIME DEPENDENT COMPONENT UNAVAILABILITY MODELS AND APPLICATION TO NORDIC PSA:S**

Michael Knochenhauer<sup>1</sup> and Gunnar Johanson<sup>2</sup>

<sup>1</sup> Logistica Consulting AB  
Domkyrkoesplanaden 5b  
S-722 13 Västerås, Sweden

<sup>2</sup> Industrial Process Safety AB  
Svartviksslingan 11  
S-161 29 Bromma, Sweden

### **INTRODUCTION**

During the last 10 years, a number of Nordic research projects have had the common aim of improving the capability of current Nordic level 1 PSA:s to serve as tools for risk evaluation and decision support. Specifically, the projects have addressed the evaluation of Technical Specifications and the development and utilization of the living PSA concept. A problem that has received much attention is the correct estimation of component unavailability, including time dependent aspects of component and system unavailability.

Thus, the reliability of motor operated valves (MOV) in standby safety systems has been analysed. The analyses concerned the coverage and representativity of testing, and the time dependence of MOV reliability. Based on analysis of failure reporting, parameters for a time dependent unavailability model could be derived for MOV:s.

Following this pilot project, the latest update of the Nordic Reliability Data Book has derived and presented time dependent failure data for a number of crucial components in standby safety systems.

Finally, in an ongoing project, the time dependent component model has been further refined, and a number of full scale living PSA applications have been carried out for a Swedish BWR.

This paper will give an outline of the analyses performed to generate and use time dependent unavailability models for stand-by components,

### **ANALYSES OF MOTOR OPERATED VALVES**

Within the joint Nordic research project NKA/RAS-450 "Optimization of Technical Specifications Using Probabilistic Methods"<sup>1</sup>, a number of analyses dealt with the problem of deriving realistic failure data for motor operated valves (MOV) in standby safety systems. The three main areas of concern were:

- Coverage of testing
- Applicability of test failure data at real demands
- Time dependence of MOV reliability

Figure 1 summarizes the problems encountered in testing stand-by components and in deriving reliability parameters based on the outcome of these tests.

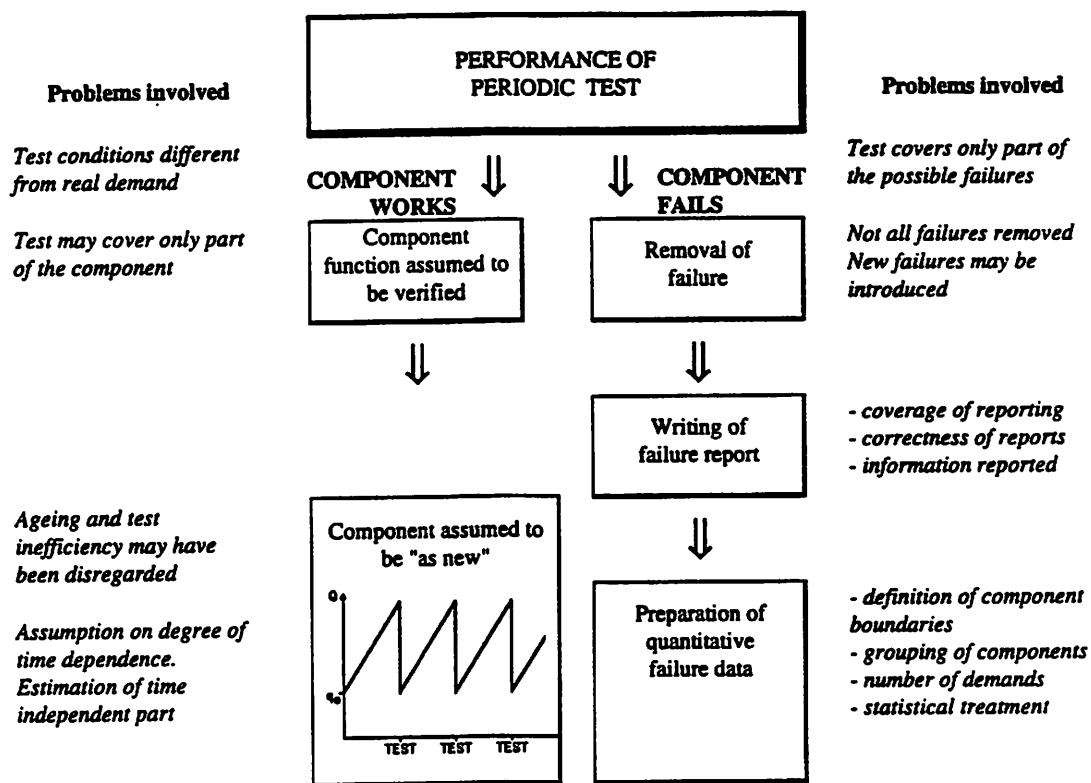


Figure 1. Problems involved in testing stand-by components and in deriving reliability parameters

### Time dependence of MOV reliability

Component data estimates for Nordic PSA:s are to a large extent based on a common failure reporting system (ATV), covering all Swedish nuclear power plants and Finnish BWR:s (14 plants). The ATV data base has been extensively used for deriving component failure data for vital components. A Nordic Reliability Data Book<sup>2</sup> is published every three to five years and has been used extensively in Nordic PSA work. Early editions of the book presented only mean failure probabilities for stand-by components; this was increasingly seen as a short-coming.

The analysis of the time dependent unavailability of stand-by MOV:s was based on failure reports in the ATV data base. The main objective of the analysis was to demonstrate in a pilot project how and to what extent existing failure reporting can be used to derive time dependent reliability characteristics for stand-by components. MOV:s were studied because they comprise a high number of components with a low degree of inter-plant variation with respect to design, operating conditions and preventive maintenance program.

The time dependent component unavailability is assumed to be described by

$$q(t) = q_0 + \lambda_s(t-TL) \quad (1)$$

where  $q_0$  is the time-independent failure probability,  $\lambda_s$  the standby failure rate, and TL the time for the latest test. More generally, TL represents any time point when a latent failure could have been detected. This can be at a surveillance test, at preventive maintenance or at a real demand.

The analysis covers a total of 78 plant years/ 3300 valve years, during which period about 110 critical failures were reported. In the analysis, the valves were divided into groups according to their test interval (TI); TI=3 days, 2 weeks, and 1, 3 and 12 months. Failures were classified according to criticality, failure cause, and time of detection (operating year or revision period). For the test interval 12 months, there is a concern, that the number of failures may have been underestimated. The reason for this is that the total number of failures reported during the plant refuelling outage is very high, and that failures detected in periodic testing cannot be positively identified.

The main result of the analysis, i.e. the MOV unavailability as a function of test interval length based on all plants is shown in figure 2. The straight line is a least square fit to the unavailability points, described by the formula  $q(t) \approx 1.4 \cdot 10^{-4} + 2.8 \cdot 10^{-6} \cdot t$ .

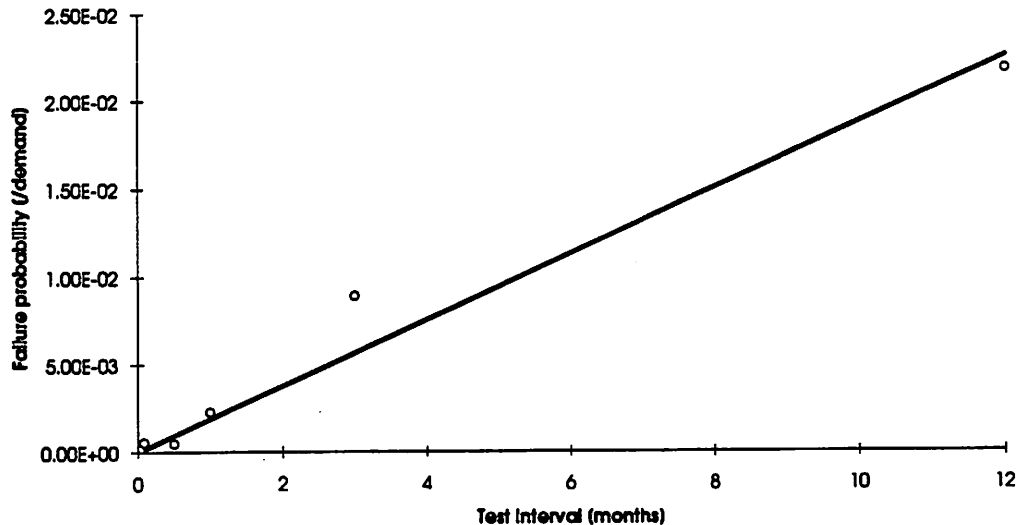


Figure 2. Plot of the unavailability of MOV:s as a function of test interval length

### Validation of Results

The results and conclusions from the data analyses are sensitive to a number of factors. As some of these may have considerable influence, some further comments will be given, based on conclusions from the projects described in this paper.

**Analysis Method.** In the MOV analysis, it was tried to validate the least square fit results by grouping the failures that had occurred into time dependent and time independent, and deriving time dependent parameters based on the resulting size of these groups. The results were inconclusive, partly due to lack of information in the written failure descriptions and partly because many failures have characteristics that appear to involve both time dependent and time independent elements.

**Failures Per Valve Year.** To get a measure of the effects of differing test intervals without involving the number of activations, the number of failures per valve year was calculated for each of the groups of MOV:s. The result was:

- $2.6 \cdot 10^{-2}$  failures/valve year for TI=1 month
- $4.2 \cdot 10^{-2}$  failures/valve year for TI=3 months
- $4.4 \cdot 10^{-2}$  failures/valve year for TI=12 months

In conclusion, there seems to be a correlation between number of failures per valve year and test interval length. The results also indicate that the total number of failures with test interval 12 months may have been under-estimated.

**Plant Level Results.** When comparing the MOV unavailability of different plants, a definite common tendency in the time dependence was found, while the mean unavailability differed considerably. It was also concluded, that these variations are partly due to differences in reporting practices.

**BWR Generation (Ageing).** The plants represent three generations of ABB Atom BWR:s. A comparison of mean unavailability and of time dependence yields the result, that older plant generations have higher mean unavailabilities than newer ones, but that the time dependence (i.e.

the slope of the  $q_0 + \lambda_s t$  line) is not significantly different.

**Plant Systems.** The systems analysed were the auxiliary feedwater system, the emergency core cooling system, the residual heat removal system, and the shutdown cooling system. No significant differences in MOV unavailability could be identified.

**Valve Dimensions.** In previous versions of the Nordic Reliability Data Book, MOV:s were grouped according to valve dimension. Therefore, a comparison with the same grouping was made based on the present data. No significant differences in MOV unavailability could be identified.

**Test Inefficiency.** The unavailability model used in the MOV analysis assumes the component is "as new" after testing. This disregards test inefficiency. Measures of test inefficiency are extremely hard to derive from failure data and therefore usually disregarded. In an analysis of diesel generator data<sup>4</sup>, 1% of the failures could be attributed to test inefficiency; this was shown to correspond to 31% of the diesel generator unavailability.

**Time Dependence of Common Cause Failures.** In living PSA applications, time dependent CCF:s of redundant components must be modelled. The choice of approach will have decisive influence on the level of system unavailability. In NKS/SIK-1 applications, it was assumed that CCF phenomena have the same time dependence as single failures.

### The Nordic Reliability Data Book

After the conclusion of the NKA/RAS-450 project, a third edition of the Nordic Reliability Data Book (1992)<sup>2</sup> has been issued. This edition presents time dependent unavailability parameters for components in standby safety systems. The parameters presented are  $q_0$  (time independent failure probability),  $\lambda_s$  (stand-by failure rate), and  $\lambda_d$  (runtime failure rate). The following are examples of component groups included in the data book:

- Centrifugal pumps
- Reciprocating pumps
- Pneumatical isolation valves
- Check valves
- Motor operated control valves
- Safety valves
- Diesel generators
- Gas turbines

### Derivation of Living PSA Component Models

The ongoing Nordic Project NKS/SIK-1, "Safety Evaluation"<sup>5</sup> has defined and demonstrated the use of living PSA (LPSA) for safety evaluations and for identification of improvements in operational safety.

In this project, routines and procedures of how to utilize LPSA are demonstrated in case studies. The demonstrations include applications such as planning of surveillance tests and test schemes, maintenance planning, optimization of limiting conditions of operation and risk control of exemptions from Technical Specifications.

Often, "living PSA" simply means that a PSA is kept up to date with plant changes. Here, a much wider definition is used. Thus, LPSA implies making use of the dynamic properties of a PSA to assess, monitor and follow up plant risk. The modification of static component and system models into dynamic ones is the main effort to be carried out in the development of a basic LPSA model.

In table 1 key features of the LPSA approach as covered in the Safety Evaluation project are summarized.

In an LPSA model, all observations, such as maintenance and repair should be included and easily updated in order to reflect changes in component configuration. This requires an extensive and flexible component model<sup>6</sup>. The basic model used in the project, is an extension of the component model used in the Nordic Reliability Data Book, including unavailability due to test and repair, and with the possibility to model periodic testing. The model should account for the fact that some failures cannot be detected in tests, but will only manifest themselves at a real demand. A

general model, covering all combinations of time-dependent and time independent failure modes, detectability with respect to both modes, etc. is difficult to create, and even more difficult to apply.

Figure 3 describes the model. TI is the test interval, TR the average repair time, TPM the average (scheduled) preventive maintenance time, and TPMI the average preventive maintenance interval. The risk impact from the hidden and evident unavailability is controlled in different ways:

- Hidden unavailability is controlled by optimization of test intervals
- Evident unavailability is controlled by optimization of allowed outage times (AOT)

Table 1. Living PSA as studied in the NKS/SIK-1 project

	Long term risk planning	Risk planning of operational activities	Risk analysis of operating experience
<b>Approach</b>	Risk assessment	Risk monitoring	Risk follow-up
<b>Result</b>	<ul style="list-style-type: none"> <li>• Identification of risk contributors.</li> <li>• Comparison of alternative designs and procedures</li> </ul>	<ul style="list-style-type: none"> <li>• Test and maintenance planning.</li> <li>• Evaluation of TechSpecs</li> <li>• Operational decision making</li> </ul>	<ul style="list-style-type: none"> <li>• Analysis of operating experience.</li> <li>• Feedback of operational risk experience.</li> <li>• Verification of PSA models.</li> </ul>
<b>Risk measure</b>	Nominal risk. Baseline risk	Instantaneous risk	Retrospective risk Probabilistic indicators
<b>Objective</b>	To continue the risk assessment process started with the basic PSA by extending and improving the basic model and data to provide a general risk evaluation tool for analyzing the safety effects of changes in plant design and procedures.	To support the operational management by providing means for searching optimal operational, maintenance and testing strategies from the safety point of view. The results shall provide support for risk decision making in the short term or in the planning mode.	To provide a general risk evaluation tool for analyzing the safety effects of incidents and plant status changes. The analyses are used to identify possible high risk situations, rank the occurred events from the safety point of view and get feedback from operational events for the identification of risk contributors.

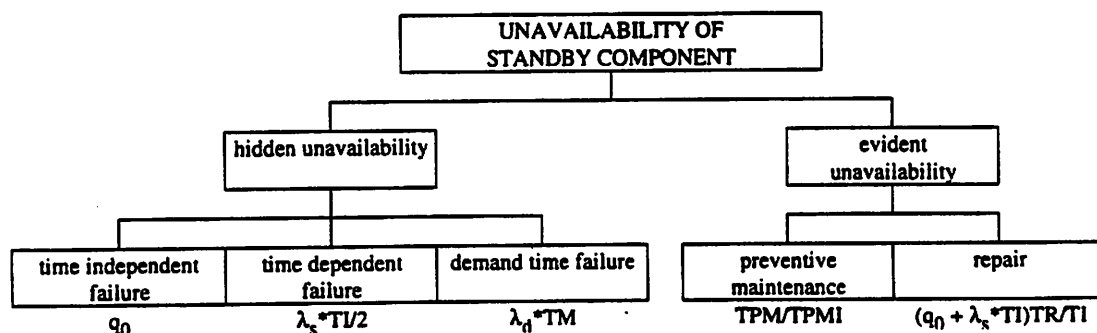


Figure 3. A standby component unavailability model

In a number of demonstration case studies, an LPSA model for the Oskarshamn 2 BWR has been developed and evaluated<sup>7</sup>. Time dependent component models were introduced and updated with data from the Nordic Reliability Data Book. Figure 4 shows the variations of the plant risk level over one operating year with the existing test scheme. The risk measure is the relation between the instantaneous risk  $f(t)$  and the baseline risk  $f_0$ . By making systematic use of time dependent component data and risk importance measures, the number of tests could be reduced by 43% without increasing the average risk.

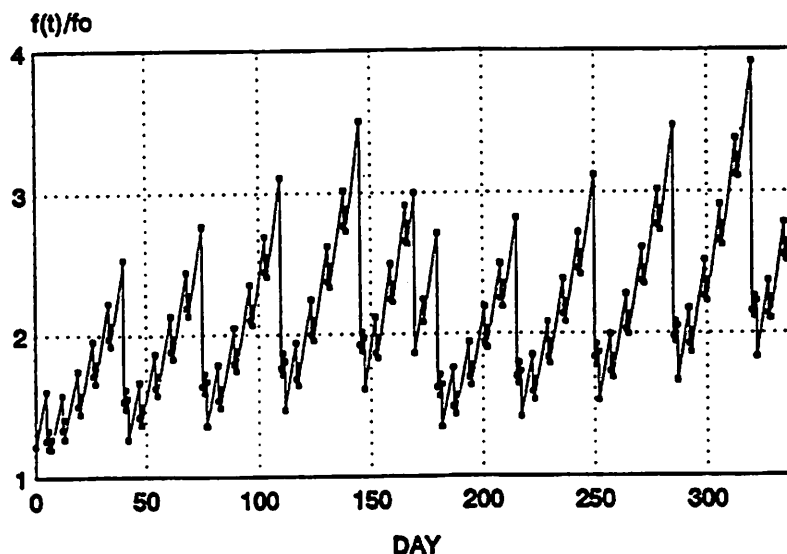


Figure 4. Evaluation of test intervals for Oskarshamn 2 BWR

## ACKNOWLEDGEMENTS

The projects described in this paper are part of a long-term research program of the Swedish Nuclear Power Inspectorate (SKI), aiming at the evaluation and development of methods for safety analysis and decision making in safety related matters. The work described has been performed with the financial support of the Swedish Nuclear Power Inspectorate.

## REFERENCES

1. K. Laakso, M. Knochenhauer, T. Mankamo, and K. Pörn, "Optimization of Technical Specifications by Use of Probabilistic Methods -- A Nordic Perspective", Nordic Liaison Committee for Atomic Energy (NORD 1990:33).
2. "T-book, Reliability Data Book for Components in Nordic Nuclear Power Plants", Version 3 (1992). Prepared by the ATV Group and Studsvik AB.
3. M. Knochenhauer, Pilot project on valve data analysis. ABB Atom Report RPC 88-59, Report NKA/RAS-450S(88)3 1988.
4. T. Mankamo, Test strategies for standby diesel generators. SKI research program "Defence against CCF", pilot study for diesel generators. Draft report.
5. K. Laakso, G. Johanson, S. Björe, R. Virolainen and L. Gunsell. NKS/SIK-1 Safety evaluation by use of living PSA and safety indicators. Work plan 1990-93. Report NKS/SIK-1(90)8. Espoo 1990.
6. J. Holmberg, G. Johanson and I. Niemelä. "Risk Measures in Living PSA Applications". VTT Publication 146. Technical Research Centre of Finland. Espoo 1993.
7. J. Sandstedt, Demonstration case studies on Living PSA. SKI Technical Report 93:33, (Report NKS/SIK-1 (92)27), (August 1993).

**094 Applications of Human Reliability Analysis**

*Chair: D.I. Gertman, INEL*

**HRA for Explosive Ordinance Disposal**

*L.N. Haney, R.G. Peatross, D.I. Gertman (INEL)*

**Nuclear Case Study for A SGTR Sequence**

*D.I. Gertman, W.J. Reece, M.B. Calley, C.L. Smith (INEL)*

**Insights into Pilot Situation Awareness Using Verbal Protocol Analysis**

*H. Blackman, C. Sullivan, K. Seidler (INEL)*

## **HRA FOR EXPLOSIVE ORDINANCE DISPOSAL**

Lon N. Haney, Rodney G. Peatross, and David I. Gertman

INEL/EG&G Idaho Inc.  
P.O. Box 1625  
Idaho Falls, ID 83415-3855

### **ABSTRACT**

This study presents the use of human reliability analysis (HRA) to support the characterization and failure rate quantification of activities associated with gunnery range ordinance disposal. The accident sequence evaluation program (ASEP) nominal HRA technique for pre-accident activities was used to estimate the human error probabilities (HEPs). Four major task groupings were identified and analyzed. They consist of the following: detection of ordinance by a walking ground search, safe excavation of ordinance, ordinance characterization, and use of explosives in ordinance disposal. A subject matter expert participated in the study and recovery factors were modeled according to ASEP procedures. Findings are discussed in terms of the usefulness of an ASEP job performance aid applied during the course of the study and the ability of the ASEP approach to support HRA for DOE facilities.

### **INTRODUCTION**

In the 1940s a gunnery range was contained within the current boundaries of the Idaho National Engineering Laboratory (INEL). The range was used to determine the efficacy of various munitions for the U.S. armed forces. To this day unexploded projectiles remain, some which are partially exposed and others completely below ground level. INEL is in the process of implementing new environmental programs that will result in the construction of new facilities at various locations. Because of the lack of information available regarding the disposition of ordinance in certain areas of the site, i.e., their presence and potency, a program has been undertaken regarding identification and disposal of the explosive ordinance. As part of this effort, EG&G's chemical and radiological risk assessment unit and human factors and system analysis unit conducted a limited scoping study of important human errors for a technique being used at the site for explosive ordinance disposal.



## **METHOD**

### **Scope**

A limited scope analysis requires that human error estimates be determined for relatively high level tasks. The goal of this analysis was to support emerging DOE requirements in the areas of human factors and human reliability analysis present in DOE Order 5480.23 (1990) for important aspects of proposal ordinance disposal activities without completely decomposing the activities into their discrete subtasks. The Accident Sequence Evaluation Program (ASEP) (Swain, 1987) nominal human reliability analysis (HRA) technique for pre-accident tasks was selected as a method of estimating human error probabilities (HEPs) for the activities identified. ASEP was chosen because it can provide conservative error estimates of high level tasks given minimal task decomposition. The analysis was accomplished with the assistance of a subject matter expert (SME) for the ordinance disposal activities. ASEP was used to provide scoping type estimates as opposed to performance of a resource intensive, detailed HRA (Procedures for indepth HRA may be found in Swain and Guttman, 1983).

### **Procedure**

Discussion with the subject matter expert was used to characterize the ordinance disposal activities and obtain details relevant to estimation of errors of interest using ASEP. Important steps and relevant details were determined for each of the following activities: visual sweep, geophysical survey, ordinance excavation, ordinance characterization, and disposal of ordinance by using explosives. The geometry of walking search lines including placement of trained supervisors and searchers is specified. Geophysical survey includes use of metal detection equipment. Excavation of buried ordinance is performed with heavy equipment for deeply buried ordinance and hand tools are used within the last two feet of depth. During excavation a metal detection survey is specified prior to every two feet of depth excavated. Ordinance characterization is performed using written descriptions and pictures relative to ordinance and markings, requires agreement between technician and supervisor, and provides access to additional trained experts. Disposal of ordinance using explosives includes relevant administrative type controls concerning area, personnel, and use of initiators for detonation systems. At the time the analyses was performed, no data base regarding failure rates associated with the activities was available for review.

Four aspects of the ordinance activities were identified by the SME as key to overall task success. These are: detection of ordinance by a walking ground search, safe excavation of ordinance, characterization of ordinance, and use of explosives in ordinance disposal. ASEP was used to estimate an HEP and associated error factor (EF) for each of these operations. Aspects of the substeps of the operations were considered in the analysis but subtasks were not modeled separately as they would be in a detailed HRA. Details pertaining to substeps were maintained in an engineering design file (EDF).

### **Job Performance Aid**

A one page job performance aid for HEP estimation using the ASEP pre accident nominal technique had previously been developed by the human factors and system analysis unit (Richards, 1992). This aid provides systematic consideration and documentation of the necessary assessments required to estimate the particular ASEP table item (i.e. ASEP CASE) that applies for a particular task. Each ASEP CASE represents a particular mix of specific recovery factors including: the presence or absence of a

compelling signal for the initial error, the effectiveness of post action or calibration type tests, second person or original performer verifications, and shiftly checks. The job performance aid is presented as Table 1.

### Assumptions

The ASEP nominal pre accident approach uses a basic HEP estimate of .03 for omission and commission error (.02 omission plus .01 commission). This estimate is then modified based on the presence of specific recovery factors identified for the actions analyzed. The basic HEP is multiplied by the failure probability estimates (.1 or .01 depending on type of ASEP recovery) for each specific recovery factor assessed. The basic HEP of .03 assumes adequate human factors for the action. If human factors are assessed as poor, then ASEP specifies employing a basic HEP of .05 in place of .03. Based on the description of staffing, training, procedures, administrative control, workload, psychological stress, reference material, ordinance markings, and other related variables by the SME an assumption of adequate human factors is used for the operations analyzed. Other assumptions for the analysis include the following. It is assumed that written procedures and steps are correct. The ASEP modeling estimates the failure of the specified activities due only to human error (i.e. hardware failures are not modeled in this ASEP HRA). Each HEP estimate provided is an estimated failure rate per each performance of the action (i.e. HEP per demand).

The ASEP procedure also provides estimated error factors for each HEP (multiplying and dividing the HEP by the error factor respectively provides the upper and lower bound estimates for the HEP). The following section presents and discusses the four ASEP estimates (and associated error factors in parens) from the ordinance analysis. The ASEP table reference for each estimate is provided. Chapter 5 of ASEP provides details about the ASEP nominal methodology for estimation of HEPs for pre accident tasks.

## RESULTS

Table 2 presents the HRA findings. The following paragraphs provide a discussion of each potential error, the error probability estimates, and the ASEP table references.

Table 2. ASEP HRA for ordinance disposal.

Task	Median HEP	Error Factor	Table Reference
Detect Ordinance	.003	10	5-3, III
Avoid forceful contact	.0003	10	5-3, VI
Ordinance characterization	.003	10	5-3, III
Explosives attachment	.003	10	5-3, III

The ASEP HEP estimate for "failure to detect an ordinance during the walking ground search" is .003(10). The ASEP reference for this estimate is Table 5-3, Case III. Recovery credit is given for a second person verification. ASEP requirements for a written check off to assess credit for the verification is relaxed for this estimate. It is

assumed that the configuration and staffing of the search lines and the inclusion of a separate geophysical search using metal detection equipment is analogous to a second person verification, and that the formal nature of the procedure is analogous to a written sign off. During discussion with the SME the order of the visual and geophysical search was not confirmed. From a human factors perspective the optimal order in terms of safety would seem to be geophysical search followed by visual search.

The ASEP HEP estimate for "failure to avoid forceful contact with ordinance during excavation due to failure of proximity detection" is .0003(10). The ASEP reference for this estimate is Table 5-3, Case VI. Recovery credit is given for a post maintenance/post calibration type test. The estimate assumes that geophysical survey is specified prior to every 2 ft depth of excavation using appropriate metal detection equipment/procedure, and that only small hand tools are used for the last 2 ft of excavation depth. This ASEP estimate assumes that the geophysical survey is analogous to a post maintenance/post calibration type test.

The ASEP HEP estimate for "failure of characterization of unexploded ordinance" is .003(10). The ASEP reference for this estimate is Table 5-3, Case III. Characterization of the ordinance refers to identification of ordinance, fuse, and explosive type. Recovery credit is given for a second person verification. The estimate assumes that the assessment of a well trained explosive ordinance disposal (EOD) expert is confirmed by an experienced EOD supervisor, and that the verification includes the use of written documentation specific to the ordinance type encountered.

The ASEP HEP estimate for "failure of safe attachment of explosives" used for ordinance disposal is .003(10). The ASEP reference for this estimate is Table 5-3, Case III. Recovery credit is given for a second person verification. Assumptions include an independent verification and sign off by a qualified expert for the absence of unwanted initiators for detonation systems.

## SUMMARY AND CONCLUSIONS

This limited HRA was deemed by Radiation Control management to support the analysis report (SAR) process required as part of INEL response to DOE Order 5480.23. The ASEP nominal technique for pre-accident tasks was useful for determining scoping value HEP estimates for high level tasks associated with the ordinance disposal activities and required only minimal task analysis and decomposition of tasks. The SME facilitated identification of the high level tasks used to support the risk assessment. The role of the SME in supporting HRA activities is a necessary one. Use of the job performance aid for data collection facilitated timely identification and evaluation of task characteristics needed to perform the ASEP analysis.

The basic HEPs provided by ASEP are based on data from assembly and control room type tasks. Therefore the quantitative results of the analysis described cannot be considered realistic estimates of the "true" error rates for the tasks analyzed. This is the case because empirical conformation of the applicability of the basic HEP from ASEP to the identified ordinance disposal tasks is lacking. The analysis is valuable as a systematic identification of the type of recovery factors existing for each task. The HEP estimates are useful as indices of relative error likelihood between the tasks analyzed.

## Acknowledgements

This work was supported in part by the U. S. Department of Energy (DOE), Assistant Secretary for Nuclear Energy, under DOE Idaho Field Office Contract DE-AC07-76ID01570.

## REFERENCES

- R. E. Richards, 1992, "The Applications of Performance Technology to Human Reliability Analysis," *in*: "Proceedings of IASTED International Conference on Reliability, Quality Control and Risk Assessment," Washington D.C.
- A. D. Swain and H. E. Guttman, 1983, "Handbook of Human Reliability with Emphasis on Nuclear Power Plant Operations," Sandia National Laboratory, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington D.C.
- A. D. Swain, 1987, Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772, U.S. Nuclear Regulatory Commission.

Table 1. ASEP nominal pre-accident job aid task sheet.

ASEP PRE-ACCIDENT TASKS		JOB AID	
Instructions: Starting with block 1, mark the answers to each of the following questions. (Note: If there is a compelling signal, no further ratings are needed.) Transfer your ratings to the ASEP RFP table to identify the mean RFP for the identified ASEP-level task.		ASEP PRE-ACCIDENT TASKS: ANALYSIS: DATE:	
1. COMPELLING SIGNAL		PM/PC TEST	
Is the pre-accident erroneous action fully recoverable by compelling signals--one or more annunciators or alarms that signals the error after the completion of the test but before an accident can occur?		Can errors in pre-accident actions be recovered by a post-maintenance (PM) or post-calibration (PC) test that is performed correctly?	
YES NO		YES NO	
2. ADEQUATE HUMAN FACTORS		5. IS RESULT VERIFIED?	
If overall attention to administrative controls, emergency and operating procedures, and training is very poor or if the human-machine interface is quite deficient rate adequacy as NO, otherwise rate as YES.		Order of questions	
YES NO		"Second person verifies component status after action?" Yes No	
		Original per-former checks at different time & place? Yes No	
		Is a written check-off used? Yes No	
		Rate as VERIFIED YES NO	
3. DETERMINE DEPENDENCY		6. IS STATUS CHECKED REGULARLY?	
Order of questions		Order of questions	
Action takes place within content of which type of system?	How many minutes between actions on smaller components?	How close to each other are similar components to be acted on?	Written sign-offs are made for each component?
Parallel (multiple backup systems to prevent failure)	≤ 2 minutes	In same general area	Yes
		Within 4 feet	No
	> 2 minutes	Not in same area	
Series or Single Component			
			Resulting DEPENDENCY
			ZERO
			HIGH
			COMPLETE
			ZERO
			ZERO
			ZERO

NOTES: • Answer Yes only if the second individual personally verifies the results of the action.  
 .. This job aid corresponds completely to the ASEP Nominal RFA for Pre-Accident methodology as set forth in NUREG/CR 4772 Chapter 3.

## NUCLARR CASE STUDY FOR A SGTR SEQUENCE<sup>a</sup>

David I. Gertman, Wendy J. Reece,  
Michael B. Calley, and Curtis L. Smith

Reliability Analysis and Applied Mathematics Group  
Idaho National Engineering Laboratory  
Idaho Falls, Idaho 83415

### ABSTRACT

In this paper, typical probabilistic risk assessment (PRA) measures of core damage frequency (CDF) were interpreted in the presence of uncertainty and importance evaluation in order to establish the generalizability of the failure rate information contained in the Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR). Findings for a preliminary case study comparison between the failure data contained in the NUREG/CR-4550 PRA for Surry Unit 1 steam generator tube rupture (SGTR) sequence and NUCLARR rates for that same sequence are presented. Implications regarding general use of NUCLARR as a source of failure rate estimates and the ability of IRRAS 5.0 to support future case study comparisons are discussed.

### INTRODUCTION

The Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) is an NRC-sponsored data management system for storage and retrieval of human error probabilities (HEPs) and hardware component failure data for use in probabilistic risk assessment (PRA) efforts.<sup>1</sup> This database was originally designed to support generic safety issue resolution, determine important trending information, and to provide a research basis for risk-based regulation.<sup>2</sup> Risk analysis practitioners typically have used NUCLARR to verify failure rates for specific components or for individual operator actions. Estimates of the degree of correlation with contemporary analysis of event sequences have not been reported. The analysis presented in this paper uses NUCLARR estimates for an event sequence and compares the resulting core damage frequency (CDF) to contemporary efforts to characterize that same sequence.

NUCLARR includes data collected from a decade of U.S. reactor studies. Candidate data from PRAs or other special studies are screened and processed by a review committee knowledgeable in PRA, human reliability analysis (HRA), and reactor operations according to procedures documented in NUREG/CR-4639, Volume 3.<sup>3</sup> Data from international sources such as TÜV Rheinland--Germany, the Swedish Nuclear Power Plant Inspectorate (SKI), and

<sup>a</sup> Work supported by the U.S. Department of Energy under DOE Contract number DE-AC07-76ID01570. Earlier work referenced in this article was sponsored in part by the U.S. Nuclear Regulatory Commission. The opinions expressed herein are solely those of the authors, and do not necessarily reflect views of the DOE, NRC or any other U.S. Department or Agency.

the Nuclear Safety Board of Swedish Reactors (RKS) is also available in NUCLARR. Data from Eastern European and Russian-designed reactor facilities are also being processed for inclusion.

### Case Study and Data Selection

Although cut sets for all five well known and widely referenced NUREG-1150<sup>4</sup> plants were available at the INEL in the Integrated Risk and Reliability Analysis System (IRRAS) 5.0<sup>5</sup> computer code, the Surry plant was selected because the steam generator tube rupture (SGTR) sequences in the Surry PRA include hardware failures and human errors associated with recovery. (Human errors in the SGTR sequences were of particular interest because one of the goals of this case study was to address whether the HEP side of NUCLARR would correlate with HEP estimates in the Surry PRA.)

Despite the fact that the SGTR initiating event category contributes approximately four percent of the total CDF, the SGTR sequences are interesting because of the mix of component failures and human actions involved. Of the nineteen SGTR sequences presented in the PRA, SGTR Sequence 8 (T<sub>7</sub>OPQ<sub>5</sub>) represents failure of the steam generator integrity combined with operator failure to depressurize. These events lead to an eventual depletion of the refueling water storage tank (RWST) inventory through the unisolated steam generator. Sequence 8 was selected for further analysis because this sequence accounts for 87.5% of the SGTR contribution to the overall CDF.

Plant systems and accident sequence details are summarized from Section 4.4.6 of NUREG/CR-4550<sup>6</sup> in the following paragraphs.

The SG initiator (T-7) causes a breach in the primary pressure boundary into the secondary side pressure boundary. Success criteria involve maintaining both the primary and secondary side pressure boundaries. As part of this sequence, normally open effluent lines to the steam generator must be isolated because they now represent open effluent lines to the primary system.

The SGTR is assumed to be a double ended rupture of a single tube which results in an outflow that requires an equivalent makeup flow of 600 gpm. Actuation of safety injection (SI) occurs on low pressurizer pressure. Turbine trip, main feedwater isolation, and start of auxiliary feedwater occur on the SI signal. Operators must identify and isolate the ruptured SG. These actions include closure of the main steam isolation valve, auxiliary feedwater inlet valve, steam generator blowdown line, and turbine driven pump steam admission valve. Complete isolation requires reactor coolant system (RCS) pressure to be less than the SG pressure.

### TECHNICAL APPROACH

Failure rate estimates were obtained from NUREG/CR-4550 and compared directly to estimates generated from NUCLARR. This included using aggregation routines available in NUCLARR, as documented and defined in NUREG/CR-4639, Volume 4.<sup>7</sup>

### NUCLARR Search Strategy

NUCLARR data searches were limited to U.S. data collected after 1982 and specified by the components identified in the SGTR Sequence 8. In addition to searching individual components, searches were conducted on the basis of similar event sequences, i.e., those involving SGTR accidents. Surry data are included in the NUCLARR data base but were not used so that their contribution to the NUCLARR data set would not impact the correlation between the NUREG/CR-4550 and NUCLARR data sets. Event sequence analysis was performed with IRRAS 5.0.

## IRRAS Usage

The IRRAS computer code was used to evaluate the SGTR sequence for four different facets of analysis. First, the sequence minimal cut sets were generated from the Surry PRA logic models. Second, the minimal cut set upperbound (i.e., mincut) was calculated from the sequence minimal cut sets. The mincut was calculated using the following equation:

$$MC = 1 - \prod_{i=1}^n (1 - P_i)$$

where

$n$  = total number of minimal cut sets, and  
 $P_i$  = probability of the  $i$ 'th cut set.

Third, the sequence uncertainty was evaluated through the use of Monte Carlo sampling. And fourth, the Fussell-Vesely<sup>6</sup> importance was evaluated for each event in the sequence cut sets. The Fussell-Vesely importance was calculated using the following equation:

$$FV = [F(x) - F(0)]/F(x)$$

where

$F(x)$  = mincut evaluated using the mean values for the basic events, and  
 $F(0)$  = mincut evaluated with the basic event in question set to a probability of zero.

## FINDINGS

### Failure Rates and HEP Estimates

Table 1 presents a matrix of the component failure rates, HEPs, and associated error factors from NUREG/CR-4550 and NUCLARR. The first row in the table identifies the source and type of failures. The second row presents the component failure rates, HEPs, and associated error factors identified in NUREG/CR-4550. The third row presents the failure rates, HEPs, and associated error factors generated with NUCLARR. All failure rate estimates presented are mean values.

Table 1. Comparison of Failure Rates and Human Error Probabilities for SGTR.

Source	Air operated Valves	Motor operated Valves	HEP #1	HEP #2	HEP #3	HEP #4
NUREG/ CR-4550	1.0E-3 (EF=3)	1.0E-3 (EF=3)	6.4E-2 (EF=10)	6.8E-6 (EF=10)	3.4E-3 (EF=10)	2.9E-2 (EF=10)
NUCLARR	3.14E-3 (EF=8.4)	6.25E-3 (EF=4.1)	6.14E-3 (EF=2.4)	6.14E-3 (EF=2.4)	6.14E-3 (EF=2.4)	1.2E-2 (EF=1.8)

#### KEY

HEP: #1= failure of operator to terminate flow from stuck open PORV; #2= failure of operator to terminate flow from turbine driven pump steam line during SGTR; #3= failure of the operator to terminate flow from SG blowdown line; #4= operator fails to depressurize/cooldown RCS during SGTR.

Corresponding component failure rates from NUCLARR were substituted in IRRAS 5.0 for failures of motor operated valves and air operated valves (the failure mode for the two components was fails to transfer). Also, HEP estimates from NUCLARR were substituted in IRRAS 5.0 for associated human errors.



## Mincut Evaluation

The SGTR Sequence 8 mincut was calculated for two cases. Case 1 evaluated the sequence using the original Surry PRA data. Case 2 evaluated the sequence using the NUCLARR data described in Table 1. These two cases were evaluated using a probability truncation limit of  $1.0\text{E-}12$ . The mincut for Case 1 was calculated to be  $1.4\text{E-}6$  while the mincut for Case 2 was calculated to be  $1.2\text{E-}6$ .

## Uncertainty Evaluation

The uncertainty for the two cases was evaluated through Monte Carlo simulation. A total of 5,000 samples were performed for each case. The results of the uncertainty analysis are summarized in Table 2. As seen in the mincut results, the uncertainty analysis results for the two cases are very similar. Specifically, the mean and 95th percentile values for the two cases show close agreement. The 5th and 50th percentile values show a little difference between the two cases, but generally these percentile values are de-emphasized relative to the mean and 95th percentile values. This is because, where safety is concerned, it is common practice to use the mean and/or upper bound indexes rather than the median and/or lower bound indexes.

Table 2. Uncertainty evaluation results for the SGTR sequence.

Parameter	Case 1 NUREG/CR-4550 data	Case 2 NUCLARR data
Mean	9.6E-7	1.1E-6
5th Percentile	7.7E-9	7.1E-8
50th Percentile	1.4E-7	5.1E-7
95th Percentile	3.4E-6	3.7E-6
Standard Deviation	4.3E-6	2.5E-6

## Importance Evaluation

The importance for the basic events in the sequence was evaluated using the Fussell-Vesely importance calculation. Table 3 shows the top ten important basic events for the two cases. The Case 2 importance results indicate the basic event and the position of that event from the Case 1 importance results. In general, the top ten important basic events for the NUREG/CR-4550 data case appear in the top ten list for the NUCLARR data case (i.e., Case 2). One event moved from 16th place for Case 1 to second place for Case 2 on the Fussell-Vesely importance list. This event was MSS-XHE-FO-ISAFW, which represents the operator failing to terminate flow from the steam generator blowdown line during a SGTR. The Surry PRA listed this failure rate as  $6.8\text{E-}6$  per demand while the NUCLARR-generated data identified the failure rate as  $6.1\text{E-}3$  per demand. It is interesting to note that even though the failure rate for this human error probability event increased by three orders of magnitude, the sequence mincut stayed about the same.

Table 3. Top ten Fussell-Vesely importance rankings for the SGTR sequence.

Case 1 NUREG/CR-4550 data	Case 2 (Case 1 Position) NUCLARR data
1. RCS-XHE-FO-DPRT7	(1) RCS-XHE-FO-DPRT7
2. REC-XHE-FO-DPRES	(16) MSS-XHE-FO-ISAFW
3. MSS-SRV-OO-ODSRV	(3) MSS-SRV-OO-ODSRV
4. PORV-NOT-BLK	(2) REC-XHE-FO-DPRES
5. SGTR-SGSRV-ODMD1	(5) SGTR-SGSRV-ODMD1
6. PORV-BLK	(6) PORV-BLK
7. SGTR-SGSRV-ODMD2	(4) PORV-NOT-BLK
8. MSS-XHE-FO-BLOCK	(7) SGTR-SGSRV-ODMD2
9. SGTR-SGADV-ODMD	(12) REC-XHE-FO-GAGRV
10. MSS-SOV-OO-ODADV	(11) IAS-CCF-LF-INAIR

## SUMMARY AND DISCUSSION

The case study comparison between Surry data and NUCLARR and generated data for a SGTR sequence produced *equivalent* results. The mincut values obtained using IRRAS 5.0 were on the same order or magnitude ( $1.0E-6$ ) for both data sets. There was a minor shift in the Fussell-Vesely importance rankings, but the top ten events were basically the same. The most significant shift was for the "operator terminates flow from the steam generator blowdown line during the tube rupture" event. This event shifted from 16th in the importance list with the original data to second in the importance list with the NUCLARR data. This shift can be attributed to the nature of NUCLARR HEPs. The variability of NUCLARR HEPs is due to a range of performance shaping factor (PSF) attributes, including a large number of instances where more than one PSF is less than optimal. (PSFs can either raise or lower HEP values.) Additionally, a number of HRA quantification methods are represented. The plant specific value for this human error was a non-conservative estimate that accounted for the positive influence that procedures, training, and plant interface had on the operators' performance. The plant specific value for this human error was  $6.8E-6$ .

Uncertainty analysis findings were also supportive of using NUCLARR to assist in quantifying event sequences. Comparison of the mean and 95th percentile results indicated that there was little difference between the Surry data and NUCLARR data. A small difference was indicated for comparisons of the lower bound (5th percentile) and the median (50th percentile) values. This difference is influenced by the smaller error factors associated with the HEPs obtained from NUCLARR. The Surry data tended to use an error factor of 10 for all HEPs. The error factors for the NUCLARR generated data reduced the overall sequence uncertainty as indicated in the uncertainty results for Case 2.

Also, two of the HEPs from NUCLARR were higher than the HEPs used in the Surry PRA. The HEP from NUCLARR for operator failure to terminate flow from turbine driven pump steam line was three orders of magnitude higher. The HEP from NUCLARR for operator failure to terminate flow from the steam generator blowdown line was almost a factor of two higher. Even so, the minimal cutset upperbound values were indistinguishable.

During this analysis, a number of methodological insights were gained. First, the rule-based recovery factors for the sequence cut sets that IRRAS 5.0 uses facilitated the analysis. Appropriate recovery factors are automatically applied to the failure cutsets. Second, obtaining NUCLARR values required a relatively large number of data searches. Data were obtainable, but required expertise on the part of the analyst to obtain the appropriate data. Recommendations for enhancing the search strategy generator portion of NUCLARR are under review. Third, the single study comparison presented herein needs to be duplicated for another plant or for additional sequences at the same plant. Sequences where human error has been shown to dominate the CDF such as during loss of offsite power would present an interesting case study. Lastly, the efficacy of NUCLARR values to support PRA for passive systems analysis, such as that proposed for AP600 designs, may be achievable and warrants further study.

## REFERENCES

1. W. J. Reece, The NUCLARR databank, *DOE Risk Management Quarterly*. 1:3, (1993).
2. W. J. Reece, and D. I. Gertman, NUCLARR: A workstation software package to support risk assessment, *Reliability Engineering and System Safety*. 37:3, (1992).
3. W. J. Reece, B. G. Gilbert, and R. E. Richards, "Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) Volume 3: Guide to Data Processing and Revision," EGG-2458, Revision 1, Idaho National Engineering Laboratory (in press).

4. Reactor Risk Reference Document, NUREG-1150, U.S. Nuclear Regulatory Commission, Washington, DC (1987) .
5. K. D. Russell, et al, "IRRAS 5.0," NUREG/CR-5813, U.S. Nuclear Regulatory Commission, Washington, DC (in press).
6. R. C. Bertucio, and J. A. Julius, "Analysis of Core Damage Frequency: Surry, Unit 1 Internal Events," NUREG/CR-4550, SAND86-2084, Volume 3, Revision 1, Washington, DC (1990).
7. W. Gilmore, et al, "Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) Volume 4: User's Guide," NUREG/CR-4639, EGG-2458, U.S. Nuclear Regulatory Commission, Washington DC, (1990).

## **INSIGHTS INTO PILOT SITUATION AWARENESS USING VERBAL PROTOCOL ANALYSIS**

Harold Blackman, Christopher Sullivan, and  
Karen Seidler

INEL/EG&G Idaho Inc.  
P.O. Box 1625  
Idaho Falls, ID 83415-3850

### **INTRODUCTION**

In recent years, the importance of situational awareness (SA) in pilot mission success has been recognized and efforts to find ways of improving and supporting SA in the cockpit have intensified. The concept of situational awareness is intuitively appealing. It addresses the idea that some individuals are "aware" of past, existing and future states of a situation and such "awareness" enhances performance. However, actually identifying the underlying components of SA in order to operationalize the concept has proved problematic. The difficulty of measuring pilot SA arises because SA is in large part a product of covert cognitive processes occurring within the complex context of an operational aviation setting. The present study examined the utility of using verbal protocol analysis as a possible tool for capturing some of these complexities. It was believed that verbal protocol analysis would provide a relatively unobtrusive means of tapping into the internal processes of the pilots through accessing information currently being held in working memory and thus directly available for reporting (Ericsson and Simon, 1984). Specifically, the content of think-aloud verbalizations of both expert and novice pilots in combat situations was examined to see if it could be used to discriminate quality of SA. In this study, experts were assumed to have better situational awareness than novices. Each group of pilots flew three different scenarios on an F-16 Air Intercept Trainer (AIT). The scenarios simulated air-to-air interception of one, two, and four enemy aircraft by a single F-16 fighter pilot. The different scenarios were designed to represent increasing attentional demands on the pilots. Concurrent verbalizations of the pilots were recorded, encoded and analyzed for content that might reflect different aspects of SA.

### **METHOD**

#### **Subjects**

Twelve F-16 Air Force reserve pilots served as subjects. Six were expert pilots and six were novice pilots. The experts were instructor

pilots with flight time in the F-16 ranging from 1000 to 2000 hours. Novice pilots had only recently completed their introductory F-16 training course and their flight time in the F-16 did not exceed 80 hours.

### **Apparatus and Flight Scenarios**

An Air Intercept Trainer (AIT) flight simulator was used to present mission scenarios. The AIT is a fixed-base simulator with a head-up display and the standard radar configuration for an F-16. Three air intercept mission scenarios were flown by each pilot. The scenarios differed in the number of enemy aircraft to be intercepted and were selected to represent different degrees of difficulty and threat. In all scenarios, enemy aircraft flew head-on toward the pilots and no enemy aircraft could fire upon the pilots. The simplest scenario involved the interception of a single aircraft. The second scenario consisted of two enemy aircraft that flew abreast of each other. The third scenario consisted of four enemy aircraft that flew in a champagne glass formation.

### **Procedure**

Each subject participated in a single two hour session. During the first part of the session pilots practiced verbalizing while flying the AIT simulator. Once familiar with the AIT simulator and the additional task of verbalizing protocols, each pilot was required to fly the three scenarios described earlier. For each scenario, pilots were instructed to shoot down all enemy aircraft. Subjects were told that enemy aircraft could not shoot back or evade their pursuit. Subjects were not given any information about the number of air interceptions that would be required in any one scenario.

Each scenario lasted approximately five minutes. For each scenario, workload was measured at the completion of the mission using NASA's Task Load Index (TLX) of subjective workload (Hart and Staveland, 1988). The TLX assesses workload by using a weighting procedure to evaluate the relevance of six dimensions: temporal demand, physical demand, mental demand, performance, effort, and frustration.

### **Experimental Design**

A 2 X 3 mixed design was employed in the study. There were two levels of pilot experience (expert and novice) and three flight scenarios (interception of one, two, and four enemy aircraft). Flight scenario was within-subject, while experience was a between-subject variable. Scenarios were presented in a random order to each subject.

### **Verbal Protocol Analysis**

Pilot Verbalizations. The pilots' think-aloud verbalizations for each scenario were recorded, transcribed, segmented and then encoded according to a functional model of the problem space. That is, a set of codes which described the functions a pilot was taught to perform to complete the mission was developed and applied to each text segment. A total of eight functions were identified including search target, track target, place target, analyze geometry, analyze other geometry, choose intercept method, fire weapon, and aircraft position. A ninth code - "Other" was also used to encode verbalizations that were not encompassed by the functional model. The actual encoding was done using SHAPA, an interactive software tool for protocol analysis developed at the University of Illinois at Urbana-Champaign (see Sanderson, James, and Seidler, 1989). Frequency counts of each of the function codes were performed for each of the encoded protocols. In order to normalize these frequencies across protocols of different lengths, the frequencies were transformed into percentages of total verbalizations.

## RESULTS

### Workload Data

Both the TLX overall workload rating and the mental demand scale rating were analyzed. There were no significant differences in overall workload ratings as a function of experience, number of enemy aircraft or the interaction of experience and aircraft. However, for the mental demand scale, significant differences were found as a function of the number of enemy aircraft ( $F(2,20)=4.819, p<.05$ ). The mean weighted ratings for mental demand were 168, 195, and 226 for one, two, and four enemy aircraft, respectively. These values represent the relative importance of mental demand in contributing to the overall perceived workload for the scenarios. This suggests that increasing the number of aircraft across scenarios resulted in a concomitant perception by the pilots of increasing mental demand required to complete the mission, and hence an increase in mission difficulty. In addition, Figure 4 below shows the trend, although it is not significant, for experts to experience less mental demand than novices.

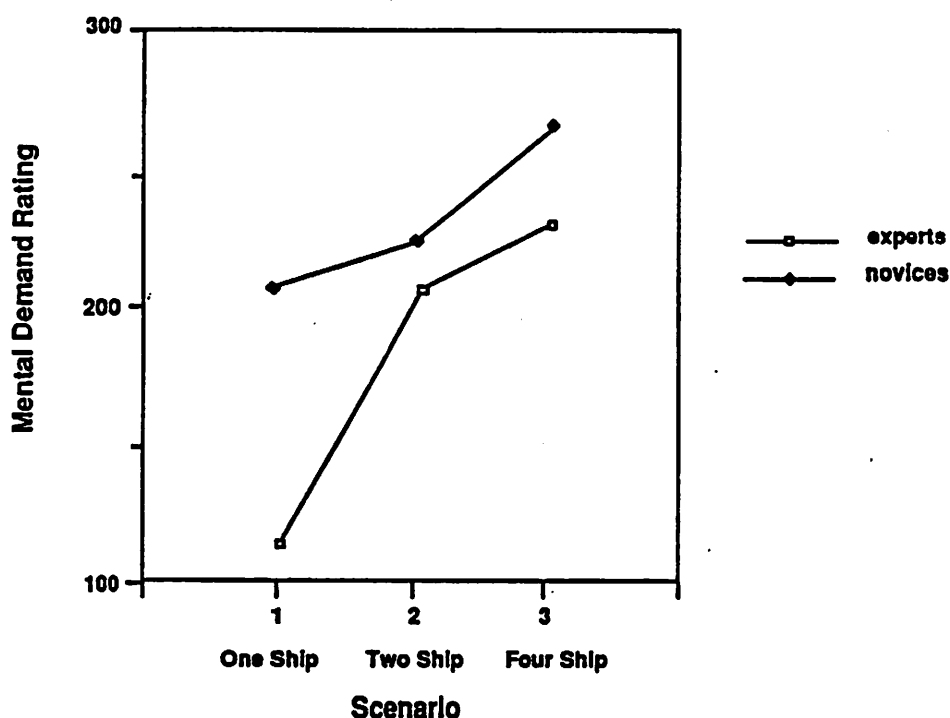


Figure 4. Mental demand rating on the TLX Workload scale.

### Verbal Protocol Analysis

The analysis of the content of the verbalizations revealed significant findings for the functions of Analyze Geometry (AG) and Analyze other Geometry (AG-other). AG refers to verbalizations made about spatial relationships of targeted aircraft. AG-other refers to verbalizations made about spatial relationships of non-targeted aircraft. Novices were found to verbalize proportionally less than experts about analyzing geometry ( $F(1,10)= 5.579, p=.04$ ) (Figure 5). In addition, novices verbalized proportionally less about analyzing geometry as the number of enemy aircraft increased (one ship v. three ship:  $t(5) = 3.170, p<.03$ ; two ship v. three ship:  $t(5) = 3.316, p<.02$ ) (Figure 5). There was no comparable significant difference in the proportion of AG verbalizations for experts as the number of enemy aircraft increased.

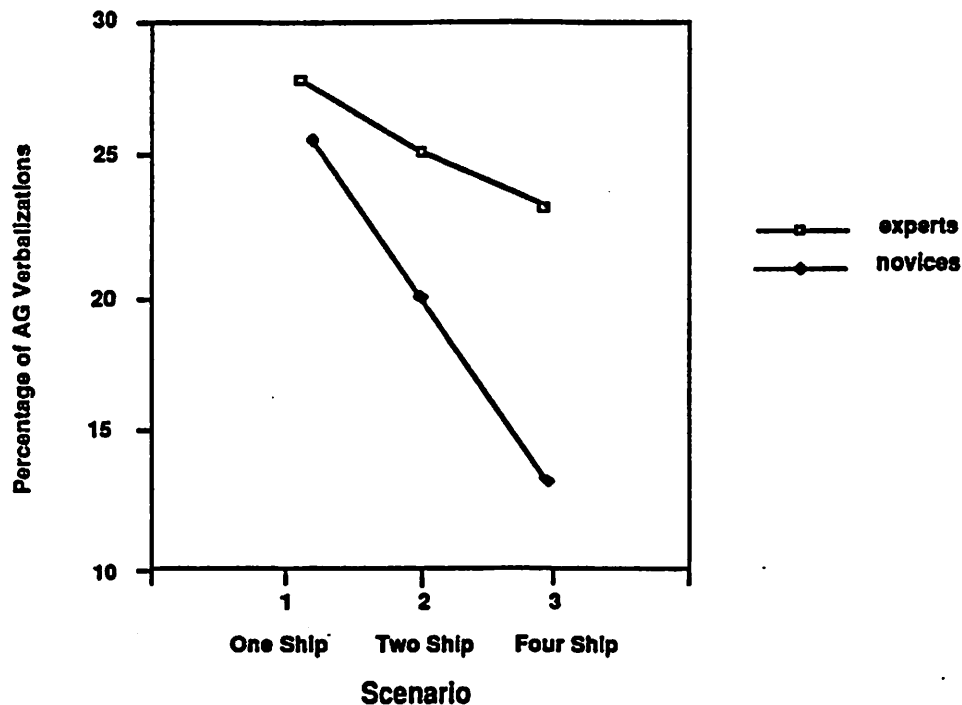


Figure 5. Analyze Geometry verbalizations as a function of scenario and level of expertise.

Novices were also found to verbalize proportionally less than experts about non-targeted aircraft ( $F(1,20)=7.158, p<.02$ ) (Figure 6). There was a significant interaction of experience and scenario ( $F(1,10)=4.697, p<.05$ ), though, with post hoc comparisons showing this difference between experts and novices to be present in only the two-ship scenario ( $t=9.4, p<.001$ ). A trend by experts to verbalize proportionally less about non-targeted aircraft as the number of aircraft to be intercepted increased can also be seen, however, it is not significant.

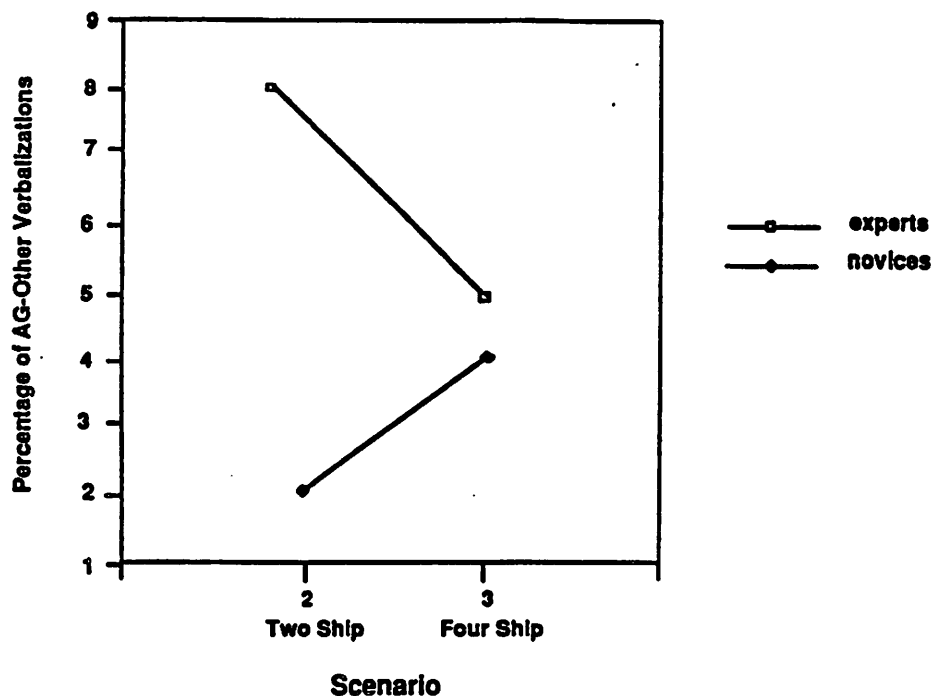


Figure 6. Analyze Other Geometry as a function of scenario and level of expertise

Additional analyses were performed to further examine the extent to which experts and novices differentially expressed concern about enemy aircraft. In this analysis, any verbalizations expressing concern about non-targeted aircraft, not just verbalizations referring specifically about spatial relationships, were looked at in addition to AG-other verbalizations. These additional verbalizations were coded under the category of "other". In the four-ship scenario, the four aircraft split into two groups so only "other" statements reflecting concern about the pair of aircraft that didn't contain the target were included in this analysis. The results are shown in Figure 7. It can be seen that the percentage of experts expressing concern about non-targeted aircraft at least once during a scenario is significantly greater than the percentage of novices ( $\chi^2 = 8.22$ ,  $df=1$ ,  $p<.01$ ). It can also be seen that experts maintain this concern about non-targeted aircraft across scenarios. Novices express a modest concern about non-targeted aircraft in the two-ship scenario, however, in the four ship scenario, they express no concern about the non-targeted pair of ships whatsoever.

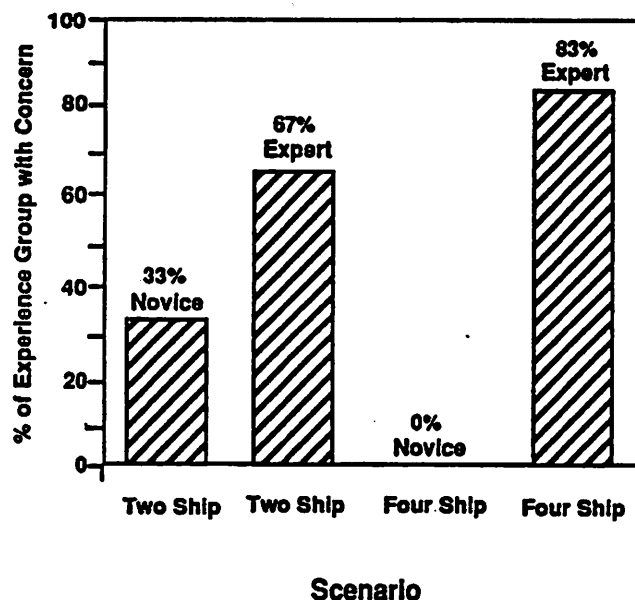


Figure 7. Percentage of pilots expressing concern about non-targeted aircraft at least once during a scenario as a function of number of enemy aircraft (i.e. scenario) and level of expertise.

## DISCUSSION AND CONCLUSIONS

The purpose of this experiment was to explore the usefulness of verbal protocol analysis in studying pilot situational awareness. Verbal protocols were examined for differences in content, as a function of experience and workload, which might reflect the quality of situational awareness. In this study, experts were assumed to have a better quality of situational awareness than novices. It was found that experts verbalize more about intercept geometry of the air-to-air intercepts in general and that they try to maintain a level of concern about the spatial locations of enemy aircraft across different scenarios. Experts may know that attending to all aircraft during an intercept mission is critical because of their experience and training. Novices appear to react more to individual scenarios and focus on targeted aircraft at the expense of building a more general awareness of the overall intercept situation. This could be a function of the demand on the novices' time due to missing schema for air-to-air combat, or due simply from a lack of knowledge of what is critical in these situations.



Fracker (1991) suggests that among the guidelines to be used in evaluating any SA metric are reliability and validity. This study looked at one aspect of validity - construct validity- which is the degree to which a measure can quantify SA. Among the criteria Fracker suggests should be used to establish construct validity are: 1) that the measure of SA should show that SA decreases when attention is spread over more complex situations and; 2) that the measure should be related to mental effort in such a way that as situational assessment becomes more difficult, then SA should decrease, mental effort should increase or both. In the present study, it was observed that the AG and AG-other verbalizations of novices decreased as mental demand increased and when attention was spread across a larger situation (as defined by the number of enemy aircraft). For experts, some evidence of a decrease in SA for non-targeted aircraft in the more attention-demanding (i.e., four-ship) scenario was also seen. This suggests that the functions of AG and AG-other are sensitive to attentional demands and mental effort and provides some support for the analysis of spatial relationships as a possible component of a metric for assessing SA. These results also suggest that protocols have promise in examining how SA is built. Future work needs to further examine not only the spatial component of SA but the temporal aspects and role of long term memory, as well. Future work also needs to include SA specific performance measures, to facilitate correlations of verbalizations to more concrete evidence of SA. This could involve supplementing verbal measures with spatial measures that directly examine the pilots' knowledge of current and future states.

#### REFERENCES

- Ericsson, K.A and Simon, H.A. (1984). *Protocol analysis: Verbal reports as data*. Cambridge, MA: MIT Press.
- Fracker, M. L. (1988). A theory of Situation assessment: implications for measuring situation awareness. *Proceedings of the Human Factors Society 34th Annual Meeting*. Santa Monica, CA: Human Factors Society, p. 102-106.
- Hart, S.G. and Staveland, L.E. (1988). Development of a NASA-TLX (Task Load Index): Results of empirical and theoretical research. In P.S. Hancock and N. Meshkati (Eds.), *Human mental workload* (pp. 139-183). Amsterdam: North-Holland.
- Harwood, K. Barnett, B. & Wickens, C.D. (1988). A conceptual and methodological framework. In *Proceedings of the 11th Symposium on psychology in the Department of Defense*.
- Sanderson, P.M., James, J.M. & Seidler, K.S. (1989). Shapa: an interactive software environment for protocol analysis. *Ergonomics*, 32(11), p. 1271-1302.

**095 Risk Methods for Defense Applications**

*Chair: M.V. Frank, Safety Factor Assoc.*

**Probabilistic Risk Assessment of Weapon-Systems Field-Testing: Accounting for System's Complexity and Unfamiliarity**

*S. Feller, M. Maharik (RAFAEL, Israel)*

**Nuclear Weapon System Risk Assessment**

*D.D. Carlson (SNL)*

**Probabilistic Risk Assessment of Disassembly Procedures**

*D.A. O'Brien, T.R. Bement, B.C. Letellier (LANL)*

## **PROBABILISTIC RISK ASSESSMENT OF WEAPON-SYSTEMS FIELD-TESTING: ACCOUNTING FOR SYSTEM'S COMPLEXITY AND UNFAMILIARITY**

S. Feller<sup>1</sup> and M. Maharik<sup>1</sup>

<sup>1</sup>RAFAEL  
P.O. Box 2250  
Haifa 31021, Israel

### **INTRODUCTION**

Full-scale field testing of modern weapon systems may impose risks on both the test teams and the civilian population adjacent to the test range. Comprehensive risk assessments are thus performed as part of the test approval process. The aims of such risk assessments are:

(a) To provide a thorough and detailed understanding of the hazards associated with the proposed test scenario. In the context of this presentation, the "test scenario" is the combination of the investigated weapon system, the test design, and the geographical and demographical setting.

(b) To identify the weak links of this test scenario, i.e., scenario points of relatively high-probability failure modes, possibly combined with severe outcomes, given failure. The aim is to eliminate such weak links, or at least to mitigate the outcomes of such critical junctions.

(c) To produce a quantitative estimate of the expected levels of additional risk imposed by the proposed test configuration on various types of populations, so that a decision can be made on whether the scenario can be approved or should be rejected.

The purpose of this paper is to present a taxonomy of weapon systems according to their degree of complexity and unfamiliarity, and a methodology that we have developed and used over the years for assessing the risks associated with testing weapon systems that correspond to different levels of these two "dimensions."

### **ASSESSING THE RISKS OF A WEAPON SYSTEM FIELD-TEST**

A complete risk assessment of a proposed weapon field-test (e.g., a missile's free flight) should comprise of the following:

1. Collecting the relevant information in detail.

2. Failure analysis of the investigated system (with failure modes and their associated probabilities as outcomes).
3. Calculation of trajectories following failures, i.e., trajectories deviating from the nominal test plan.
4. Estimation of impact areas resulting from failures.
5. Projection of the proposed test geometry on the test arena, and elicitation of the test's kinematic envelope. The "kinematic envelope" is defined as the entire ground area that can be reached by the tested system, or its debris or fragments, following any type of failure and deviation, given the initial launch or release conditions (location, altitude, velocity, and angular orientation).
6. Calculation of individual risks and integration of societal risk levels throughout the kinematic envelope of the tested system.
7. Decision-making: test approval or further iterations until safety demands are met.

## TAXONOMY

In principle, a complete, detailed failure analysis should be performed for every test of a weapon system under consideration. However, as we shall see, such an analysis is not always feasible. Based on its level of complexity, compounded by its degree of unfamiliarity, we found it practical to classify a weapon system proposed for test as belonging to one of the following three subgroups:

**Subgroup A:** Complex weapon systems, with a very meager (if at all) body of analytical and empirical knowledge upon which one could base a detailed failure analysis. In other words, highly complex systems, coupled with marked unfamiliarity of subsystems failure modes; also, data on similar systems are unavailable. On the other hand, geometrical performance characteristics of the investigated system as a whole can be estimated.

**Subgroup B:** Same type of systems as in Subgroup A, but, in addition, a large body of experience has been gained from field tests of comparable systems.

**Subgroup C:** Detailed technical information exists for the weapon's subsystems, so that each, or most, of its failure modes can be identified and analyzed. Complete and detailed failure analysis is thus feasible.

## METHODOLOGY

The following three examples illustrate the different treatment accorded each subgroup.

### Subgroup A

Consider a first-generation Point-Defense Missile (PDM). The missile involved in the test is launched vertically. After the launch it executes a bend, nominally in the direction of the perceived threat (Figure 1). Unfamiliarity is so pronounced, that at this time we perform no detailed failure analysis at all: we rely mostly on *geometrical factors*.

We assume a high level of uncertainty associated with the direction of the actual initial bend. Therefore, we have, a-priori, an omni-directional envelope. A gaussian model may be adopted, assuming that the probability of hitting the ground at a range  $r$  from the launcher is a normal function of  $r$ , with maximum probability density at  $r=0$  (Figure 2). The maximum reasonable range calculation is based on conservative aerodynamic

assumptions. When applying the model, the impact circle is divided into ten or more equal-width "rings." An assumption is made that within each ring the probability distribution of hitting along  $r$  is uniform.

As explained in detail elsewhere (Feller and Maharik, 1992), the tool that we use for go/no-go decisions is a set of benchmark number pairs. Each pair consists of the following figures: (a) the maximum allowed individual risk, that is, the probability that a given member of the exposed population becomes a fatality over a given time-period; and (b) the maximum allowed societal risk, that is, the statistical expected number of fatalities within the same population over the same time-period. Each pair corresponds to a specific type of the exposed population (non-participating, uninformed general population; non-participating, uninformed workers in industrial facilities; defense-community non-participating and uninformed personnel; and defense-community personnel who are participating in the test and are informed about the risks). Determination of the benchmark number pairs is based on a "ripple principle," stating the following: The existing background risk level of any population is not a constant; rather, it is modulated by some ripple. We require that the integrated test-generated risk increment, contributed to the existing background risk level of a population by all the tests conducted over a given time-period, will not raise the risk level of the most exposed members of that population, above the ripple that modulates its background risk anyway.

The model presented above enables the calculation of the risk imposed by the proposed test as follows (the equations refer to any single type of the exposed population):

$$P_{Pi} = P_1 \cdot P_{i/1} \cdot \frac{A_{Ki}}{A_i}$$

$$P_S = \sum_i (P_{Pi} \cdot N_i)$$

where:

- $P_{Pi}$  - Individual risk at ring  $i$ ;
- $P_1$  - Probability of the weapon system's failure;
- $P_{i/1}$  - Probability of impact within ring  $i$ , given failure;
- $A_{Ki}$  - Mean Area of Effectiveness (MAE) at ring  $i$ , given impact;
- $A_i$  - Area of ring  $i$ ;
- $P_S$  - Societal risk;
- $N_i$  - Size of population at ring  $i$ .

The model is flexible. For example, allocation of angular-dependent impact probabilities (e.g., downrange vs. uprange) is possible (Figure 3). Thus, a sensitivity analysis, which is an important and useful tool in the given uncertainty conditions, is easy to implement.

### Subgroup B

Consider a new, as yet untested, stand-off air-to-ground attack missile. This weapon consists of numerous subsystems such as propulsion, control, navigation, homing, fusing, etc. (Figure 4).

The combination of a very complex system and high level of unfamiliarity still renders a detailed failure analysis not feasible within the constraints of available time and budget. However, a large body of knowledge has been accumulated with regard to field-testing of similar systems. Hence, we adopt a model that starts with a set of *failure outcomes* typical to the family of comparable missiles (e.g., no motor ignition following

release, loss of propulsion system during free flight, loss of control at any axis or combination of axis, no target lock-on or loss of target lock-on), rather than with failures of specific components of the investigated system.

Each typical outcome leads to a corresponding ground impact area, which can be estimated on the base of the designed missile performance. Probabilities are allocated for each typical outcome according to previous experience, and a probability distribution is estimated for each impact area. For example, the along-track distance from launch to impact given a pitch/altitude control failure may run from zero to the maximum possible range (the latter based on energetic and kinematic considerations), with areas of relatively high probability density around the ballistic fall area and the nominal target range (Figure 5). Individual and societal risks may thus be calculated. Figure 6 shows a resulting impact probability map. The external contour marks the boundary of the kinematic envelope of the tested missile, while internal contours represent areas in which individual risks are of the same order-of-magnitude (typically increasing inbound).

A system belonging to Subgroup B, then, does not undergo a detailed failure mode analysis, similarly to Subgroup A systems. However, building on "external" experience gained from comparable systems, one constructs a failure outcome model to define and quantify the risk.

### Subgroup C

Here, an evaluation of a laser-guided, anti-armor, ground-to-ground missile is the case in point. The missile is based on relatively less complex subsystems than used for our Subgroup B missile. Moreover, a large body of relevant information has been assembled for the subsystems included. Combination of this positive familiarity with "reasonable" degree of complexity makes a detailed analysis feasible.

In this case, the analysis starts from a systematic identification of all the possible *technical failures*. For each failure and its relevant outcome, the derived trajectory is calculated and the resulting impact area, depending on parameters' uncertainty, is obtained (Figure 7).

The rest of the process is very much like the former one, but unlike that case, the present conclusions are related directly to the investigated system.

### CLOSURE

The methodology described above emerged gradually during two decades of field-test activity in Israel, mostly at RAFAEL's Shdema Test Range. The test scenarios performed at this range exhibit the whole spectra of complexity and unfamiliarity mentioned above. From the point of view of achieving a structured risk-management process in this context, our methodology proved to be most beneficial.

The specific models shown here have been, in themselves, used by other evaluators of weapon and flight systems. For example, NASA used both ringed and boxed probability impact maps in assessing the risks posed on the populations of Florida and the entire world, respectively, due to the 1989 launch of the Galileo spacecraft (GE Astro Space, 1988). The emphasis of the present work is in defining an organized taxonomy and a structured approach toward the "fuzzy" problem of testing weapon systems with varying levels of complexity and unfamiliarity.

Last but not least, when dealing with probabilistic risk assessment one must bear in mind what may be referred to as "The Engineering-Probability Principle (EPP)": It is legitimate to rely on probabilistic arguments, estimates and criteria, only when all that is

"engineeringwise" possible, reasonable and feasible has indeed been introduced in order to prevent a failure of the investigated system and test design. In our case, this includes performing thorough design reviews, installing flight-termination systems, and other such activities, which have been our policy throughout the years.

## ACKNOWLEDGEMENTS

The authors wish to thank C. Shen-Orr, Z. Porat, D. Perlstein and I. Naor for their contributions. The opinions expressed are those of the authors.

## REFERENCES

- Feller, S. and Maharik, M., 1992, Risk criteria for approving or rejecting field-tests of high-performance weapons, Paper presented at the Annual Meeting of the Society for Risk Analysis, San-Diego.  
 GE Astro Space, 1988, Final safety analysis report for the Galileo Mission, Vol. II - Accident model document, General Electric Corp., Philadelphia.

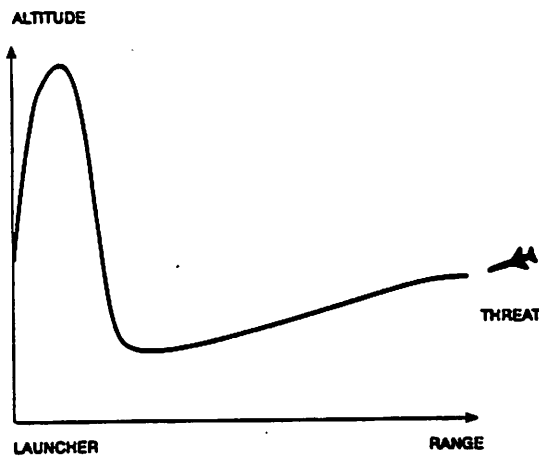


Figure 1. Typical trajectory of a vertically-launched Point-Defense Missile.

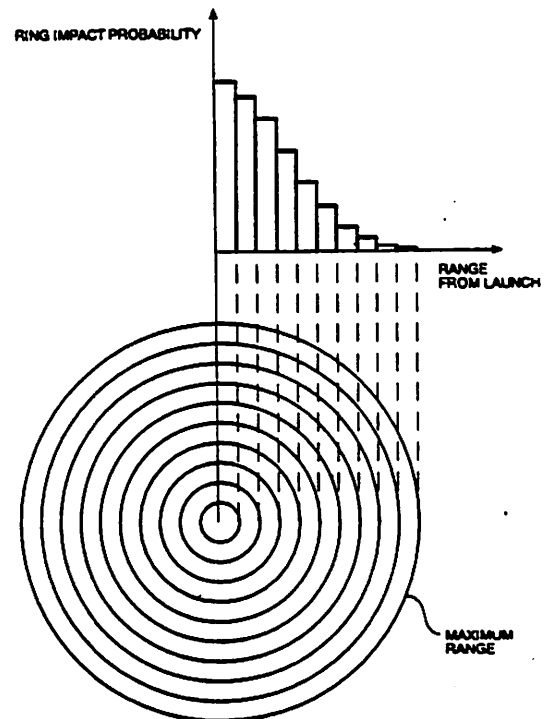


Figure 2. Cross-directional, gaussian, "ragged" impact probability model

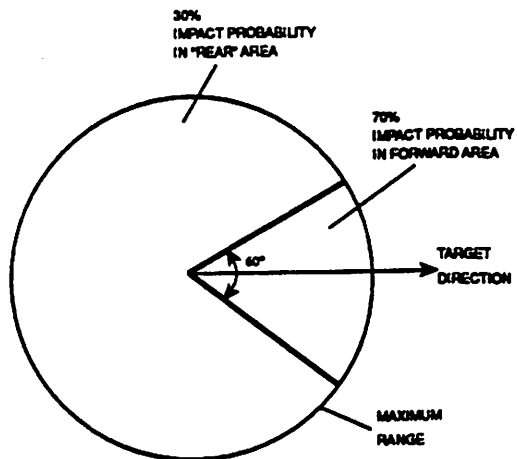
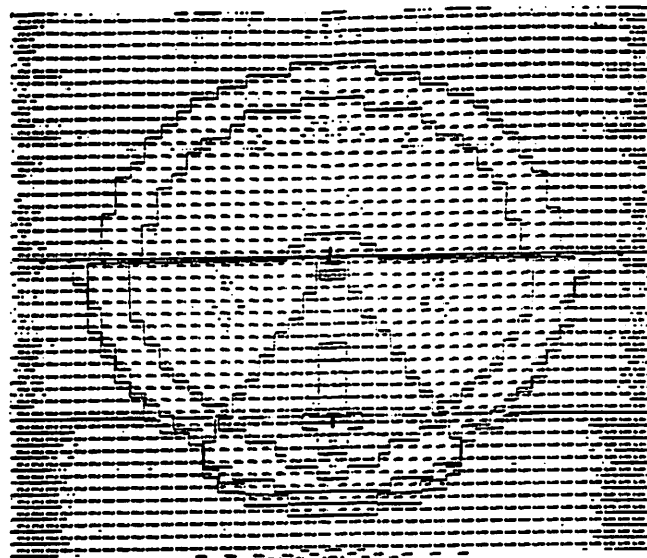


Figure 3. Introducing downwind-dependent impact probabilities into the target model.



L - LAUNCH  
T - TARGET

Figure 4. Impact probability map (adapted from Postman).

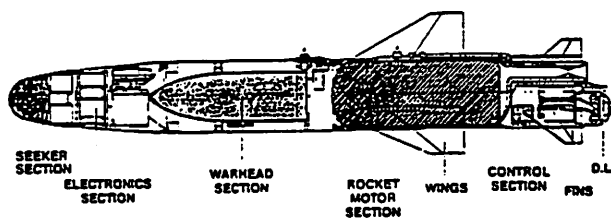
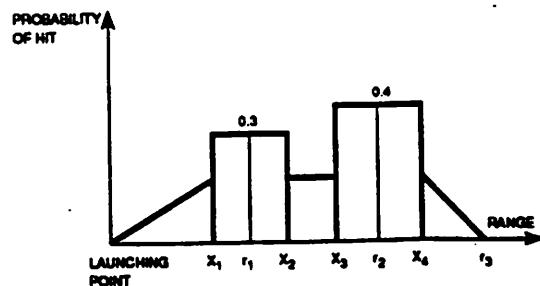
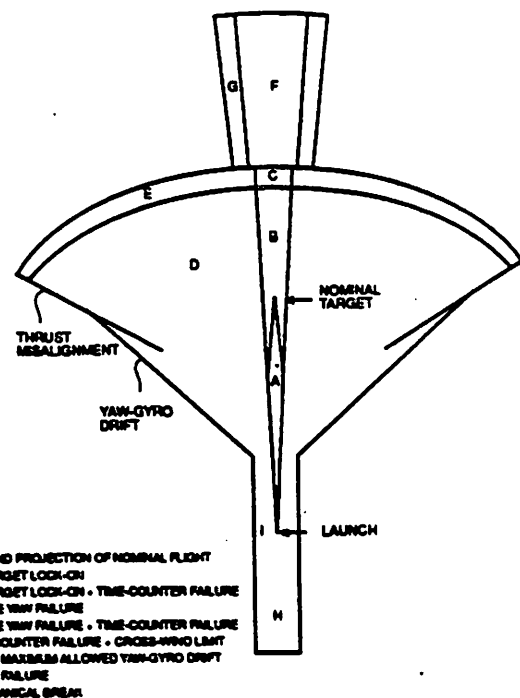


Figure 4. Layout of a typical stand-off air-to-ground attack missile.



- $r_1$  - BALLISTIC FALL RANGE
- $r_2$  - NOMINAL TARGET RANGE
- $r_3$  - MAXIMUM POSSIBLE RANGE

Figure 6. Probability distribution of deep-attack impact, given failure (adapted from Stein-Ory).



- A - GROUND PROJECTION OF NOMINAL FLIGHT
- B - NO TARGET LOCK-ON
- C - NO TARGET LOCK-ON - TIME-COUNTER FAILURE
- D - SINGLE YAW FAILURE
- E - SINGLE YAW FAILURE - TIME-COUNTER FAILURE
- F - TIME-COUNTER FAILURE - CROSS-WIND LIMIT
- G - AS F - MAXIMUM ALLOWED YAW-GYRO DRIFT
- H - PITCH FAILURE
- I - MECHANICAL BREAK

Figure 7. Impact area following identified common failure categories (C).



**SAND93-2173C****NUCLEAR WEAPON SYSTEM RISK ASSESSMENT\*****David D. Carlson**

**Special Projects Department  
Sandia National Laboratories  
Albuquerque, New Mexico 87185-5800**

**INTRODUCTION**

Probabilistic risk assessment (PRA) is a process for evaluating hazardous operations by considering what can go wrong, the likelihood of these undesired events, and the resultant consequences. Techniques used in PRA originated in the 1960s. Although there were early exploratory applications to nuclear weapons and other technologies, the first major application of these techniques was in the Reactor Safety Study, WASH-1400,<sup>1</sup> in which the risks of nuclear power accidents were thoroughly investigated for the first time. Recently, these techniques have begun to be adapted to nuclear weapon system applications.

**NUCLEAR WEAPON SYSTEM CHARACTERISTICS**

Nuclear weapon systems are designed to be exceptionally safe. The warhead is designed with the intent that, under all credible abnormal environments, the device will respond in a predictably safe manner; that is, nuclear detonation will be prevented. This is accomplished by following three safety design principles:

- isolation
- incompatibility
- inoperability

Components critical for nuclear detonation are isolated from the surrounding environment by containment within an energy barrier. By adherence to this principle, electrical energy necessary to cause nuclear detonation is prevented from entering the warhead. Of course, there must be some pathway for energy to get inside the barrier for authorized use. Thus, there is an "entrance" through the barrier that is designed to only allow energy to pass through under very particular circumstances. This entrance is safeguarded by the remaining two principles.

---

\*This work was supported by the U.S. Department of Energy under contract DE-AC04-76DP00789.

The entrance is closed so that, under normal circumstances, energy cannot pass through. However, given unambiguous indications of intent to deliver the warhead, either through human-generated signals or environmental stimuli, the entrance is opened to allow energy to pass through. These entrance signals are engineered to be truly unique inputs, incompatible with natural energy forms that may be present in an accident environment. As a result, the possibility of accidental generation of the signal is incredibly small.

Finally, recognizing that no barrier can be perfectly invulnerable, the system is designed to ensure safe response should the environment be so severe as to cause the barrier to be breached. This is accomplished by incorporating into the design components which must normally function to allow a nuclear detonation under authorized use, but which will fail under relatively mild environmental conditions rendering the system inoperable in abnormal environments. These components, known as "weak links," are engineered to fail in a predictable manner at environmental levels substantially less severe than those that can challenge the integrity of the energy barrier. In this way, safety is assured.

These concepts are incorporated into the warhead design to assure benign response under all credible abnormal environments which may arise in an accident. Thus, safety of the weapon is assured by precluding the necessary energy from reaching the detonators by (1) incorporating a barrier to the energy, (2) protecting the pathway for energy to enter so that it opens only under uniquely signaled human intent or environmental stimuli, and (3) ensuring that in severe environments components necessary for detonation will predictably fail before the barrier is breached.

Recently, the techniques of PRA have begun to be employed to provide added assurance that the system will perform as designed. The PRA methods developed for nuclear power plant risk assessment are being adapted for this application.

## UNDESIRED EVENTS

Given the presence of both high explosives and radioactive material, a significant hazard is present. We accept this hazard in the interests of national security. We control this hazard through the safety principles of the design and through highly skilled operations personnel. Nevertheless, the possibility for accidents exists. Accidents can lead to several levels of consequence, each of which is being explored through the use of PRA.

By far the most likely result of an accident is absolutely no release of radioactive material. However, the possibility does exist for the dispersal of radioactive material. The potential consequence of such an accident depends upon the manner in which the material is dispersed.

The most benign release would involve the mechanical rupture of the warhead and scattering of the material. This would involve minimal amounts of respirable radionuclides and would primarily constitute an environmental cleanup event.

More significant would be a release from the combustion of the weapon or detonation of the high explosive without nuclear yield. Such releases would aerosolize a fraction of the radioactive materials and would result in an energetic release into the atmosphere. Subsequent health effects would be governed by dispersal processes commonly considered in reactor accidents. The driving forces of a high explosive detonation would constitute the more hazardous scenario, both in terms of the amount of material aerosolized and in the dispersal potential.

The possibility of nuclear yield is remote for the reasons cited in the description of the design. PRA techniques are being used to systematically examine the range of environments that the warhead may experience to verify the performance of the design. To ensure that the system is safe, we are examining the performance of the energy barrier and the safety components in abnormal environments to ensure the integrity of the design principles. Moreover, we are evaluating whether there are, in fact, any unintended circumstances that would allow energy to pass through to the detonators.

## **METHODS**

Examination of these issues is being addressed through the adaptation of techniques developed for nuclear power plant risk assessment. Figure 1 presents the series of steps involved in the analysis. While the series of tasks appears similar to those involved in any risk assessment, there are unique aspects in the application to nuclear weapon systems.

### **Environment Definition**

The environment definition evaluates the operations involving the weapon. As in other risk assessments, the number of scenarios to be considered is nearly countless. However, through the use of event tree models, accident scenarios can be enumerated, beginning with the accident initiator and continuing through a consideration of the subsequent events and processes that may occur as the accident unfolds.

While there are many, many scenarios to be considered, of interest to the nuclear weapon system risk assessment are the environments that the weapon may encounter. These may be enumerated as combinations of thermal, impact, electrical, puncture, crush, and immersion environments. Techniques exist that can bin the accident scenarios into these combinations of environments to allow an estimate of both the frequency and severity of environments which the weapon may experience. While these environments form a continuum of conditions, in practice we group environments into regimes of unique interest to weapon response.

### **System Design Characterization**

Combinations of events that could lead to the undesired event, e.g., nuclear detonation, are delineated using fault tree analysis techniques as commonly employed in reactor risk analysis. Weapon design characteristics, however, introduce unique modeling aspects.

First, the failure modes of concern are substantially more restrictive in weapon systems. Reliability of the components is such that a combination of random failures or hardware faults leading to the undesired event is extremely unlikely. Moreover, once the system is assembled, human interaction with the system is nearly nonexistent, nor is test or maintenance performed that would lead to safety component unavailability. Thus, we primarily must consider the possibility of component failure in response to adverse environmental conditions. It is these events for which data must be collected. Given the wide variety of environmental conditions that could be encountered and the limited test information available, data base development presents some unique issues.

In addition, events leading to the possibility of nuclear detonation require precise timing of events. As discussed briefly before, the design incorporates "weak links," which are designed to fail prior to the breach of the energy barrier. Thus, the continued operability of these components must be considered. The fault tree models must consider the conditions under which these components fail to perform as designed—that is, the "weak links" continue to operate even though they are designed to fail—while, at the same time, the energy barrier breaks down. In addition, an appropriate power source must be coincidentally present. This introduces both the unique aspect of continued operability and timing into the model.

### **Physical Response Evaluation**

Given the definition of the environment and the combinations of events that can lead to the undesired event, the analysis must ascertain whether the environment, in fact, could cause these events to occur. This is done through the physical response analysis. While there are analogues to the accident process analysis in reactor PRAs, by its very nature the nuclear weapon system physical response analysis is unique to weapon system PRAs.

Using a combination of mechanical and thermal modeling codes, the external environment is translated into conditions that the components inside the weapon system will experience. Of course, this is time dependent, particularly for thermal environments. Given thresholds for component response, the analyst determines whether component failures occur and the manner in which the component responds. Because timing of events is important, the models must also determine the time at which various events occur.

In theory, the tools exist to evaluate each environment of concern. In practice, however, these highly sophisticated codes are not sufficiently efficient to make detailed calculations of every environment feasible. As a result, we are developing fast running codes that capture the essence of the detailed results to provide an initial screening of environments for further evaluation. Through a combination of these faster running models and our sophisticated thermal-mechanical codes, we seek to address the broad range of environmental challenges that the system may experience.

### **Consequence Analysis**

Evaluation of the consequences of an accident involves the same steps and processes as a reactor accident consequence analysis. The radioactive source term is the unique aspect of the weapon accident. The various release mechanisms discussed above have been evaluated, both experimentally and analytically; the results are incorporated into the codes that are used to track the subsequent dispersal through the atmosphere and the resultant contamination and effects.<sup>2</sup>

### **Integration**

Finally, all of the various elements of the evaluation are integrated together to provide insight into the potential for dispersal or nuclear detonation. Quantitative estimates of plutonium dispersal are being developed using techniques similar to those for reactor analysis. These involve sampling from assigned distributions for the various parameters of

the analysis to develop both an overall estimate of the magnitude and uncertainty of the release. Importance measures and sensitivity analyses are used to develop further insight.

Nuclear detonation evaluations, to date, are qualitative in nature. The possibility of detonation is being evaluated, and the circumstances leading to nuclear detonation are being sought. Due to the very peculiar circumstances that would be required to lead to a detonation, the estimated probability would be extremely small. This provides significant challenges in identifying the circumstances and in providing a meaningful probability estimate. These areas are under active investigation.

## CONCLUSION

Risk assessment techniques are being applied to nuclear weapon systems to quantitatively estimate the potential for radioactive material dispersal and to qualitatively evaluate the possibility for nuclear detonation. Unique aspects of nuclear weapon systems require adaptation of techniques used in other technologies and, in some cases, challenging new methodological development. These approaches are under active investigation to provide the nation with confirmation that our nuclear weapon systems perform safely as expected in all credible accident situations.

## REFERENCES

1. U.S. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400, NUREG-75/014, Washington, D.C., October 1975.
2. B. A. Boughton and J. M. Delaurentis, "Description and Validation of ERAD: An Atmospheric Dispersion Model for High Explosive Detonations," SAND92-2009, October 1992.

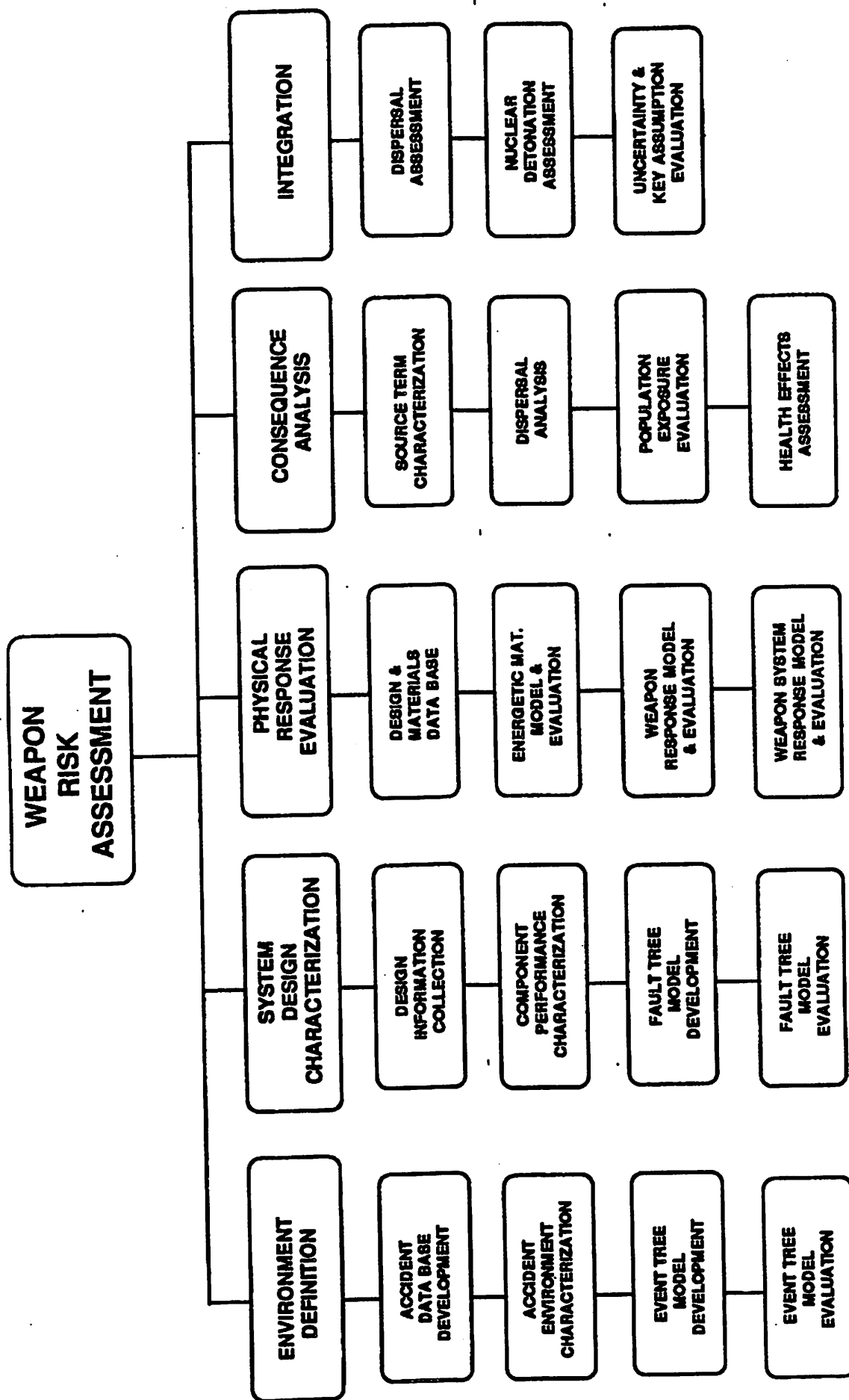


Figure 1. Steps in Nuclear Weapon System Risk Assessment

## PROBABILISTIC RISK ASSESSMENT OF DISASSEMBLY PROCEDURES

D. A. O'Brien, T. R. Bement, B. C. Letellier

Los Alamos National Laboratory, MS F684  
Los Alamos, NM 87545

### 1. Background and Charter For The Study.

The purpose of this report is to describe the use of Probabilistic Risk (Safety) Assessment (PRA or PSA) at a Department of Energy (DOE) facility. PRA is a methodology for i) identifying combinations of events that, if they occur, lead to accidents, ii) estimating the frequency of occurrence of each combination of events and iii) estimating the consequences of each accident.

Specifically, the study focused on evaluating the risks associated with disassembling a hazardous assembly. The PRA for the disassembly operation included a detailed evaluation only for those potential accident sequences which could lead to significant off-site consequences and affect public health. The overall purpose of this study was to investigate the feasibility of establishing a risk-consequence goal for DOE operations.

### 2. Methodology

The methodology outlined in Figure 1 was used to estimate the risk to the population surrounding the plant. The following summarizes the analysis process:

1. Written procedures and other applicable documentation were obtained and reviewed. These included disassembly procedures currently in use and records of the engineering and development of the hazardous assembly.
2. A two-day HAZards and OPerability analysis (HAZOP) was conducted. Unresolved issues raised during the HAZOP meeting were addressed by experts who developed the hazardous assembly.
3. A two-day site visit was conducted where all disassembly operations were observed. There were several opportunities for discussions with engineers and technicians responsible for disassembly operations.
4. Following the site visit, a number of deterministic calculations were done. These were done as part of an initial attempt to identify those accidents that could be ruled out and those that could clearly lead to significant off-site impact.
5. Event trees and fault trees were then constructed for those operational accidents that have potential off-site consequences.
6. Probabilities for failure (errors) and their associated uncertainties were determined

or estimated for both the event trees and the fault trees.

7. Fault tree and event tree equations were solved using the Set Equation Transformation System (SETS).<sup>1</sup> The associated calculations of propagated uncertainties for the errors were done on the sequence cut sets using the Top Event Matrix Analysis Code (TEMAC).<sup>2</sup> This gave the accident frequency with its associated uncertainty.
8. The consequence analysis modeled the atmospheric transport of accident-caused hazardous material as well as the resulting ground contamination and the latent cancer fatalities (LCFs). Weather variations and source term uncertainties were taken into account. This gave the likelihood of an effect (contamination or LCFs) with the associated uncertainty *given an accident*.
9. The accident frequency and likelihood of an effect were then combined probabilistically to give the final frequency of an effect with an associated uncertainty.

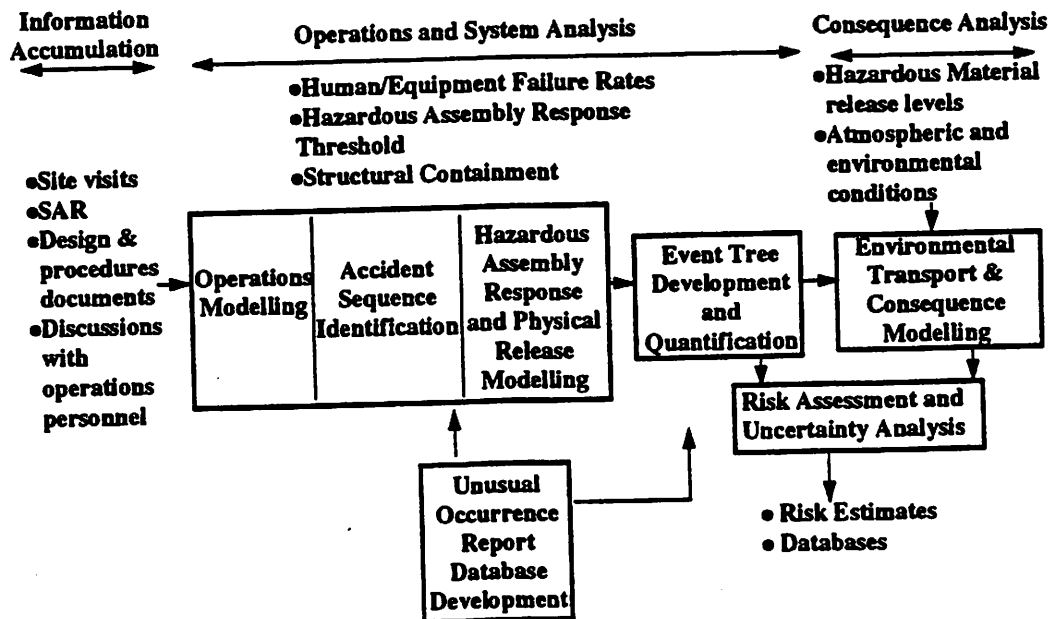


Figure 1. Outline of PRA methodology used for analysis of disassembly operations.

### 3. HAZards and OPerability (HAZOPs) Analysis

A HAZOP is a systematic method for identifying operations that have serious accident potential. A HAZOP is performed by having an interdisciplinary team of experts systematically examine a process and its procedures to attempt to identify the effects of departures from standard procedures. Experts then determine if the departures will create hazardous conditions. Identification is also made of actions or systems that mitigate the consequence.

Each step in the disassembly procedures was reviewed by the HAZOP team. Also, a training videotape showing correct disassembly was reviewed. Tables like Table 1 were developed for each procedure, listing all steps and hazards. The hazards included impact, fire, chemical, electrical, and radiological. Each of the potentially hazardous steps were then used, after screening, as event tree headings for accident-sequence identification.

### 4. Event and Fault Tree Development

Event trees were used to quantify the possibility of off-site consequences caused by disassembly accidents. Unlike reactor "accident-sequence analysis", where event trees are de-



veloped for each accident initiator and each branch on an event tree represents an accident mitigating system, the event trees in this study were developed around the normal disassembly procedures. The entry points (corresponding to the usual initiating events) for the event trees were the beginning of specific procedures and not the occurrence of an accident. All of the probabilities obtained by solving these trees were on a per disassembly basis rather than on a time or frequency basis and were converted to yearly frequencies by multiplying by the number of disassemblies each year.

**Table 1. Sample Hazardous Operations Analysis table.**

Step No.	What If..;	Direct Consequence	Increased Vulnerability	Protection or Mitigation	Interactions with Other What Ifs	Disposition
W	Hoist failure; handling; lifting and rotating	Dropping assembly	Refer back to T- same	Well protected by case; front section	---	Revisit
X	Electrical bonding failed; result susceptible to static discharge	Low-energy components could fire	Common squibs; vulnerable to firing	Low-energy--contained and protected	---	Revisit
Z	Front dropped on center	None	None	Well sealed center; protected	None	None

Each operation identified by the HAZOP was represented by a top event on an appropriate event tree (an illustration of this is given in Figure 2). The top events were developed further by constructing fault or human error trees. In some cases, the human error trees were developed to feed information into fault trees. An example of a fault tree feeding into a top event (from Figure 2) is shown in Figure 3, where a human error, Failure to Electrically Bond, is further developed in a subsequent human error tree, Figure 4. In developing the human error trees, the procedural steps were broken down into fundamental human actions for which some kind of failure rate could be estimated. It should be noted that the trees presented in this paper are for illustration purposes only and do not represent the actual trees developed.

## 5. Human Error Estimation

Several branches of the event trees and basic events in the supporting fault trees involve human actions that can lead to human errors. These human activities were modeled using human error trees, which were developed using the methods described in Swain and Guttman.<sup>3</sup> The process of developing the trees involves breaking down the procedural steps into those fundamental actions for which typical failure-rate data can be obtained from data bases or estimated in some other reasonable manner. These trees themselves are relatively simple, with binary branching corresponding to success or failure of each activity. However, in a few cases, multiple branching is used to include recovery actions. In these cases it is necessary to account for the fact that different levels of recovery can occur depending on how many previous errors have occurred.

In general, a branch to the right (labeled by a lower case letter) by convention will correspond to a failure to properly complete an activity. A branch to the left (labeled by an upper case letter) corresponds to successful completion of an activity. Depending on what the activity is, a "failure" to complete a procedural step in some cases might actually lead to a less hazardous condition. Therefore, terminating branches of the trees are labeled with an "s" or "f" to indicate whether that sequence is considered an overall "success" or "failure".

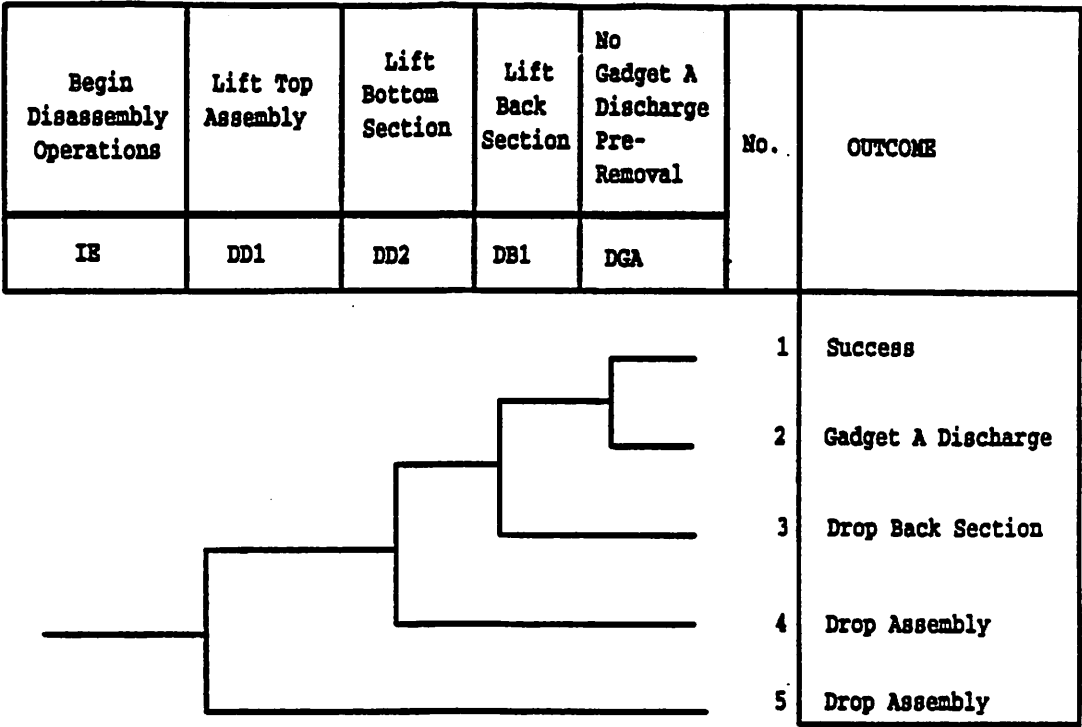


Figure 2. Sample Event Tree.

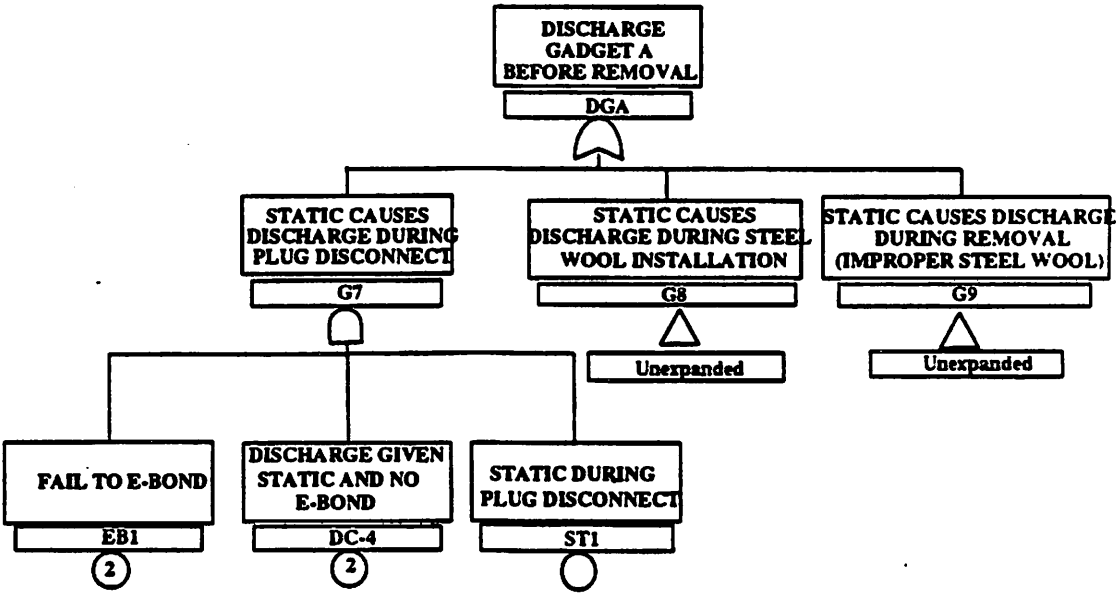


Figure 3. Sample Fault Tree.

6. Integration of Risk Sources - Consequence Analysis

The Sandia National Laboratory "ERAD" code was selected for use in this study. It is a constant weather, flat terrain model with a sophisticated detonation plume-rise description, and a Monte Carlo particulate transport package. The code assumes that the atmosphere conditions vary only with altitude.

ERAD takes account of the variation of particle settling rate with particle size, and

treats the stochastic nature of particulate diffusion under unstable atmospheric conditions. ERAD outputs land contamination and integrated air concentration data on a grid extending down wind from the source point. A post processor was used to plot contours of contamination level and potential inhaled dose (for an assumed ICRP standard human, breathing at 330 cc/sec). Plumes were tracked to any distance necessary to bound the regulatory action limit contour of 100 mrem for inhalation and .2  $\mu$ ci for deposition, typically 80 to 100 km. This analysis was repeated for 60 typical weather profiles for the area, and the resultant "potential inhaled dose" contours were combined with appropriate weather probabilities, accident probabilities, and population data to produce expected area contamination and population radiological exposures (person-rem) per disassembly operation.

Each set of 60 weather profiles with a single source term yields 60 consequence values which can be expressed as a cumulative distribution function (CDF). Each CDF can be subtracted from one (1) and expressed as a complimentary CDF (CCDF). If the CCDF is multiplied by the accident frequency, the resulting exceedance function (EF) gives the unconditional frequency of a consequence at least as severe as a specified value.

Randomly chosen source-term values were paired with randomly chosen accident frequencies to yield 40 EFs. Figure 5 shows a hypothetical example of 40 EFs for a consequence metric. From this set of EFs, one can determine the expected value (mean) and range of likely values (the 5th and 95th percentiles) of the exceedance frequency over a range of consequences.

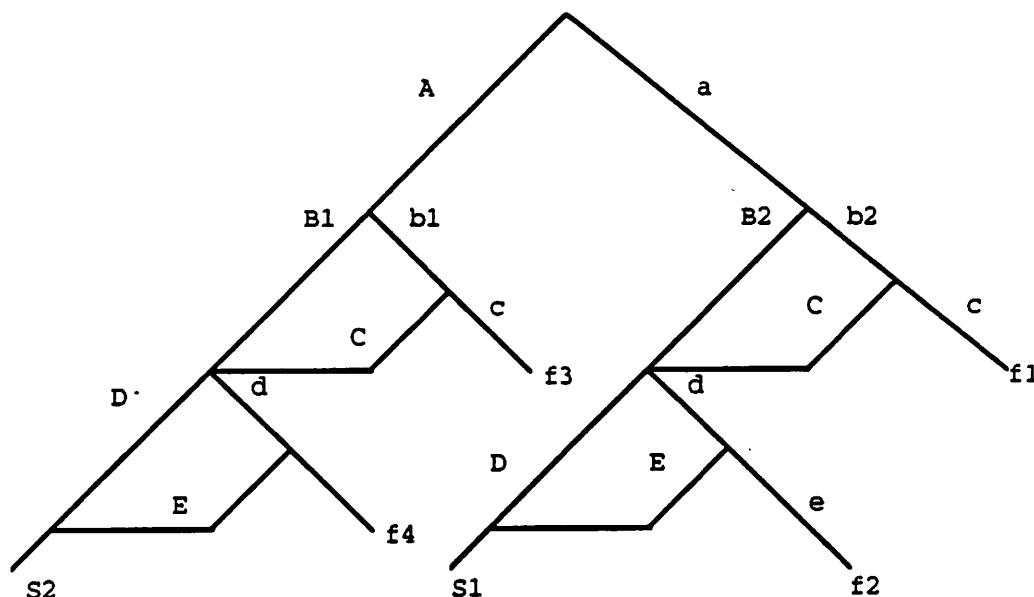


Figure 4. Human error tree for electrical bonding.

## 7. Risk of Disassembly Operations and Risk Reduction Measures

Using the actual trees developed for this study, the risk of the disassembly procedure was found to be very small. The expected individual risk for latent cancer fatality was calculated to be  $3.5 \times 10^{-12}$  per individual per year. This is many orders of magnitude less than the Secretary of Energy goal for nuclear facilities of  $2 \times 10^{-6}$  per individual per year (which equates to less than a 0.1% increase in an individual's risk of cancer).

The true benefit of the PRA approach, though, is in risk reduction. By providing importance measures for basic events, the analyst can determine which events contribute the most to the accident frequency. Plant operators may then be able to implement positive measures to minimize the likelihood of the important base events occurring. This is clearly an iterative

process in which plant operators are heavily involved.

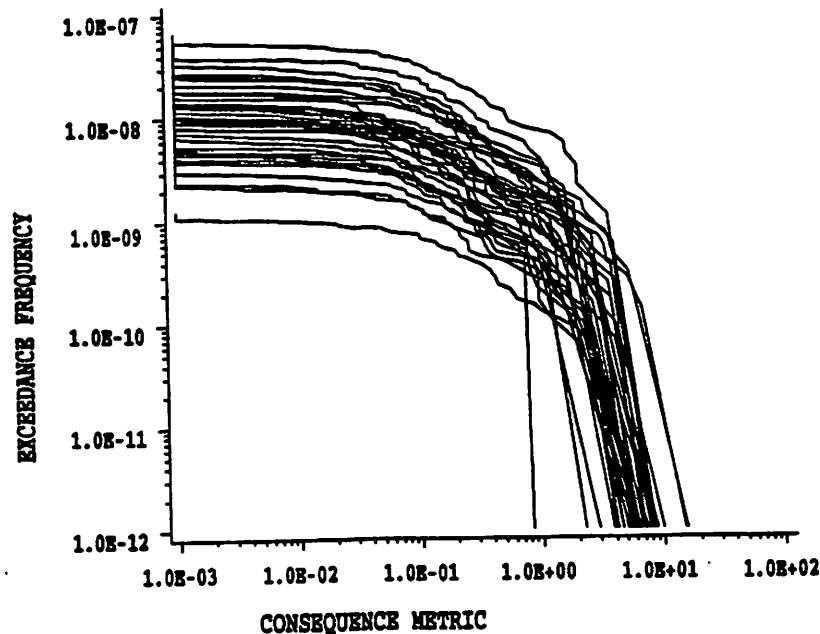


Figure 5. Generic example of 40 Exceedance Frequency vs. Consequence curves.

## 8. Conclusions

Several conclusions were drawn from this study:

- ☐ PRA can provide a rigorous, systematic approach to safety assessment for DOE operations,
- ☐ PRA can be used to evaluate total risk and provide a consistent framework for risk management,
- ☐ Though the uncertainties in the final numbers are large, qualitative interpretations of results are valuable in identifying
  - the safety benefits (gains) of proposed positive measures,
  - the relative risks posed by various parts of the process or procedure,
  - areas needing further study which will have the greatest effect on reducing uncertainty.

Finally, the analysts concluded that the establishment of a DOE risk criteria (regulatory criteria) was premature.

## 9. References

1. D. W. Stack, "A SETS User Manual for Accident-Sequence Analysis," Sandia National Laboratories report SAND 83-2230, NUREG/CR-3547 (January 1984).
2. R. L. Iman and M. J. Shortencarrier, "A User's Guide for the Top Event Matrix Analysis Code (TEMAC)," Sandia National Laboratories report SAND 86-0960, NUREG/CR-4598 (August 1986).
3. A. D. Swain and H. E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (Final Report)," NUREG/CR-1278-F.

**096 Risk Communication to the Public**

*Chair: M.E. Pate-Cornell, Stanford U*

**Effectively Communicating Risk to the Public and to Regulators: Can It Be Accomplished?**

*G.M. Pilie, G.T. Croxton (Adams & Reese)*

**Effectively Communicating Risk Assessments to the Public**

*C. Lambert, M. McDaniel (UNOCAL); S. Santos (FOCUS Grp.)*

## **EFFECTIVELY COMMUNICATING RISK TO THE PUBLIC AND TO REGULATORS: CAN IT BE ACCOMPLISHED?**

Glen M. Pilié, Gayle Tennison Croxton

Adams & Reese  
4500 One Shell Square  
New Orleans, Louisiana 70130  
(504) 581-3234

### **INTRODUCTION**

One of the many challenges faced by industrial facilities, environmental managers and their lawyers is to effectively communicate the comparative risks posed by an operating facility or a waste site. These relative risks must be communicated to the public, to regulators and to our legally designated peers, civil juries, in a fashion which they can readily understand. These parties must be informed as to the potential risks posed by emissions and releases from a facility as compared to the risks encountered in everyday life. Successful communication of risk is an important step toward peaceful coexistence with surrounding communities and thus, toward avoiding litigation. For example, if a facilities' neighbors understand the relatively low risk of harm posed by a release or an incident, they may be less likely to bring a lawsuit against the facility for fear of disease or nuisance caused by that incident. Furthermore, an understanding of the risks posed by a facility or a process on the part of regulators will likely result in increased cooperation from the regulator. Such cooperation is beneficial to a facility during permitting, other regulatory procedures and civil litigation and may help avoid unnecessary expenditures.

### **RISK ASSESSMENT AND REGULATORY POLICY**

An additional problem facing industry and environmental managers is the use of risk assessments to formulate regulatory policy. Risk assessment is used to set exposure standards for the general public in some cases, for workers, and for hazardous waste site cleanups, among others.

As an example, the Environmental Protection Agency (EPA) relies heavily on risk assessment in setting cleanup standards under the Comprehensive Environmental Response, Compensation and Liability Act (CERCLA). In many cases, particularly where soil contamination is suspected, published cleanup standards are nonexistent. In such cases, EPA often conducts a site-specific risk assessment. These risk assessments are directed by the Agency's

risk assessment guidance<sup>1</sup>, often referred to as RAG. This document contains several "standard default exposure factors" or assumptions used in conducting risk assessments. These assumptions are quite conservative, however, and result in estimates of risk significantly higher than those likely to affect people nearby. In 1991, EPA issued another guidance document for use in risk assessment which adds even more conservatism to the process. The directive issued by the Office of Solid Waste and Emergency Response (OSWER) provides that three of the six variables in the standard exposure equation are "upper bound values" referring to the 95th percentile of the risk range. A commentator pointed out that using a simple relationship from probability, multiplying these three numbers results in a value close to the 99.8th percentile.<sup>2</sup> Loosely translated, the number means that a fraction of one percent of the population is expected to have an increased risk. This level of exposure is significantly more conservative than the Agency's stated goal of determining the "reasonable maximum exposure."

Furthermore, an additional dose of conservatism is often added to risk assessments at EPA's regional level. Agency personnel tend to interpret guidance even more conservatively than it is written. To determine the health risk posed by a site, the regions very often make multiple "worst-case" assumptions which make the risk assessment virtually incredible. In particular, exposure factors are often used that stretch the bounds of credibility. At a site, for example, the Agency will assume that the entire quantity of material present is toxic when the data shows that a percentage of the material is not toxic. The agency may also assume, when sampling shows varying concentrations of toxics, that the highest level of contamination is present at the entire site. These worst-case assumptions are often used instead of useful scientific data that is specific to the site at issue. In addition, the EPA often relies on exposure scenarios that ignore reality. For example, EPA may assume that a family builds a house on top of a contaminated site, eats vegetables grown in the contaminated soil, and sinks a well on the site from which the family drinks water every day for 70 years. EPA may assume a trespasser scenario wherein a child repeatedly swims in a contaminated pond many times a year for several years and regularly ingests the water. At one site, the agency assumed that children would breach the cap at the site ( 5 feet of clay) and ingest the soil below.<sup>3</sup>

Finally, the agency often extrapolates animal data to make determinations regarding safe levels of human exposure. This procedure necessarily involves policy choices which have little relation to the scientific determination of whether exposure to a particular substance is dangerous to humans. Furthermore, the use of laboratory animal data has several significant shortcomings. When conducting experiments on animals, scientists often subject the animals to very high doses ensuring an adverse result.<sup>4</sup> Such doses are decidedly above those incurred by humans. In addition, the animals used in such studies may respond to a substance in a way that is very different from the human response. Varying responses are due differences in physiology, metabolism and sensitivity of humans and animals. Lastly, often times the route of exposure and the duration of exposure of the animals are completely unlike those possible in a human exposure scenario.

These assumptions and scenarios are unreasonable and have no scientific foundation. Their use as a basis for regulatory action results in unnecessary and very costly remedial goals. Under the current risk assessment system, substantial amounts of money are spent to cleanup these highly speculative risks. Industry consequently finds itself in the difficult position of challenging EPA's risk assessment, and having to explain to the public why EPA's assessment of the risk posed to public health by the site is overly conservative.

---

<sup>1</sup> *Risk Assessment Guidance for Superfund, Volume 1, Human Health Evaluation Manual* (EPA 1989).

<sup>2</sup> R.H. Harris and D. E. Burmaster, *Restoring Science to Superfund Risk Assessment, Toxics Law Reporter* 6:1320 (March 25, 1992).

<sup>3</sup> *Id.* at 1321.

<sup>4</sup> V.L. Dellarco and C.A. Kimmel, *Update on Noncancer Assessments, EPA Journal* Jan.-Mar. p. 31 (1993).

The large number of conservative assumptions and policy decisions which make up risk assessments render them questionable as objective scientific tools. Multiple layers of worst-case factors and assumptions that ignore reality undermine the credibility and reliability of risk assessment in the regulatory setting. Nonetheless, once the risk assessment is put out for public consumption by a governmental agency, the risk becomes reality. At this point, it is very difficult for industry, which already is suspect in the public's eye, to successfully communicate and point out the scientific flaws and lack of reality contained in the risk assessment.

## COMMUNICATION OF RISK

Communication of risk through risk assessment results is particularly challenging when the audience is the public or lay persons serving on civil juries. The job of effectively communicating risks associated with chemical emissions is compounded by the seemingly constant barrage of negative publicity that the chemical, petroleum and petrochemical industries receive. A prime example of this is the fairly recent phenomenon of negative press coverage associated with toxic release inventory reporting. This reporting, a requirement of the Superfund Amendments and Reauthorization Act (SARA) of 1986, quantifies the amount of specified substances released from a given facility. While the raw numbers show that the quantity of chemicals released is declining each year both overall and for specific facilities, media reports focus on the number of tons of substances released countrywide. The significant progress which is made every year at reducing these releases while maintaining productivity is rarely even mentioned.

In addition to media attention, this statutory reporting has been discovered by plaintiff attorneys as a vehicle upon which to base toxic tort lawsuits which, among other things, typically include a claim for increased risk of future disease or fear thereof. Such lawsuits squarely put at issue the ability of companies as defendants and their lawyers to communicate to plaintiffs and ultimately to judges and juries, the related risk associated with their reported releases. A key part of this communication process is always the formulation of a comparative risk analysis. Beyond formulation of the technical analysis, however, lies the more difficult problem of overcoming the negative bias which already exists in the public's mind, *i.e.*, the jury, and effectively communicating a technical concept to a non-technical audience.

Research into how laypersons perceive risk indicates that unfavorable media coverage and negative imagery associated with large industry, especially the chemical, petroleum and petrochemical industries, makes overcoming these biases very difficult.<sup>5</sup> Individuals base their perceptions of what is "risky" on a combination of factors, many of which are unrelated to scientific determinations of risk based on the number of deaths expected annually. These factors, such as dread, fatal consequences, voluntariness, controllability and familiarity, are often based on emotions and have little scientific certainty. For example, in one study experts rated the risk of nuclear power twentieth out of thirty activities and technologies in light of the low number of injuries or deaths from nuclear accidents. College students, however, ranked nuclear power as the single riskiest of the thirty activities and technologies.<sup>6</sup> These and other studies indicate that laypersons' perception of risk includes many personal, subjective factors other than the scientific quantification of risk used by experts. This broad conception of risk makes the task of accurately conveying the meaning of risk assessments to the public even more difficult. Because people's perceptions of risk are based on a broad range of factors, attempts to alter those perceptions based on technical data and statistics will likely meet resistance. Furthermore, to many people, statistical methods and probabilistic processes are difficult to comprehend.

<sup>5</sup> P. Slovic, Perception of Risk, *Science* 236:280 (April 1987).

<sup>6</sup> *Id.* at 281.



Effective communication of risk is twofold, it must make scientific and technical determinations of risk easy to understand for laypersons and it must address those emotional and cognitive factors which comprise laypersons' perceptions of risk. Evidence indicates that the presentation of scientific and statistical data has a significant effect on whether juries understand the meaning of the data<sup>7</sup>. Visual aids, including video presentations, as well as clear and simple language are often useful. In a trial setting, allowing jurors to take notes and ask questions has been effective. Furthermore, presentation of complex information by a neutral expert as opposed to dueling experts has been suggested as a way to reduce confusion. Finally, experts and others seeking to influence risk perceptions must understand the factors upon which laypersons base their perceptions of risk.

## LEGAL IMPLICATIONS

While companies and environmental managers focus on statistics and technical risk assessments to make business decisions, legal liability is often based on contrary principles. A company may find itself in litigation in which it may be held liable simply by virtue of its operations. The legal doctrines of strict and absolute liability often provide that where dangerous substances are involved, any level of risk is unacceptable. In these instances, a company may be liable regardless of the prudence and diligence it exercises. For example, in many cases the plaintiff only has to prove that 1) he has been damaged, and 2) that the damage was caused by activities at or conditions of his neighbors property. The plaintiff is not required to prove that the specific facility which caused the damage presents an unreasonable risk of harm.

Furthermore, liability may be imposed upon those engaged in "ultrahazardous" or "abnormally dangerous" activities. The plaintiff must only prove that the facility is engaged in an activity that can cause injury to others, even when conducted with great care. Courts have found that the generation, treatment and handling of hazardous waste is an "abnormally dangerous" activity and, thus, subjects the facility to strict liability regardless of the level of care exercised.<sup>8</sup> Other operations deemed "abnormally dangerous" include oil refining, shipment of chemicals, and disposal of toxic wastes. Once the plaintiff establishes that the activity at issue meets the definition of "abnormally dangerous," there are no defenses to liability. In addition, some states allow the plaintiff to recover punitive damages against companies which engage in "abnormally dangerous" activities. These damages are levied over and above those necessary to compensate the plaintiff for injuries sustained, and are entered in order to punish a wrongdoer. These legal principles disregard risk analysis and can limit the value of risk assessment in decision making.

## CONCLUSION

Risk assessments are often touted as objective, infallible determinations which are dispositive of the question of the potential harm posed by a particular activity. In reality, however, these assessments often raise public relations and regulatory questions that may also have legal implications. The education of the public, jurors, and regulators can engender an understanding of risk assessments, their uses, and their limitations. Furthermore, regulators must be urged to maintain the line between objective assessments and policy decisions, and to recognize the differences. Risk assessments, in their proper context, can help the public and regulators to set priorities and can help to direct monetary and other resources.

<sup>7</sup> J.S. Cecil, V.P. Hans and E.C. Wiggins, *Citizen Comprehension of Difficult Issues: Lessons From Civil Jury Trials*, *American University Law Review* 40:759 (1991).

<sup>8</sup> *Lutz v. Chromatex, Inc.*, 718 F.Supp. 413,430 (M.D. Pa. 1989).

## **EFFECTIVELY COMMUNICATING RISK ASSESSMENTS TO THE PUBLIC**

Charles E. Lambert,<sup>1</sup> Mary F. McDaniel,<sup>1</sup> and Susan L. Santos<sup>2</sup>

<sup>1</sup>UNOCAL Corporation  
1201 West 5th Street, P.O. Box 7600  
Los Angeles, CA 90051

<sup>2</sup>FOCUS GROUP  
29 Welgate Road  
Medford, MA 02155

### **INTRODUCTION**

Efforts to communicate risk are often hampered by the lack of a common language between professionals working on the risk assessment and the audience. Terms such as "significant risk", "background level" and "adverse health effects" have different meanings to the risk assessor and to the lay public. Research indicates that the public perceives risk quite differently than scientists and policy and decision makers. Experts tend to view risk in terms of the hazard that contaminants or processes pose, the exposure to the hazard, and the probability of the event occurring. The public assesses risk on the basis of a wide range of characteristics (1) many of which have to do with attributes not related to toxicity, exposure or probability. One of the most difficult aspects of risk communication is creating a common language with definitions that are understood by everyone.

As the public's "right to know" broadens, there has been a growing trend to release risk assessment documents and numeric risk calculations to the community at large. For example, in California, AB2588 the Air Toxics "Hot Spots" Bill, requires that risk assessment information be communicated to employees and neighboring communities. Sometimes community health concerns, rather than regulatory mandate, call for risk assessments to be commissioned and communicated. In this paper we discuss problems of conveying risk assessment information to varied audiences and the need to present information in the overall framework of a risk communication strategy. An example of the communication of risk information is described along with recommendations for improving communication.

## **RISK ASSESSMENTS HAVE A LIFE OF THEIR OWN**

Risk assessments have traditionally been produced with a specific purpose and audience in mind, such as satisfying a regulatory requirement. But in reality, the document ends up in the hands of many different audiences including: the general public, environmental activist groups, potential litigants, other regulatory agencies, the press, and local, state and federal government. These parties have different agendas and levels of technical knowledge which can lead to diverse interpretations of the document. As public documents, risk assessments can end up almost anywhere and used for purposes never originally intended. For example, the use of California's Air Toxics "Hots Spots" risk assessments by the District Attorney's office to ensure company compliance with Proposition 65. Because of different audience needs, risk assessments need to be easily understandable and responsive to each audience's questions. The document or supplemental information must clearly define the purpose of the risk assessment, how the information will be used, and how the information will be translated into risk management decisions.

## **AN EXAMPLE OF A POORLY COMMUNICATED RISK ASSESSMENT**

We recently experienced the reaction resulting from the public release of a risk assessment which was performed to answer community concerns about an industrial facility in a residential neighborhood. In response to concerns that the company's contracted risk assessment would be biased towards underestimating the risk, an environmental/engineering consulting firm was selected by a citizen's committee to perform what was seen as an "independent risk assessment". UNOCAL agreed to fund this health risk assessment as part of a risk communication strategy. The objective was to empower the community so that it could reach its own conclusions regarding health risk, rather than debate the community on the level or significance of "risk" that the company and public define differently. The intent was to provide clear information, build credibility and ultimately, to engage the community in discussions of what needs to happen differently to achieve resolution of community fears and concerns. Several problems hindered the public's interpretation of the risk assessment: many number-intensive tables that had no real import to the document, including "numbers" for numbers sake, scientific notation and units not explained and not consistent throughout the document ( $\text{ug}/\text{m}^3$  and ppm were used interchangeably), lack of an executive summary, or clear conclusions. From our experience, this is not a unique case, but tends to be the norm for risk assessment documents.

Risk assessment documents should be prepared with the prospective audiences in mind. A team approach, including risk assessors, engineers, risk managers and risk communicators, should be applied to both writing and presenting the final document. The key is to make information accessible by avoiding the use of technical jargon and regulatory phrases. Professional risk assessors need to recognize "non-technical" characteristics that the public considers in assessing risk: whether the risk is voluntary or involuntary, artificial or natural, whether "dread" substances are involved, and whether or not children are particularly at risk. In addition, if the public distrusts the risk information source, particularly if that source is industry, this must be taken into account.

## CAUSES OF, AND REMEDIES FOR, A POORLY COMMUNICATED RISK ASSESSMENT

The implications of a poorly communicated risk assessment are numerous. An unintelligible report forces the public to rely on other sources of information such as the press or activist groups. These groups provide interpretations of the document which may be biased, inaccurate, or both. The failure to provide an intelligible report may force the press to rely on second-party interpretations. A poorly written or inappropriate document can aggravate and alarm a community unnecessarily and does not lead to constructive risk management.

Given the complexity and importance of risk assessment information and the increasing public demand for such information, it's critical to write a report that is clear and meaningful to a community audience. As a result of our experience with this risk assessment, we have come to a number of conclusions about what makes risk assessment documents effective or ineffective vehicles for communicating risk. Suggestions for an effective document include:

- Putting the report in narrative form to tell a story that the concerned individuals can follow to a meaningful conclusion.
- Providing a clear executive summary that presents conclusions in "sound bites" that are media friendly and could appear in the local press.
- Having a non-technical "naive reader" review the report to see if it answers the questions that led to the risk assessment in the first place. Focus groups and pretesting of the material should also take place before the document is released in final form.
- Presenting the material graphically instead of using tables or other number-dense formats.
- Placing the highly detailed technical material in separate appendices, rather than including it in the body of the report.

## CONCLUSION

In conclusion, the goal of communicating a risk assessment is to share technical information with a number of different audiences in an understandable way, and to empower these audiences to reach their own conclusions about the actual risk. To achieve this end, a prospective risk assessment contractor should be not only technically competent, but also capable of communicating clearly to many different audiences. Communicating about health and environmental risks will always be emotionally charged. It will continue to present technical experts with challenges they are often not well equipped to manage. Integration of risk communication concerns at the beginning of the risk assessment process is essential to the positive acceptance of the document by all concerned audiences. Ultimately, those responsible for assessing and managing risks must come to terms with the public's definition of risk and understand that this definition is based on more than just the public's difficulty in understanding technical information. The communication of risk assessment information must be part of a broader risk communication strategy - one that recognizes that effective environmental management is multifaceted and that communication must be two-way. If communication planning isn't included as part of the risk assessment process, communicating "results" will continue to be frustrating for all those involved.

## REFERENCES

1. P. Slovic, F. Baruch, and S Lichtenstein. Facts and fears: understanding perceived risk, in: "Societal Risk Assessment: How Safe is Safe Enough," R.C. Schwing and W.A. Albers, eds., Plenum, New York (1980).

**097 Broad Risk Perspectives Within the DOE Weapon Complex**

*Chair: H.P. Alesso, LLNL*

**A Global Overview of Risk Management of the DOE Complex**

*H.P. Alesso, K.C. Majumdar (LLNL)*

**The Integration of Human Factors into the Risk Assessment of a Nuclear Device Arming and Firing System**

*T. Altenbach, W. Ferrell (LLNL)*

**A Method for Determining Risk to Ground Facilities from Aircraft Accidents**

*C.Y. Kimura, C.T. Bennett (LLNL)*

## **A GLOBAL OVERVIEW OF RISK MANAGEMENT OF THE DOE COMPLEX\***

**H.P. Alesso, and K.C. Majumdar**

**Lawrence Livermore National Laboratory  
Nuclear Test Engineering Division  
Lawrence Livermore National Laboratory**

### **ABSTRACT**

No endeavor is risk-free and as we realize the inherent risks in society, our only viable solution is to manage the risk. Application of an integrated risk management program of a large technological system like the DOE complex is a difficult task; but it is the only rational means to optimize the risk-benefit equation.

An effective risk management culture within the DOE complex will in the long run, ensure a consistent response to mitigate identified risks.

An effective risk management program provides responsible administrative planning and logical application of the best technical analyses. It requires the involvement of all personnel.

A risk management program utilizes the following broad risk management principles:

1. Integration
2. Risk/safety goal
3. Risk awareness and perception
4. Planning, communication and implementation for risk avoidance, risk mitigation and risk benefit optimization
5. Risk management tools: risk assessment and decision analysis.

Some specific elements are: hazard identification, risk assessment, risk mitigation, emergency planning, incident investigation, audits, training, procedures (operating, maintenance, testing and inspection, and change control), and continuous improvements through feedback.

Currently, risk management methods, applications, and results have not yet been demonstrated in a uniform self-consistent effort throughout the DOE complex.

The quality assurance review of so many diverse applications, methods, and differing results presents a complex risk management issue for DOE.

Our objective in this paper is to point out broad perspectives that raise concerns about future DOE risk management issues and to suggest some possible remedies.

---

\* This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract no. W-7405-Eng-48.

## **A GLOBAL OVERVIEW OF RISK MANAGEMENT OF THE DOE COMPLEX**

### **1.0 INTRODUCTION**

#### **1.1 Background**

The DOE complex consists of a diversity of facility types including; reactor, non-reactor, weapons, chemical process, and others. Many of these diverse facilities are physically located in a single geographical location (See Table 1). These facilities operate complex technological systems that have potential risks (like any other modern technological process) to facility personnel, the general public and the environment.

As the global political changes have affected DOE/DOD planning and policy, new priorities have emerged. The nuclear weapons dismantlement efforts have become a primary focus of safety and risk assessment. Only very recently a general awareness about these risks has developed within the DOE organization. This is a fallout of (1) the general public recognition of the risk of any complex system that was precipitated in the wake of the such events as TMI, Chernobyl, Challenger, and Bhopal, and (2) as the external threat of war has diminished, the willingness of the public to accept nuclear weapons related risks has diminished.

DOE has recognized the value of risk management as an additional dimension of its activities and performance. However, this recent recognition has not translate into a uniformly focused activity. This may be due to such various reasons as:

1. Organizational diversity and jurisdictional complexity among diverse organizations.
2. Lack of independence of regulators from the operating authority and the absence of regulatory enforcement authority at the facility.
3. Fragmentation of regulatory criteria and absence of independent regulatory process.
4. Uncoordinated regulatory practices among multiple regulatory authorities, e.g., DOE, NRC, EPA, OSHA, state and local governments.
5. Inertia of the old culture.
6. Rate of introduction of the new risk-based culture throughout the complex.
7. Lack of consistent goals, policy, criteria, and methods commensurate with facility type and functional process.
8. Lack of expertise, training, tools, data bases, and organizational structures through out the complex.
9. Recognition of the usefulness of information generated at a facility and its implication on the benefit and cost parameters.
10. Rational implementation of the policy, goal, criteria commensurate with the nature, magnitude and other important attributes of risk.



Other industries, viz., aerospace and commercial nuclear power, have been applying the methodologies of risk assessment for quite sometime and are lately applying integrated risk management techniques to make rational business decisions. In the DOE complex the recent activities devoted to risk management process seems to be very limited and preliminary results in many cases show unrealistic low magnitudes of estimated risk (See Figures 1, 2).

## 1.2 Objective

Our objective in this paper, is to give an overview of the status of risk management activities in the DOE complex. A comparison of the status is made with that of the commercial nuclear industry to get a perspective on the state-of-affairs in the DOE complex.

## 2.0 UNIQUE ACTIVITIES AT THE DOE COMPLEX

Risk Management at the DOE Complex has unique aspects that differ significantly from other industries. Some of those major aspects are: plutonium handling, tritium handling, transportation of nuclear weapons and weapons grade materials through wide regions of the country, safeguards of special nuclear materials and weapons, and interface with Department of Defense.

Modernization and consolidation of the DOE Complex in the Complex-21 Reconfiguration has been considered. It will be important to integrate these efforts with a risk assessment of the complex as a whole, so that rational decisions may be made. Risk comparisons of alternate configurations could be valuable to the decision makers.

Another area of concern is weapons grade plutonium disposition in the United States and the former Soviet Union which will be available from the dismantling of the weapons. In this area also, elements of risk management principles could provide some insights in choosing between alternatives. For example, whether "burning" of the mixed oxide fuel in a suitable reactor is more desirable compared to vitrification and disposal of plutonium in geologic repository or some other alternative.

## 3.0 STATUS OF RISK MANAGEMENT ACTIVITIES

Throughout the DOE complex there have been very few complete probabilistic risk assessments (PRA) performed. Only recently, Savannah River Plant submitted the Safety Analysis Report to DOE/DP that contains PRA. A few of the other facilities, such as the N-Reactor at Hanford and High Flux Test Facility (HFIR) at Oak Ridge have done PRA using similar modeling techniques that have been applied to commercial nuclear plants. A number of other facilities are also performing PRA of their facilities. The status of these studies is summarized in Table 1.

Previously master studies were performed for the DOE complex which were hazard analysis and lacked quantitative analysis. Applications are now being performed in the weapons community reporting accident events as  $10^{-12}$  per year. Such a low value is not indicative of safe weapons. It is indicative of PRA efforts that overly limit scope (no common cause/mode analysis, no human factors analysis, and no external events analysis) and use inappropriate non-conservative simplifying assumptions (statistical independence and over-extrapolation of data).

#### 4.0 RECOMMENDATIONS AND CONCLUSION

We would like to recommend that data on related DOE risk assessments be evaluated similarly to NRC's NUREG 1150 study.

**TABLE 1: DOE FACILITIES**

Location	Site	Facility	PRA Studies*	
			Completed	In Progress
Albuquerque (AL)	Allied Signal	1		
Albuquerque (AL)	EG&G Mound	8		
Albuquerque (AL)	General Electric	2		
Albuquerque (AL)	M.K. Ferguson	1		
Albuquerque (AL)	Mason & Hanger-Silas	2		
Albuquerque (AL)	Sandia (Albuquerque)	2		
Albuquerque (AL)	Sandia (Livermore)	2		
Albuquerque (AL)	University of California	9		
Albuquerque (AL)	Westinghouse Albuquerque	1		
Chicago (CH)	Brookhaven National Lab-BNL	5		
Chicago (CH)	Princeton University	1		
Chicago (CH)	Universities Research Association	1		
Chicago (CH)	University of Chicago/ANL	10		
Chicago (CH)	University of Tenn./Space Instit.	1		
Idaho (ID)	EG&G/Idaho	6		
Idaho (ID)	Mountain States Energy Inc.-MSE	1		
Idaho (ID)	West Valley Nuclear Services (Westinghouse)	1		
Idaho (ID)	Westinghouse Industries Nuclear Corp.	2		
Nevada (NV)	EG&G/Energy Measurements	1		
Nevada (NV)	REECO, EG&G, et al	1		
Nevada (NV)	Reynolds Electric Engineering Co.	1		
Oak Ridge (OR)	Bechtel Oak Ridge	2		
Oak Ridge (OR)	Boeing Petroleum Services -BPS	1		
Oak Ridge (OR)	M.K. Ferguson	1		
Oak Ridge (OR)	Martin Marietta Energy Systems	16		
Oak Ridge (OR)	Westinghouse Oak Ridge	2		
Rocky Flats (RF)	EG&G/Rocky Flats	4		
Richland (RL)	Westinghouse Hanford Co.-WHC	10		
San Francisco (SAN)	Bechtel Corp.	1		
San Francisco (SAN)	Rockwell International	1		
San Francisco (SAN)	Stanford University	1		
San Francisco (SAN)	University of California-LBL	3		
San Francisco (SAN)	University of California-LLNL	9		
Savannah River (SR)	Westinghouse Savannah River Co.-WSR	0		

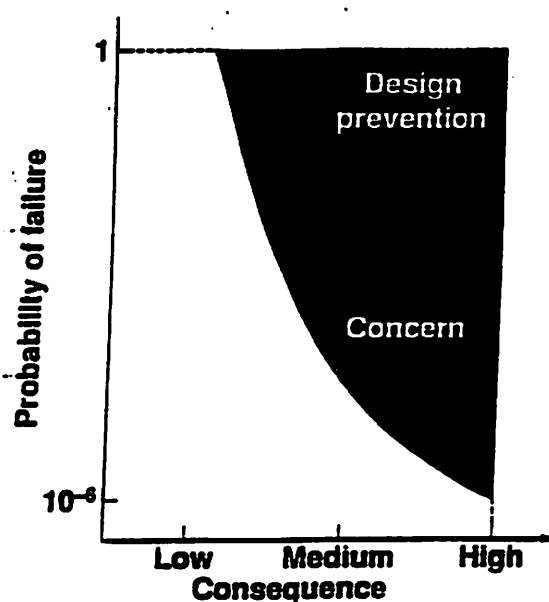
\*Available upon request at the PSAM Conference.

TABLE 2: WEAPONS RELATED PRA

Risk Assessment	Planned	*
B57 Level 1	9/93	
W79 Level 1	9/93	
W48 Level 1	2/94	
W68 Level 1	6/94	
W69 Level 1	6/94	
W70 Level 1	12/94	
B61-0,2 Level 1	12/94	
W56 Level 1	4/95	
W62 Level 1	10/95	
Pantex Onsite Tra	1/94	
Pantex Staging/sto	1/95	
Pantex Assembly	3/95	
NTS Arming & Firing	1/94	
NTS Assembly, Disassembly	3/94	
NTS Insertion, Inst	12/94	
NTS Offsite	10/94	

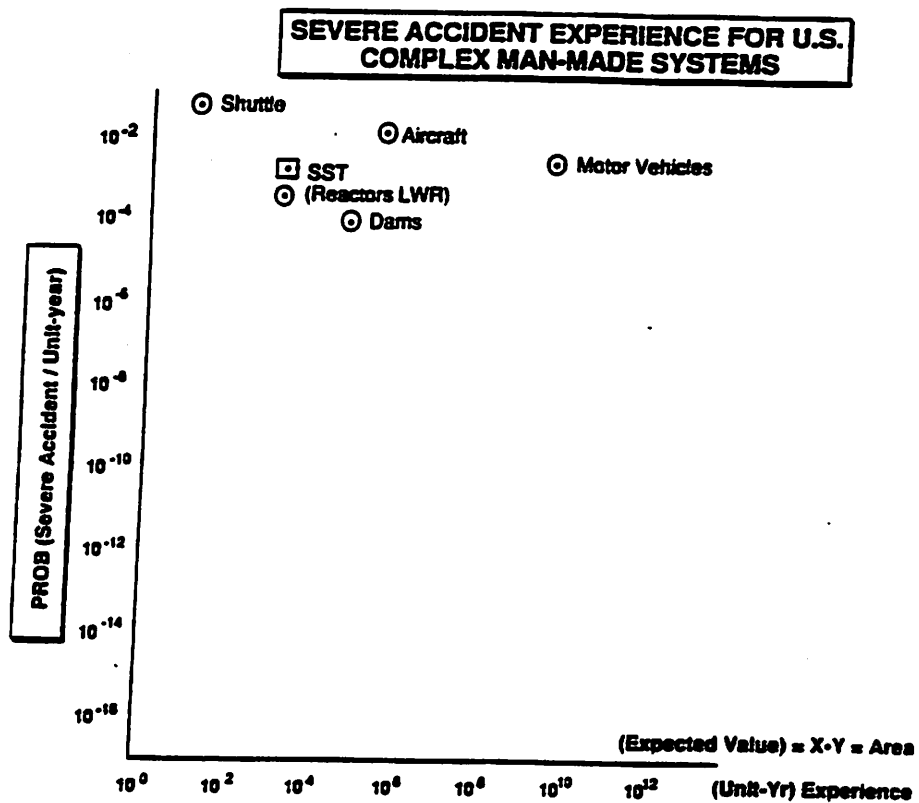
\* Available upon request at the PSAM Conference.

Figure 1



Type of analysis	Data needed
Quality Assurance	Expert judgment
PRA	Component failure data to estimate system failure
Reliability Analysis	Need system & component failure data

Figure 2



# **THE INTEGRATION OF HUMAN FACTORS INTO THE RISK ASSESSMENT OF A NUCLEAR DEVICE ARMING AND FIRING SYSTEM\***

Thomas Altenbach, and Walter Ferrell

Risk Assessment and Nuclear Engineering Group  
Nuclear Test Engineering Division

## **BACKGROUND**

Assuring the safety of the arming and firing (A&F) system for nuclear device testing at the Nevada Test Site has been an important priority since the start of the nuclear test program. Recently analytical work has been done using risk assessment techniques to update safety evaluations for the A&F system used by Lawrence Livermore National Laboratory. In 1990, Lappa<sup>1</sup> presented a fairly typical probabilistic risk analysis, based on work by others dating back to 1976. This study took the original A&F fault trees and updated them to correct mistakes, to improve descriptions of the fault paths, and to better reflect current designs. In 1992, Clay<sup>2</sup> presented an analysis which made some minor changes to the Lappa fault tree, and then discussed the first and second order cut sets in various detail. Some calculations were done to estimate the likelihood of the occurrence of these cut sets; however, there was no systematic probabilistic evaluation of the overall fault tree. Neither study attempted a detailed treatment of human factors. Then it was recommended that a more thorough follow-on risk assessment be performed that included human factors. It's intended that this latest study<sup>3</sup> will comply with the Department of Energy (DOE) Orders 5610.11 (Chapter 9) and 5610.11A, as evaluated by the DOE Nuclear Explosive Safety Study Group.

## **SCOPE**

This study is concerned with the potential for the release of plutonium from a nuclear device due to hardware component failures, human errors, and/or external natural phenomena affecting the A&F system. Intentional human actions such as sabotage or terrorist subversion were excluded from this analysis. The time period of concern begins when the device and the A&F equipment are located physically adjacent at ground zero, until the device is fully stemmed. This time period is divided into the following phases: device delivery and installation, hot dry run testing, and device insertion. Dispersal following a detonation of the device high explosive is the only release mode considered, and no attempt was made to estimate the consequences of a dispersal.

---

\* This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract no. W-7405-Eng-48.

## SYSTEM DESCRIPTION

The purpose of the A&F system is to reliably detonate the nuclear device at the intended time, while safely preventing detonation at any other time. Command signals and power are sent from the control room to an electrical panel called the zero interface unit (ZIU). The downhole cables connect the ZIU to the A&F components. When arming power is supplied, capacitors (the X-unit) are charged. Then on the firing signal, the stored energy is discharged into the detonator cables leading to the nuclear device. Critical safety considerations involve the connections between the ZIU and A&F cables, and between the A&F capacitors and device detonator cables. Figure 1 shows a simplified sketch of the A&F system as it is configured for four operational phases.

## ANALYSIS

We began with a thorough review of both the device system engineer's checklist and the arming and firing checklist procedures to identify the time periods when hazards could threaten an inadvertent detonation. Next we identified those credible initiators which could cause a high explosive detonation. Due to differing accident initiators, the resultant complexity of the analysis required for each operational phase was quite different. This ranged from a simple qualitative analysis for the device delivery phase, to a human factors screening analysis for the hot dry run phase, and finally a more detailed task analysis and accompanying fault tree for the insertion phase.

### Device Delivery and Installation Phase

This is the first phase in which the A&F system and the nuclear device are in close proximity. However, all the A&F system cables are physically locked out from the power sources located in the zero interface unit. Furthermore, the device detonator cables are also physically locked out from the A&F system. Although in proximity to the device, the A&F system is electrically isolated from both the device and power sources during this phase. A qualitative analysis concluded that due to this dual isolation of the A&F system in this configuration, the risk of an accidental high explosive detonation due to failures related to A&F was negligible.

### Hot Dry Run Phase

This is a phase of A&F system testing where the A&F cables are connected to power sources at the ZIU. The device detonator cables remain locked out. In order to test the A&F system, commands and charging power are sent through the ZIU to exercise the entire system, with the final firing power diverted to a load simulator which takes the place of the device. Qualitative analysis showed that the risk of a detonation during this phase is dependent upon human action, as the potential for an error of commission in connecting the detonator cables to the A&F system does exist.

The key factor in ensuring that a detonation cannot take place during a HDR is maintaining that the device detonator cables remain locked out. During the HDR test, all of the downhole cables are connected to the A&F system, and since the device is locked out, a load simulator is used to measure the magnitude and duration of electrical pulses. It is not possible to tell from the control room if the actual connections are to the simulator or to the real device. Therefore, the possibility exists that if the detonator cables were connected instead of the load simulator, there would be an detonation during the HDR. This possibility is prevented by administrative controls, and there are no procedural steps to connect the device during the HDR.

We used the Accident Sequence Evaluation Program<sup>3</sup> (ASEP) methodology, developed for the nuclear power industry, to produce conservative quantitative estimates on the human error frequency. An error of commission is assumed to occur during a HDR in which someone mistakenly unlocks the detonator lock box, disconnects the load simulator from the A&F system, and then connects the detonator cables to the A&F system. Four recovery factors as defined by the ASEP method were identified which mitigate the likelihood of this error. Assuming an initial human error probability (HEP) of 0.03, and a value of 0.1 for each recovery factor, yields a frequency of  $3 \times 10^{-6}$ . While the values used in this screening process are extremely conservative, the results do indicate that the above event is potentially credible.

### **The Device Insertion Phase**

During the Device Insertion phase the device is lowered down into the hole, and once lowered the hole is stemmed. The device detonator cables are connected to the A&F system, but the downhole cables are locked out from the ZIU. Instead, the ZIU is connected to a simulator to perform signal dry run (SDR) tests. During this phase, downhole cable testing and SDR testing are done on a daily basis. This continues the entire length of the phase, assumed to be 14 days. These tests are typically performed as follows. Two authorized personnel unlock the A&F downhole cable lock box, perform cable tests, then secure the lock box. Next the simulator equipment is checked out, and connections to the ZIU are verified. At this point, a phone call is made to the control room, notifying that all is ready for the SDR and requesting that power be sent. Actions at the control room then power up the ZIU. Next an automatic command sequence is started, which charges the X-unit simulator. After a delay of about 3 minutes, the X-unit simulator is automatically fired. During this interval, the test director at the command post does have the option to delay firing, or to cancel the test and disarm the X-unit simulator.

The opportunity does exist for human error to cause a detonation of the device during the SDR test. A sequence of errors must occur for this to happen. A brief task analysis of the test procedures produced the following scenario judged most likely to result in inadvertent detonation. A more complete HRA that could develop all credible sequences was beyond the scope of this project.

1. The authorized person, denoted by K1, responsible for securing the lock box fails to follow the written procedure and leaves the box open after completing the cable tests.
2. The other authorized person, denoted by K2, responsible for checking that the box is locked fails to do so.
3. K1, in violation of the standard two-man policy and without following an appropriate checklist, independently disconnects the SDR simulator and connects the A&F cables to the ZIU. This might occur if the K1 was very confused, and believed a hot dry run was to be performed instead of the signal dry run. In a HDR, the A&F cables are connected to the ZIU, as discussed previously.
4. K2, and any other authorized personnel nearby, fail to check the work that K1 has done and do not notice the A&F cables are hooked up. Instead K2 calls the control room for power to be sent to the ZIU to complete the SDR.
5. The test director fails to stop the SDR. Although there is no direct indication in the control room on the status of the lock boxes and cable connections, personnel monitoring the charging voltage on the X-unit simulator should notice a discrepancy in the charging time if the actual A&F X-unit were being charged. This is because the simulator is charged

with only a single power supply, whereas the actual X-unit is charged with two power supplies. Therefore the simulator takes twice as long to charge as the actual X-unit.

While it is possible to again use the ASEP methodology to provide a quantitative screening probability for this scenario, we chose to apply the more detailed Technique for Human Error Rate Prediction<sup>4</sup> (THERP). This allowed us to estimate the probability of the sequence and uncertainty within fairly tight bounds for use in the insertion phase fault tree. The results from the THERP calculation follow. The frequency of leaving the lock box open is estimated at .0015; the frequency of the A&F cables being connected and undetected by Red Shack personnel, given the lock box was left open, is .000125; and the frequency of the test director to fail to detect the X-unit charging discrepancy is .27, all per day. Then the probability of inadvertently charging the X-unit is  $.0015 * .000125 * 14 = 2.6 \times 10^{-6}$ , and the probability of inadvertent detonation via human error is  $2.6 \times 10^{-6} * .27 = 7.1 \times 10^{-7}$  per test.

The uncertainty of this result was estimated by assuming a lognormal distribution for each error in the sequence, with error factors derived from THERP. Then a Latin Hypercube simulation was run on the sequence, and the resulting best estimate had an associated error factor of about 15. This value was then used for the error factor for the human errors used in the insertion phase fault tree as basic events.

There are some simple positive measures which could be taken to mitigate the risk from this scenario. The most obvious is the addition of an annunciator in the control room to indicate an abnormal condition with respect to the downhole cable lock box and/or the actual cable connections. If properly configured, failure of the test director to respond to such an annunciator has a very low probability, and assuming a low level of dependence, the value used for that error would be reduced from .27 to .05. The installation of an interlock which prevents power from being sent by the control room whenever an abnormal condition is indicated would further reduce the error probability.

Another simple way to reduce the probability of this sequence is to reduce the number of signal dry runs performed during the insertion phase. A reliability analysis needs to be done to determine the benefits of doing the daily SDR test. For example, it is conceivable that performing 14 SDRs provides only a marginal increase in A&F system reliability over performing merely 2 SDRs, one at the beginning and one at the end of the insertion phase. In this example, a factor of 7 decrease in risk is accomplished by trading off a potentially negligible decrease in reliability.

A new fault tree was developed for the insertion phase, including basic events consisting of hardware component failures, lightning strikes, and human errors. The two human errors of inadvertent arming only, and inadvertent arming and firing, are explicitly included as basic events. Imbedded in these basic events are dependencies developed in the human error sequences explained previously. Although other human errors due to common cause are conceivable, a better understanding of the A&F operations as they are actually carried out in the field is needed before additional common cause errors can be included. The fault tree was graphically input with the IRRAS code<sup>5</sup>, and solved for minimal cut sets. The fault tree was quantified, and we have documented the sources for all basic event failure rates used. The mincut upper bound calculation resulted in a value of  $7.3 \times 10^{-7}$  per test. This represents our point (or best) estimate of the probability of system failure per test during the insertion phase. This is similar to the result from the previous study<sup>1</sup>, and we believe it is realistic for a very safe and reliable system that nevertheless is susceptible to hardware failures, lightning, and human error.



We have also performed an uncertainty analysis using a Latin Hypercube simulation, which provides a probability distribution for the results. The uncertainty analysis yielded a distribution with the 5th percentile =  $5.5 \times 10^{-8}$ , and the 95th percentile =  $4.8 \times 10^{-6}$ , and the median or 50th percentile =  $4.7 \times 10^{-7}$ . An importance calculation was performed which ranks all the basic events according to their contribution to the system failure probability. The most important events are human error which arms and fires the device, and direct lightning strikes. Lower in importance are failure of the lightning protection devices, a failure of the X-unit switch tube, and human error which inadvertently charges the X-unit capacitor.

## RESULTS AND CONCLUSIONS

We have produced qualitative and quantitative results, which assessed the likelihood of having an inadvertent detonation of the device caused by A&F system failures. It is our finding that the A&F system is well designed, and operated by dedicated personnel. The continuous testing done on the system assures that the hardware will function safely and reliably to a high confidence level. However, the safety is highly dependent on the human. Although very thorough administrative controls are followed and written checklists are well understood by experienced and knowledgeable people, the opportunity for serious human error is present during the hot dry run and insertion phases. Although several human errors are required for a detonation, the potential for a common cause such as miscommunication and confusion threatens to bypass the engineered safety redundancies and administrative controls. Qualitatively, we believe human interaction may be the most important factor in the safety of the A&F system.

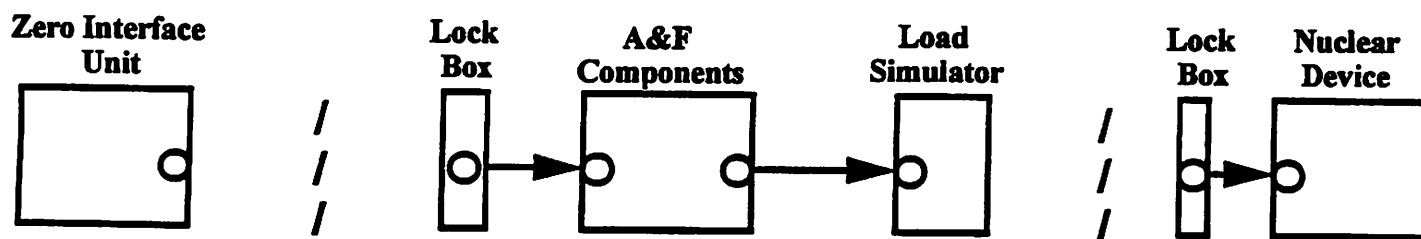
The risk due to human error in the device delivery and installation phase was judged to be minimal and was not analyzed in detail. The risk due to human error in the hot dry run phase was evaluated using the ASEP methodology. The resulting accident probability estimate is  $3 \times 10^{-6}$  per test. While the values used in the screening process are very conservative, the results do indicate that human error in this phase is a concern. The fault tree analysis produced a best estimate failure probability of  $7.3 \times 10^{-7}$  per test for the insertion phase. This risk was approximately equally shared by human error and lightning events.

Since human factors are so important to the safety of the A&F system, we recommend that a more detailed human reliability and task analysis be done on the hot dry run and insertion phases. This would require the analysts to observe the actual operations being performed for the next nuclear tests. Although we believe the human error frequencies used in this analysis are conservative, it's possible that a greater understanding of the actual operations, and the potential for common cause among events previously considered independent, could further increase the importance of human factors. Future work should also show how human error can be mitigated, possibly by tighter administrative controls, more detail and redundancy in checklist procedures, and other means designed to make potential common cause errors more independent.

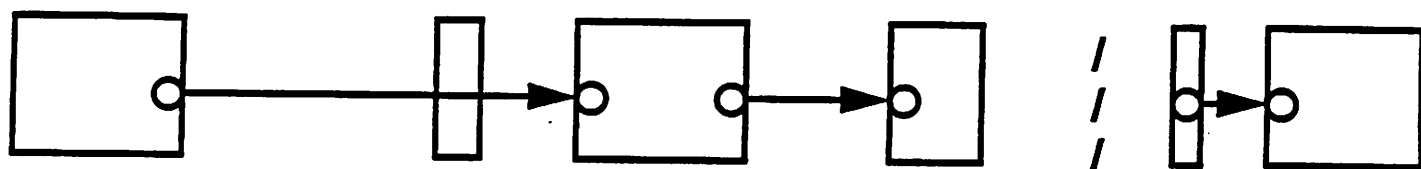
## REFERENCES

1. David A. Lappa. "Assessment of the Probability of a Nuclear Explosives Safety Incident Due to Failures in the Arming and Firing System," Lawrence Livermore National Laboratory informal report, Livermore, CA, (October 9, 1990).
2. John Clay. "Risk Analysis of the Arming and Firing System," Lawrence Livermore National Laboratory report NES92-199, Livermore, CA, (June 8, 1992).
3. Thomas Altenbach, Walter Ferrell, and Edward Greybeck, "Risk Assessment of the Arming and Firing System at the Nevada Test Site," Lawrence Livermore National Laboratory report UCRL-ID-114809, Livermore, CA, (July 1993).
4. Alan D. Swain. "Accident Sequence Evaluation Program Human Reliability Analysis Program, U.S. Nuclear Regulatory Commission report NUREG/CR-4772, Washington, D.C., (February 1987).
5. K. D. Russell, et al., "Integrated Reliability and Risk Analysis System (IRRAS) Version 4.0, " U.S. Nuclear Regulatory Commission report NUREG/CR-5813 (EGG-2664), Washington, D.C., (January 1992).

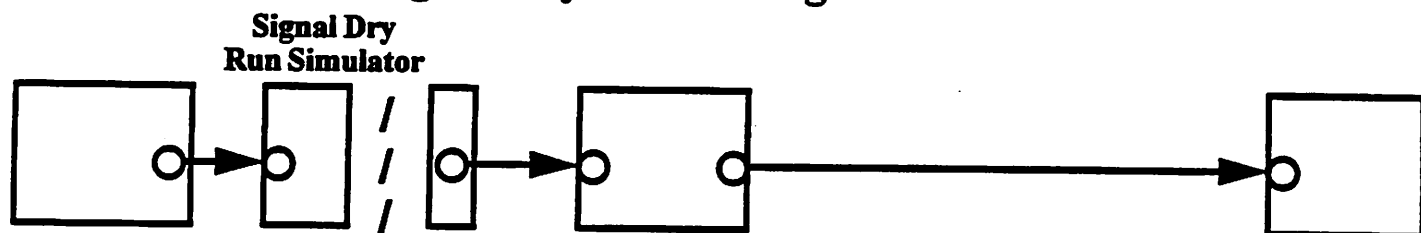
## Device Installation Configuration



## Hot Dry Run Configuration



## Signal Dry Run Configuration



## Firing Configuration

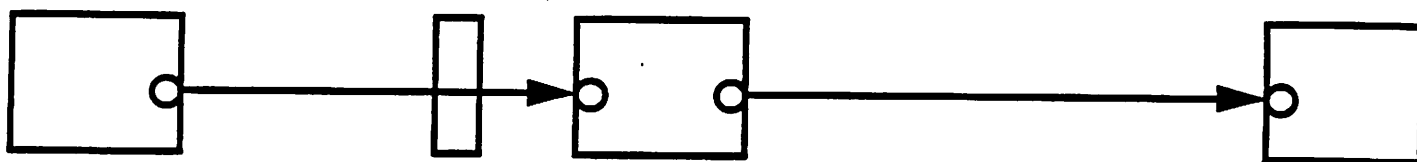


Figure 1. Simplified schematic of the Arming and Firing System showing the different configurations used in four operational phases. The lines represent cables, and the series of slashes (/) indicate breaks in the connections which are depended upon for safety from inadvertent detonation before the firing configuration is established.

## A METHOD FOR DETERMINING RISK TO GROUND FACILITIES FROM AIRCRAFT ACCIDENTS\*

Chris Y. Kimura, and C. Thomas Bennett

Fission Energy and Systems Safety Program  
Lawrence Livermore National Laboratory  
Livermore, CA 94550

### INTRODUCTION

#### Background

Many local special interest groups, as well as government agencies, have raised the threat of an aircraft crashing into a ground facility near an airport. For example, many large commercial shopping malls are located near the approach and departure routes of nearby airports.

Two such examples in California are the Eastridge Mall in San Jose, which is located near Reid-Hillview general aviation airport, and the Sun Valley Mall in Concord, located near Buchanan Field serving both general and commercial aviation traffic. The Sun Valley Mall was hit by a twin engine aircraft on December 23, 1985. All aboard the aircraft were killed, as were several individuals within the shopping mall. This is not an isolated incidence.

The same sorts of problems exist with federal facilities. Recently, FAA has proposed to locate an air traffic control (ATC) facility on the final approach of a major airport in Ohio. One of the better known instances of potentially high risk collocations of airports and federal ground facilities is the Pantex nuclear weapon production facility, located near Amarillo International Airport.

*Risk resulting from an aircraft accident has been viewed as a stochastic process, with the probability density function being distributed evenly with respect to geography* (Goldstein, et alia, 1992). Other aviation risk researchers have used exponential probability density functions, PDFs (Krivokapich, 1976). In this latter study, the investigators applied PDFs to airways near facilities being studied, but without considering whether those airways are actually used during normal air operations.

In other domains, risk investigators have used similar conceptual approaches (Sandman, et alia, 1987). That is, these researchers applied isoprobability PDFs plotted simply as a function of distance from a hazard.

#### Statement of the Problem

*We question the validity of examining aviation risk as a function of geography, without considering the pattern of aircraft operations.* The significance of this lies in the fact that airplanes do not operate in a random fashion around an airport. For the most part, there are very specific approach and departure paths associated with each airport.

For example, the manner in which aircraft enter and exit Airport Traffic Areas is determined by such factors as (a) geography, (b) noise abatement issues, (c) location of navigation facilities, (d) position of airways, and (e) runway lengths and orientations.

---

\* This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract no. W-7405-Eng-48.

In both the Goldstein and Krivokapich papers referred to previously, little regard was given to how aircraft actually use the airspace allotted to them. In the Goldstein work, PDFs were applied to a sector of airspace located at the approach end of the runway.

On the surface this might appear logical if, and only if, all approaches are essential straight-in to the airport. An approach is considered straight-in if an aircraft intercepts and tracks the extended centerline of the runway beginning at a point several miles from the airport.

In the Krivokapich paper, PDFs were applied in an orthonormal pattern, perpendicular to published airways. Again this would seem logical if, and only if, aircraft flew on those published airways.

The problem in the first paper discussed is that straight-in approaches may or may not be used at any given airport. If they are used at an airport, the pattern of usage may be determined by the direction from which the aircraft is arriving, or seasonal wind patterns.

The problem with the Krivokapich work is that rarely do aircraft fly routes published on navigation charts, once they start preparing for a landing. The reason for this is that once an airplane nears its destination, frequently ATC will provide vectors to the final approach course. The reason for this is to save time and money.

Essentially, the only time that published approaches are used are (a) during training, (b) communications failures, and (c) when air traffic is delayed and a back log exists of aircraft waiting to land.

The obvious point we are trying to make is that a ground facility is at risk to an aircraft accident only if aircraft fly over it. The magnitude of the risk is then determined by the frequency of the air traffic, and accident patterns that might be associated with specific procedures being used during flight over that facility.

In essence, the previous studies have failed to ask a question that can be answered fairly simply: *"Do air traffic control procedures require aircraft to fly over the site being studied?"*

## METHODOLOGY

### Determining Air Traffic Patterns

There are several sources that need to be consulted to understand and determine the how an aircraft will approach and depart a given airport. The information sources examined by an investigator would include (a) FAA navigation charts and textual documents, (b) non-FAA, authoritative, local air traffic procedure guides, and (c) local air traffic control personnel.

The official navigation charts include: (a) Standard Instrument Approach Procedures (SIAPS), (b) Standard Terminal Arrival (STAR) plates, (c) Standard Instrument Departure (SID) plates, (d) Sectional Aeronautical Charts, (e) Low and High Altitude Enroute Charts, and (f) Airport/Facility Directories. These sources provide a basic understanding of the overall structure of the air traffic around an airport.

Non-FAA navigation information is often published by state aviation agencies and commercial vendors. Air traffic control procedures are often provided such organizations in a format that is more detailed than provided by the FAA.

Local air traffic control offices that should be interviewed should include: (a) Air Route Traffic Control Centers (ARTCCs), (b) Traffic Control Centers (TRACONs), and (c) Airport Traffic Area (ATA) controllers. The information provided by these sources will provide the core of airspace usage analysis. The analysis methods used these data to determine how Probability Density Functions should be applied geographically.

### Air Traffic Activity and Accident Reports

Air traffic activity is defined by the number and type of operations conducted around an airport. These data are compiled by local ATC personnel and reported to FAA Headquarters.

Two approaches can be used to describe accident rates at a given airport. The first is less specific, but more powerful statistically than the second. This more powerful method is based on determining the accident rates at airports similar to the one under investigation. Averaged data, based on a larger sample size is then used during the analysis.

But, it is important to understand is the sampled data is representative of the airport being studied. This can be determined by applying standard tests of central tendency and variation.

Air traffic activity and accident reports used during the analysis should include: (a) Aviation Statistical Handbook, (c) F.A.A. Federal Air Traffic Activity, (d) actual aircraft accident reports obtained from the National Transportation Safety Board, and (e) runway usage rates that can be obtained directly from the airport being studied.

The activity measures provide the basis for the denominator of a basic probability equation—the number of possible occurrences. The accident reports provide the frequency of the events in question.

Runway usage data is normally gathered by a tower, but archived for only fifteen days. If there is evidence that the pattern of runway usage may affect the analysis, then discussions with a specific tower

will be required in order to obtain the data for long periods of time. This process requires coordination; but, it is not a difficult process.

### Accident and Risk Calculations

The accident frequency data can be incorporated into the analysis depending upon whether a chronological description of the events is relevant. If not, and if the airport being studied appears to be representative of other similar airports, then the data may be averaged across time and airport sites.

Accident probabilities are then computed based on the operational usage information gathered earlier. Now, instead assigning crashes to geographical areas through which air traffic would normally not fly, only that area that has been designated by the air space usage analysis is considered.

How aircraft accident are assigned to those operational areas is determined by what information is available in the NTSB reports for that airport. If information concerning where accident were located with respect to an airport are not available, because they were not systematically coded into those specific reports, then other studies must be used. See Bennett and Schwirzke, 1992 and Kimura, 1993. These reports provide statistics to assign accident rates to certain distances from an airport.

These data are then applied only to the geographical areas shown to have relatively high usage by the activity analysis. Probability density functions are then applied to those specifically identified air corridors.

A parallel step in determining the probability of an aircraft crashing into a given site is calculating the probability of an aircraft flying over the site in question. These methods use a process similar to the one Krivokapich used. That is, take the appropriate data on activity for the airport and assume that the aircraft is following the routes established by local operational convention.

## DISCUSSION

During this discussion, we will provide parts of a risk analysis that might be conducted at a specific airport. Because of space, the full analysis will not be presented, but rather excerpts from different steps in the process.

### Air Route Usage Analysis

Discussions with Amarillo ATC revealed that there was a season specific change in the usage of the runways. Runway 22 is typically used in the Summer; and, Runway 4 is used in the Winter months. This would suggest that a detailed risk analysis of Amarillo should include a runway usage analysis, as discussed above.

### Accident and Activity Analysis

Table 1 presents the aircraft operations data for the Amarillo International Airport from 1964 to 1990 obtained from the F.A.A. Federal Air Traffic Activity by Fiscal Year. Prior to 1968, the Amarillo International Airport was an active U.S. Air Force Base but accepted commercial air carrier traffic for the Amarillo region, according to discussions with the Amarillo ATC.

Table 1 also presents the accident data near the Amarillo region from 1964 to 1990 obtained from the National Transportation Safety Board (NTSB). In addition to the Amarillo International Airport, there is a general aviation airport, Amarillo Tradewind Airport, located approximately 5 1/2 miles West, Southwest of the Amarillo International Airport. There are also two small private general aviation airports, Palo Duro, and Buffalo located South of Amarillo. As shown by Table 1, there were 131 aircraft accidents in the Amarillo, Texas area from 1964 to 1990. Of this total, we were able to assign 58 as occurring at the Amarillo Tradewind Airport and 8 to other airports in the Amarillo area. A total of 27 aircraft accidents were designated as occurring at the Amarillo Air Force Base, Amarillo Municipal Airport, Amarillo Air Terminal, or the Amarillo International Airport. We assumed that all of these titles refer to the same airport. Thirty eight other accidents either could not be assigned to a particular airport or occurred somewhere in the Amarillo area.

As for the 131 accidents occurring near Amarillo, only three involved large aircraft. A Trans World Airline Boeing 727 suffered an in-flight emergency and required an emergency landing at the Amarillo Air Force Base on December 16, 1965. Only minor damage occurred to the aircraft and no fatalities or serious injuries were sustained during this event. On July 20, 1966, a Boeing 720 on a training flight suffered a hard landing and gear collapse at the Amarillo Air Force Base. Substantial damage occurred to the aircraft but no fatalities or serious injuries were sustained during the event. Finally, on April 28, 1985, a Southwest Airline Boeing 737-3H4 ran off a wet Runway 04 during a thunderstorm at the Amarillo International Airport. Substantial damage occurred to the aircraft but no fatalities or serious injuries were sustained during this event. Of these three accidents, only two can be considered as occurring during 14 CFR 121 operations. From Table 1, a total of 396,329 air carrier operations are tabulated. So a

preliminary air carrier accident rate of  $(2/396,329) = 5.05 \text{ E-6}$  per air carrier operation can be calculated. This compares quite well with the average 14 CFR 121 accident rate of  $3.74 \text{ E-6}$  per departure obtained from the F.A.A. and the N.T.S.B. by averaging the number of accidents and departures for the U.S. from 1979 to 1992.

A preliminary general aviation accident rate for the Amarillo International Airport can be determined using the data from Table 1 as follows. Assuming, conservatively, that the number of general aviation accidents is equal to the total number of accidents assigned to the Amarillo Air Force Base/Amarillo International Airport (27) minus the accidents involving air carriers (2) plus the other accidents in the Amarillo area (38) for a total of 63. The total number of general aviation operations for the Amarillo International Airport is equal to the Air Taxi operations and General Aviation operations or 68,621 plus 1,119,425 for a total of 1,188,046. The preliminary general aviation accident rate of  $(63/1,188,046) = 5.30 \text{ E-5}$  per general aviation operation is calculated. Unfortunately, it is not possible to compare this accident rate with a U.S. general aviation accident rate because the number of departures for general aviation is not tabulated by the F.A.A. or the N.T.S.B. A logical next step to confirm this general aviation accident rate is to compare this rate with a general aviation accident rate at a nearby airport which has aircraft operations similar to Amarillo such as Lubbock or Midland, Texas.

## CONCLUSION

This paper has attempted to outline the steps necessary to perform a credible assessment of the risk to ground facilities from aircraft accidents. Some preliminary aircraft accident and operation data at the Amarillo International Airport in Texas was presented as an example. Future work would require estimating the location of the accidents as a function of distance from the runways and overlaying this estimate with the location of various ground facilities near Amarillo.

## REFERENCES

- Bennett, C.T., and Schwirzke, M., Analysis of Accidents During Instrument Approaches. *Aviation, Space, and Environmental Medicine*, 63:235-61, 1992.
- Goldstein, B.D., Demak, M., Northridge, M., and Wartenberg, D., Risk to Groundlings of Death Due to Airplane Accidents: A Risk Communication Tool, *Risk Analysis*, 12(3):339-341, 1992.
- Kimura, C.Y., *World Commercial Aircraft Accidents, 2nd Edition, 1946-1992*, UCRL-ID-112905, Lawrence Livermore National Laboratory, Livermore, CA, January 1993.
- Sandman, P.M., and Weinstein, N.D., and Klotz, M.L., Public Response to the Risk from Geological Radon, *Journal of Communication*, 37:93-108, 1987.

Table 1  
Aircraft Operations at Amarillo International Airport, TX (AMA)

Year	Air Carrier FY		Air Taxi FY		Gen. Av. FY	Military FY	Total FY	
	Operations	Rank	Operations		Operations	Operations	Operations	Rank
1964	14,610	127			25,605	36,409	76,624	184
1965	15,980	115			26,171	45,864	88,015	174
1966	17,877	108			27,356	53,554	98,787	181
1967	15,959	120			27,414	63,071	106,444	195
1968	17,556	118			28,065	64,606	110,227	205
1969	17,699	126			42,863	40,732	101,294	232
1970	16,980	127			44,020	44,016	105,016	231
1971	14,958	117			38,970	39,543	93,471	251
1972	14,679	113	552		37,496	34,340	87,067	262
1973	15,051	111	529		34,280	31,778	81,638	268
1974	14,143	117	730		63,314	30,977	109,164	224
1975	13,326	121	1,063		44,194	27,952	86,535	280
1976	13,584	122	1,278		51,459	26,063	92,384	272
1977	12,679	132	1,565		54,101	28,417	96,762	284
1978	15,410	113	1,271		50,763	21,443	88,887	301
1979	16,352	108	3,228		58,184	21,549	99,313	281
1980	14,894	113	5,371		53,690	22,318	96,273	280
1981	12,833	119	5,749		58,435	24,934	101,951	251
1982	12,953	109	5,734		55,478	30,956	105,121	194
1983	13,751	110	7,373		54,306	31,585	107,015	206
1984	12,294	124	5,947		50,376	32,156	100,773	229
1985	12,789	123	6,945		39,586	31,099	90,419	262
1986	12,375	127	5,550		35,248	35,888	89,061	268
1987	15,339	114	4,854		31,983	41,140	93,316	264
1988	15,610	111	2,451		29,335	39,692	87,088	276
1989	13,480	115	3,694		28,147	39,688	85,009	275
1990	13,168	120	4,737		28,586	39,690	86,181	285
Total	396,329		68,621		1,119,425	979,460	2,563,835	

Airport operations data from Federal Aviation Administration "Federal Air Traffic Activity, Fiscal Year"



**Table 2**  
**Aircraft Accidents Near Amarillo, TX**

<b>Year</b>	<b>Amarillo AFB/ Amarillo Intn'l Airport</b>	<b>Amarillo Tradewind Airport</b>	<b>Other Amarillo Airports</b>	<b>Amarillo, TX Area</b>	<b>Total Accidents</b>
1964	3	2	3	2	10
1965	2	8	1	1	12
1966	3	5	1	3	12
1967	0	3	0	1	4
1968	2	4	0	2	8
1969	2	5	1	3	11
1970	1	0	1	1	3
1971	0	1	0	1	2
1972	1	2	0	1	4
1973	0	2	0	1	3
1974	1	3	0	3	7
1975	1	3	0	4	8
1976	2	1	0	3	6
1977	4	2	0	1	7
1978	0	4	0	1	5
1979	0	3	0	1	4
1980	0	0	0	0	0
1981	2	2	0	0	4
1982	0	0	0	2	2
1983	0	1	0	0	1
1984	1	4	0	4	9
1985	1	2	0	0	3
1986	0	0	1	0	1
1987	1	0	0	0	1
1988	0	0	0	1	1
1989	0	1	0	1	2
1990	0	0	0	1	1
<b>Total</b>	<b>27</b>	<b>58</b>	<b>8</b>	<b>38</b>	<b>131</b>

Accident data from National Transportation Safety Board (NTSB)

**098 Risk Management - International Space Applications**

*Chair: C. Preyssl, European Space Agency*

**Risk Assessment - The European Space Agency Approach**

*C. Preyssl (European Space Agency)*

**Risk Management of the Japanese Experiment Module on Space Station Freedom**

*J.C. Lin, D.H. Johnson, W.R. Fuller (PLG); K. Sakata, H. Suzuki, S. Kojima  
(Mitsubishi Atomic Pwr. Ind., Japan); H. Himeno (Mitsubishi Heavy Ind., Japan)*

**Rocky the Rover: PRA Meets ET**

*M.V. Frank, S.A. Epstein, A.J. Spurgin (Safety Factor Assoc.)*

## **RISK ASSESSMENT - THE EUROPEAN SPACE AGENCY APPROACH**

Dr. Christian Preyssl

Product Assurance and Safety Department  
European Space Agency  
2200 AG Noordwijk - The Netherlands

### **1. INTRODUCTION**

The European Space Agency ESA has developed a new and advanced safety analysis and risk management approach. This approach involves probabilistic risk assessment and provides the basis for the implementation of the ESA safety policy and program on ESA projects. The ESA safety policy and program aims at minimizing risks of loss of life and of spacecraft within the mission constraints. The safety program is an integrated part of all safety & product assurance activities.

It is the aim of this paper to illustrate the principles of risk assessment, its role in the safety program and the development of the method.

### **2. PRINCIPLES OF RISK ASSESSMENT**

With spaceflight high risks are associated. These risks are considered to originate from hazardous characteristics of the system, from hazardous effects from failures of functional constituents and from associated potential accident scenarios. A space system comprises hardware, software, human operators and the operation environment, which are necessary to perform the various functions and to achieve the mission objectives.

Typical risk increasing characteristics of a space system are large amounts of energy required to be contained and controlled, severe mass constraints imposed resulting in limited design & operational margins and failure tolerance, utilization of new and not necessarily mature technologies and the high complexity of the design and dynamic operational regime.

Before risks can be reduced and managed they must be identified. For this purpose safety analysis is used, which is supported by other analyses.

Safety analysis comprises deterministic hazard analysis and probabilistic risk assessment. This analysis supports a total system and system specific approach and involves a combined "bottom up" and "top down" method. The bottom up concept addresses the "devil that hides in the details" and the top down concept assures an optimization of the system. The method supports the integration of safety with reliability efforts and increases the dialogue with engineering.

In hazard analysis the hazardous characteristics of the system, the hazardous effects from failures and all associated accident scenarios are identified. This corresponds to answering the question:

"what can go wrong, what are the consequences and how severe are they ?"

FMECA and functional analysis provide input to hazard analysis.

In risk assessment the risks of the individual accident scenarios are determined, cumulated in order to identify the overall risk and ranked according to their relative risk contributions. This corresponds to answering the question:

"how likely are the scenarios, what is the state of knowledge about them and which are the most critical ones ?"

Reliability prediction provides input to risk assessment.

Hazard analysis and risk assessment provide the basis for risk management. Risk management comprises risk reduction, the prioritization of resource allocation, the verification and tracking of risk reduction efforts; monitoring the risk trend and finally the acceptance of the residual risk. This corresponds to answering the question:

"what can be done about it ?"

Risk reduction is achieved by prioritizing the application of the hazard reduction precedence to main risk contributors. The hazard reduction precedence mainly comprises hazard elimination, minimization and control. Main risk contributors are dominating accident scenarios as identified in risk assessment.

Figure 1 provides an overview of the interfaces between elements of safety analysis and risk management.

### 3. ROLE OF RISK ASSESSMENT IN SAFETY PROGRAM

Safety analysis, which includes risk assessment supports engineering and management during all project phases.

Engineering is supported by safety analysis in driving the system design, operation and environment by iterative risk reduction. Safety analysis and risk reduction are applied to the concepts of a system as well as to the real system, which is the implementation of the concept. A concept of a system is characterized by the lack of detailed definition and information. Risk reduction is more efficient during the conceptual phase than later during the system development as it is reflected in the ESA safety program. The concept of a system needs to be driven such that an optimum spatial and functional arrangement is achieved. A spatial and functional arrangement is optimized by considering damage propagations and safety and mission critical functions. Risk

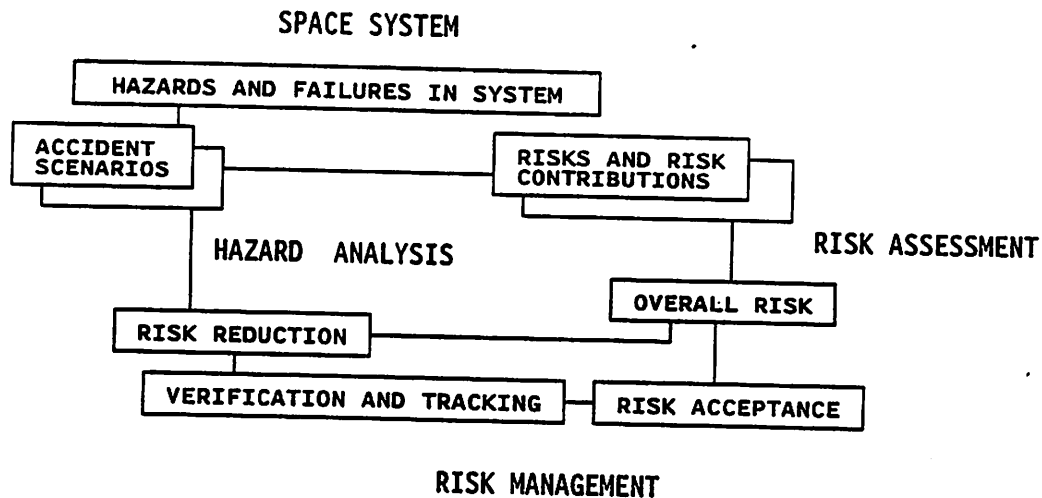


Figure 1 Interfaces between Elements of Safety Analysis and Risk Management

reduction applied after the conceptual phase addresses more and more the design and operation details which can be potential risk contributors.

Management is supported by safety analysis in providing the basis for risk management. Risk assessment establishes reporting lines between engineering and management. The overall risk trend is monitored and risk reduction efforts are prioritized verified and tracked. Risk management is supported by critical item control, configuration management, parts-material-processes procurement and application control, quality assurance and manufacturing-assembly-test control. Risk acceptance is a multi-stage process that involves demonstration of compliance with risk targets and provides input to certification.

An overview of safety analysis and risk management during the system development phases is provided in figure 2.

#### 4. DEVELOPMENT OF RISK ASSESSMENT METHOD

The development of the ESA risk assessment method started in 1987 and has involved the generation of theoretical concepts, practical procedures and supporting prototype software tools. Extensive support from contractors has been used. The risk assessment method was presented on a broad basis during an international ESA conference held at the end of 1992.

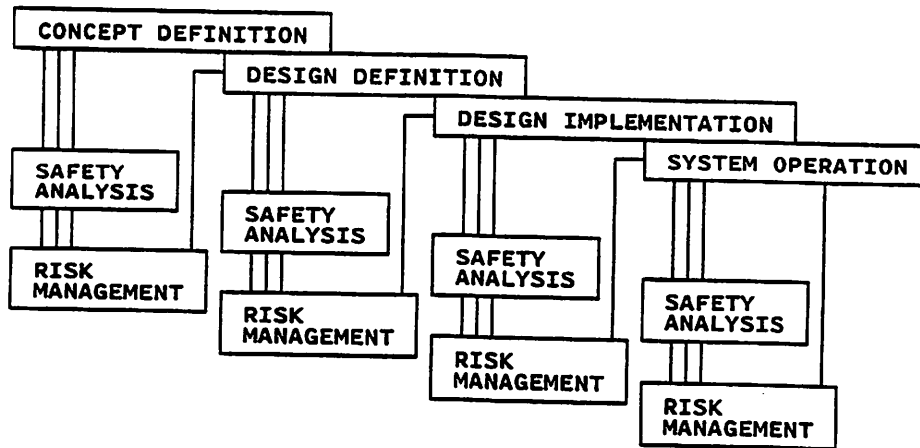


Figure 2 Overview of Safety Program

The risk assessment method has evolved from classical PRA and is characterized by several innovative features.

The deterministic modeling of accident scenarios is based on hazard trees and consequence trees, which are developed in hazard analysis and are similar to event and fault trees.

The probabilistic modeling of accident scenarios is based on the systematic treatment of uncertainties. Uncertainties are propagated using "dependent uncertainty analysis", which considers information dependencies and the subjectivity of data sources. Non consideration of information dependence can lead to an underestimation of risk. As it is difficult to deal with distributions rather than point values the concept of "potentiality" has been introduced. Potentiality is defined as a representative pointvalue of a distribution. The potentiality is more sensitive than the median to the location of mass in the upper part of the distribution, but not as sensitive as the mean to extreme tails.

The risk assessment concept supports the use of the full data spectrum ranging from subjective to objective data. For the structured elicitation and optimization of subjective expert judgement data the "calibration entropy method" was developed.

The risk assessment algorithm does not only allow to rank events or accident scenarios but also entire constituents of the system. The ranking is based on the identification of their risk and uncertainty contributions.

In order to support practical applications an ESA risk assessment prototype software package was developed.

Current development work includes the definition of an advanced risk assessment data development concept and data base format.

First application domains of the ESA risk assessment method include the fire suppression system of Columbus and the Hermes propulsion system. Further applications are planned.

## 5. CONCLUDING REMARKS

The ESA risk assessment method is a probabilistic tool supporting decision making under uncertainties and risk is used as a safety and reliability measuring stick. Risk assessment has been introduced in order to meet the challenges of future space projects by building on and improving traditional methods.

There is still lack of understanding and misinterpretation of the concept of probabilistic risk assessment as illustrated by the statement: "one can not perform risk analysis because there are no data". It seems to be not yet recognized that "one never has no data or perfect data", that "no data and little data are important data" and that "the role of no or little data vis a vis good data" needs to be assessed. Risk assessment is still believed to be too complex and expensive. The return on the investment in terms of potentially substantial cost reduction and life saving is not yet considered. Engineers are not yet used to express uncertainties and are still biased towards success oriented thinking. Probabilistic data are still misinterpreted as as true values rather than expressions on state of knowledge. It should be recognized, that only systematically identified and traceable risks can be reduced by engineers and accepted by management. In order to introduce cost saving an effective ranking of problems and setting of priorities are necessary. Progress is no progress when not verified and measured in a systematic way.

Training courses for engineering and management are in the process of being organized in order to increase the understanding and support the practical application of risk assessment. The motto will be: "the biggest risk comes from not assessing the risk".

## REFERENCES

- K.Wright, C.Preysl "Spaceflight Hazard Analysis: The Devil Hides in the Details" - IAA.6.1-93-729, 44th IAF Congress, Graz 1993
- R.M.Cooke "Experts in Uncertainty - Opinion and Subjective probability in Science" - Oxford University press, New York 1991
- C.Preysl et al. "Safety Risk Assessment for ESA Space Programmes" - ESA SP-316, ESA Symposium 'Space PA for Europe in the 1990's', Noordwijk 1991
- K.Wright "Safety Risk Management for ESA Space Systems" - ESA SP-316, ESA Symposium 'Space PA for Europe in the 1990's', Noordwijk 1991
- R.Cooke, C.Preysl "Expert Judgement in uncertainty Analysis: the European Space Agency Model for Uncertainty Analysis with Dependent Information Sources" -

PSAM Conference, Beverly Hills 1991

C.Preyssl "Combined Qualitative-Quantitative Risk and Safety Evaluations for Space Flight Systems" - International Topical Conference on 'Probabilistic Safety Assessment and Risk Management', Zuerich 1987



## ROCKY THE ROVER: PRA MEETS ET

Michael V. Frank, P.E., Ph.D., Steven A. Epstein, and Anthony J. Spurgin

Safety Factor Associates, Inc.  
1410 Vanessa Circle  
Encinitas, CA 92024

### INTRODUCTION

The goal of the Mesur (Mars Environmental Survey) program is to establish a dozen (or more) small robotics stations on Mars by early in the next century to study geology, surface chemistry, and meteorology of Mars. In 1997, the first spacecraft of Mesur, called Mesur Pathfinder, is scheduled to land on Mars. Pathfinder is designed primarily to help develop technologies for use later in the larger Mesur network of small robotics stations. It will be among the first planetary spacecraft to showcase NASA's commitment to quicker, less expensive - but technologically riskier - missions.

Flying a direct descent without orbiting Mars first, Pathfinder lander must enter Mars atmosphere at about 14,000 miles per hour. The actual payload of scientific instruments is surrounded by an aeroshell that will slow the lander to a mere 560 miles per hour. A parachute will then deploy to slow the lander to about freeway speed (78 miles per hour). About 1 second before landing the payload will deploy a set of airbags (quite similar to those in your car) which will keep the landing forces on the instruments to less than 50 g. The lander will be shaped like a three sided tetrahedron. Its sides or petals will open to lie flat on the surface of Mars revealing the lander's solar arrays and package of instruments. One of these instruments is Rocky the microrover. Rocky is a semiautonomous, remote controlled, six wheeled, extraterrestrial vehicle who will rove around the Martian landscape conducting experiments and taking pictures. And with the help of the lander, this ET will call home every day.

The Jet Propulsion Laboratory (JPL), whose forte has become robotics missions to deep space, has built and tested Rocky IV, the mother of the Rocky who will go to Mars and is currently designing the Mars version. She is an interesting specimen of slashed budgets, electronic miniaturization, and damned cleverness.

The microrover team at JPL had performed a series of brainstorming sessions to identify hazards that might jeopardize the success of Rocky's mission. However, they were interested in an independent pursuit of a more structured approach that had the potential to place in perspective the lists of identified hazards. The answer to two questions were of interest: 1) what hazards, failures, design aspects, events, or mission aspects could

jeopardize the mission's success, and 2) what mitigation programs, workarounds, or design changes could be undertaken to increase the likelihood of mission success?

We answered the first question by constructing a scenario based engineering risk model using event sequence diagrams and fault trees. An early constraint on the study was that a formal quantification would not be performed. We were asked to make observations about risk and provide recommendations directly from the scenario models. This turned out to be straightforward to accomplish because certain parts of the design and assumptions about the mission repeatedly arose as single points of failure in the risk model. Of course, informal order-of-magnitude estimates of cut set failure rates influenced our thinking. We answered the second question in consultation with the microrover team at JPL. This paper summarizes Rocky's design and mission on Mars, the risk model and observations derived from it, and the recommendations to JPL's microrover team about ways to improve the chance of a successful mission. While we were working on this study, the microrover team at JPL also continued their efforts at hazard reduction. Their identification of areas of improvement were markedly close to ours.

## ROCKY AND HER MISSION

Rocky has three serious missions. First, it is a demonstration of the technology of microrovers to operate and communicate in the Mars environment. Second, it will carry, conduct, and communicate the Mars rock and soil composition and structure data from an alpha proton X-ray spectrometer (APXS) and a camera. Third, it will take a picture of the lander and communicate the images to the lander. Although the size of a child's remote controlled toy (about 2 feet long and 20 pounds), she is far from one. The sheer distance and alignment of earth and Mars means that she must have some ability for independent action. Communication for Rocky will always be between herself and the lander using a pair of half duplex commercial RF modems, one on the lander and one on Rocky. The lander will be equipped with communications equipment capable of transmitting to and receiving from earth. One of the lander's first tasks will be to take pictures of the surrounding landscape with twin cameras and transmit the results to earth. The rover operators at JPL will view the pictures in stereo, decide what would be a nice spot for Rocky to investigate, and tell her to go there. This whole process will take the better part of a day.

Once directed, Rocky's mission is to explore the strange world of Mars in small increments of terrain. Small increments are necessary for two reasons. First, she has only two speeds, stop and go, with "go" being about 1 meter per minute. Second, her small size constrains her independence. Rocky will be endowed with the approximate ability of an insect. She will be able to sense and avoid obstacles to a limited extent; report her progress to the lander; and if she can not report to the lander, she will have the brains to go backwards to the spot of the last successful report. Furthermore, if she can not get to the place where she was directed or she can not avoid an obstacle after a few trials, she will stop and call for help.

She will have remarkable mechanical abilities for her size. She will have six independently powered wheels each with a 2 watt motor (0.016 brake horsepower) driving 2000:1 reduction gears. The four wheels on her corners have independent steering so she can turn on herself. She has the ability to lock five wheels and spin the sixth. Because of her instrumentation package, this allows a measurement of the resistance of Martian soil. She has no brakes except for friction of the electric motors. She can climb soil slopes up to 20 or 30 degrees and roll right over obstacles that are nearly as tall as her wheels which are about 5 inches in diameter. The wheels are steel and the "tires" are stainless steel bands. Each wheel is mounted on a hub that is, in turn, attached to a bogie or a rocker-arm.

Rocky will be powered by a set of solar arrays that are adequate for her expected energy use of about 100 W-hr/day. She will also carry sufficient non-rechargeable Lithium-

Thionol Chloride batteries to power her through night time experiments and to achieve a three or four day planned mission without solar power, if needed.

The electronics of the CPU, I/O cards, power sources, and instruments are housed in a thermos bottle type warm electronics box mounted on the chassis that is intended to prevent the electronics from experiencing temperatures below -40C during the Martian night. She will sense obstacles ahead by dual CCDs sensing the pattern of laser light stripes and also be able to navigate by dead reckoning. Control instruments to be carried include, for example, bogie angle encoders, motor speed, voltage, and current, motor temperature, strain gauges on wheel struts, pitch and roll sensors, accelerometers, and thermocouples.

A typical day for Rocky would start with a wake-up call either generated by electricity from the solar arrays after the Martian dawn or by an internal clock. Rocky would contact the lander that she was awake and await instructions that had been previously transmitted from earth. Rocky would receive path waypoints and an activity command sequence. She would then amble along using her dead reckoning and obstacle avoidance routines to the designated target. (The JPL team expects that a 10 meter radius from the lander would be a reasonable boundary of exploration.) Every time one half of the rover length is traversed, Rocky sends a "heartbeat" to the lander, a signal that she is still functioning and within communication range. The lander responds with a "heartbeat" of its own. Rocky will be programmed to reverse course to the spot of the previous confirming heartbeat when she does not receive a confirming heartbeat. This is intended to keep her within communication range so that the data so vital to mission success can be sent back to the lander. As the target is neared, Rocky may take a picture of it and perform an automatic approach. At the target site, she would execute whatever commands for experiments had been given. For example, she might lock wheels and perform a soil resistance test, take a picture of a rock, or place her APXS tail on a rock and perform spectroscopy. At the end of the day, she is required to pose for the lander for a picture. Before the sun sets, she transmits her data back to the lander, settles down for a long spectroscopy session (or just settles down) and goes to "sleep" for the night.

## THE RISK MODEL

The risk model used a scenario approach. Scenarios in this study were strings of successes and failures of activities of the microrover mission. Scenarios were developed for each of the several mission phases defined as cruise (from earth to Mars atmosphere), entry & landing (Mars atmosphere to Mars surface), deployment (lander to surface and a picture of Mars terrain), day operations (as described above), and sleep operations (as described above).

Scenarios were documented as event sequence diagrams (ESDs). These diagrams use boxes, ellipses, diamonds, and triangles to depict the flow of activities. As illustrated in Exhibit 1 for the operations phase, the order of activities (called events) from left to right is generally chronological but need not be. A scenario is any path through lines and boxes that leads from the prior phase to either an end state portrayed by a diamond or a transfer to the next phase depicted by a triangle. Functional redundancy is modeled in an ESD as shown with the events Solar Power Available and Battery Power Available in Exhibit 1. Contingency actions are modeled in a similar way. The events in the boxes in an ESD are binary in that only two outcomes (yes or no) are depicted. Success (or yes) is represented with a horizontal line coming from the event and failure (or no) with a downward line coming from the event. For example, if rover moves to its next location successfully, then the next action is questioned (experiments). If the rover can not move to a location, then the downward line leads to the Call Home contingency, experiments are not performed for the day, and the rover goes to sleep until new instructions are issued on the next day. If the contingency fails to recover the rover, the mission is over. Ellipses are used to depict

adverse effects or degraded states that allow the mission to continue (e.g. premature battery failure).

The risk model also documented our investigation into the causal factors affecting the outcome of each event in the ESDs. Where causal factors were complex enough to require disaggregation for adequate understanding, fault trees were developed. The fault trees ended with basic events that were component failure modes of the rover. Twenty six fault trees were developed in all. In general, the fault trees showed the logical relationship among component malfunctions that taken together lead to failure of an event in an ESD. The event sequence diagrams may be viewed as a connectivity structure for the underlying fault trees. To allow the mission, as depicted in the event sequence diagram, to proceed from one event to the next, the (failure) events in a fault tree of the preceding event must not have occurred.

## **OBSERVATIONS AND RECOMMENDATIONS**

Our model successfully integrated the hazards developed by the JPL rover team and ourselves with the expected activities of each phase of the mission. The process of building and reviewing such a model provided observations about the technical risks of the mission that are not easily attainable without such a model. The risk model, resultant observations, and recommendations reflect the design as we understood it on May 7, 1993. Such observations included aspects of the design that most contribute to risk, aspects of the microrover for which adequate redundancy is available, suggestions for contingency planning, and suggestions for resource allocation to decrease technical risk. It is interesting to note that these observations were possible without applying explicit numerical failure rates to the events in the risk model. However, the observations and recommendations presented below implicitly used the knowledge and background of failure rates (with uncertainties) of generic classes of components of the microrover. The model is also a usable framework that is easily modified to reflect the evolving design. Moderate additional work would be required to change this model into one that is amenable to a rigorous quantitative analysis of risk. Specific technological risk related observations are as follows:

- ◆ The desirable quality of "graceful degradation" is evident in the ability of the rover to function with failures. Ample redundancy is exhibited by the CCDs, wheels, batteries, solar arrays, sleep initiation, and wake-up calls. Contingency operation is adequate to preserve the mission (albeit in a very degraded condition) in the event of failing to unfurl an antennae. Ample functional redundancy is exhibited with respect to thermal protection of components and with respect to guidance and navigation over the landscape.
- ◆ All communications (e.g. commands, heart beat, and data transmission) are via two half duplex commercial grade modems (one on rover and one on lander). Failure of either one will cause inability to transmit information and commands between rover and lander. In addition, power is provided via a series of contacts, switches and voltage regulators without redundancy. The modems and power supply string are single points of failure of the mission as illustrated in the fault tree of Exhibit 2.
- ◆ There is little redundancy in distribution circuits leading from the power bus to rover components. Similarly the string of power

converters, switches, and contacts in the CPU power supply will limit the reliability of the rover's "brains".

- ◆ We noted that the May 7, 1993 electrical design provided circuitry for heating the warm electronics box from the solar arrays but not from the batteries.

We believe that the principal vulnerability of the microrover is the communication function. Communication between rover and lander and between lander and earth permeates every phase of the mission. Indeed, it is a requirement to maintain essentially continuous communication (via the "heartbeat") while the rover is in motion. We recommended the reallocation of available project resources to improve the communication devices (or add redundancy) and improve the power supply.

For this first microrover mission to Mars, we strongly recommended that software for vehicle movement control be kept as simple as possible. Rover operations should be directed from the ground as much as feasible rather than relying on the intelligence and flexibility of onboard software. This will tend to minimize software development expenditure, minimize coding for redundancy management, and minimize the chance that unanticipated combinations of events will cause "paralysis" of the microrover. Such paralysis may be caused, for example, by software caught in nested loops. Maintaining simplicity of software may allow the project to reallocate software budget to the communication reliability improvement budget.

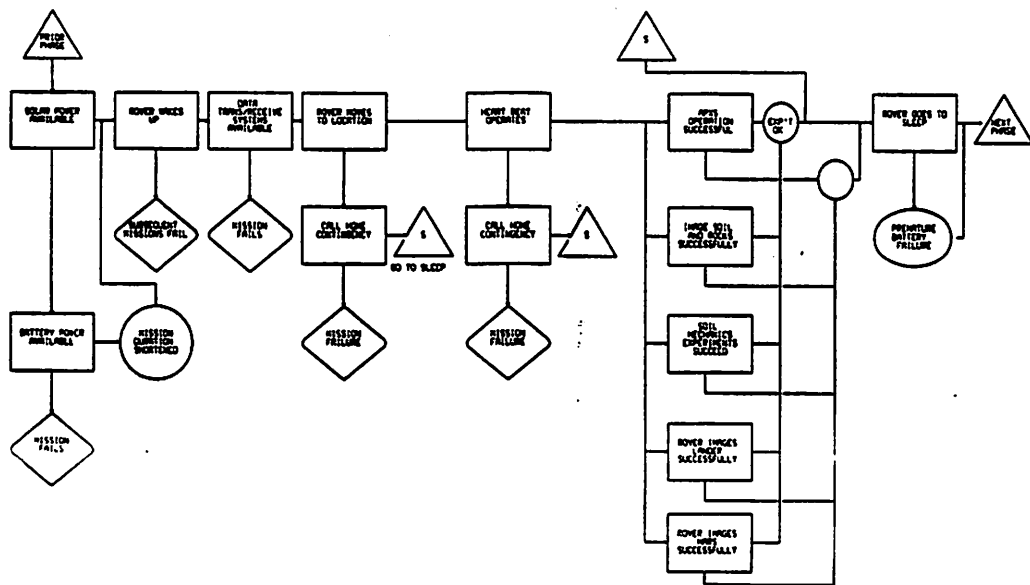
Because of the central importance of maintaining heart beat communication between the rover and lander, we recommended that clear contingency operations be developed for the possibility of loss of heart beat because of component failure. We noted that a contingency plan had been developed under the assumption that an object is blocking communication between rover and lander. However, heart beat is triggered by advancement of the rover by 1/2 length. This introduces the possibility of single point failures of such components as odometers, wires, switches, voltage regulators in addition to the modems themselves (Exhibit 2) that are need to inform the CPU when each 1/2 rover length has been traversed.

We were pleased that not only were these recommendations taken seriously by the JPL microrover project team but their own review processes had led them to similar observations.

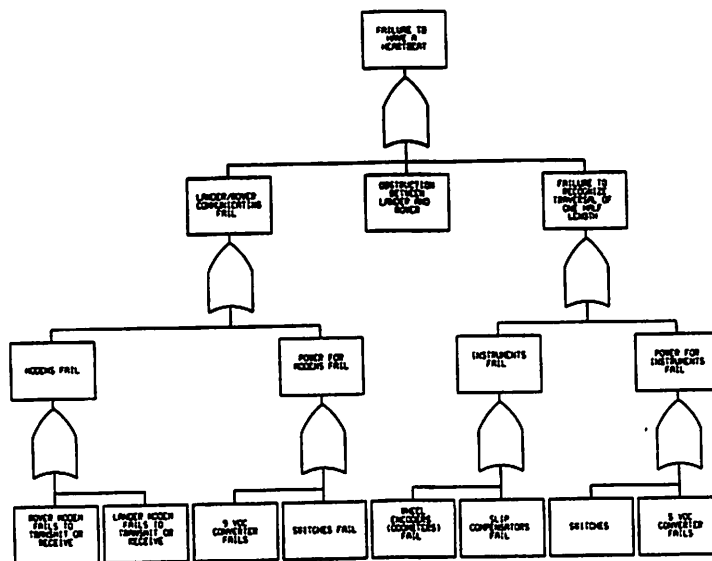
To continue to be useful, the risk model should be updated to reflect the evolving design. This will continue to place individual changes into an integrated systems context. Inevitably in a technology project, difficult decisions arise that deal with competing attributes such as cost, schedule, technical performance, and mission risk. Having quantitative risk estimates of risk (including uncertainties) would be most useful for such decisions. This can be initiated now and the estimates updated as additional information becomes available.

## ACKNOWLEDGMENTS

The authors wish to thank the microrover project team at JPL, led by Donna Pivrotto, whose enthusiastic support and openness helped make this a successful risk assessment.



### Exhibit 1. Event Sequence Diagram for Day Operations Phase



### Exhibit 2. Simplified Fault Tree for Failure to Maintain Heartbeat

**099 Root Cause and Precursor Analysis**

*Chair: M.G.K. Evans, NUS*

**The Barseback Incident - A Precursor Challenging Fundamental Safety Principles of LWRs**

*L. Carlsson, S. Erixon, C. Karlsson, B. Liwang, J. Olsen (SKI); G. Johanson (Ind. Proc. Saf.)*

**Inferring Safety Trend From The Accident Sequence Precursor Analysis Program**

*M. Modarres (U. Maryland)*

**Estimating the Frequency of Electrical Overload Events in the Proposed Space Station**

*T. Paulos, F. Issacci, I. Catton, G. Apostolakis (UCLA)*

## THE BARSEBÄCK INCIDENT - A PRECURSOR CHALLENGING FUNDAMENTAL SAFETY PRINCIPLES OF LWRs

Lennart Carlsson<sup>1</sup>, Stig Erixon<sup>1</sup>, Gunnar Johanson<sup>2</sup>, Christer Karlsson<sup>1</sup>,  
Bo Liwång<sup>1</sup> and Jan Olsén<sup>1</sup>

<sup>1</sup> SKI, Swedish Nuclear Power  
Inspectorate  
BOX 27106  
S-102 52 Stockholm Sweden

<sup>2</sup> Industrial Process Safety AB  
Svartvikslingan 11  
S-16129 Bromma, Sweden.

### INTRODUCTION

This paper will present an overview of the "Barsebäck - Incident" on July 28 1992, from a regulatory point of view. The incident is described as it was interpreted right after the event and during the following weeks and months, as the severity of the incident and the understanding of the phenomena involved was better understood. Before the Barsebäck incident the discussion was concentrated on the issue if backflush operation (BFO) was needed or not as a part of the design of the emergency core cooling system (ECCS) and containment spray (CS). Most light water reactors (LWR) do not include BFO in their design basis and are not equipped with any possibilities to prevent cavitation of pumps, due to clogging of suction line strainers in ECCS recirculation mode. This incident and the lessons learned include important issues that are generic for all western boiling water reactors (BWR) and pressurized water reactors (PWR). The clogging phenomenon is a generic problem for all reactor designs using the concept of recirculation for emergency core cooling, and our experience indicates that this problem applies to all plants and therefore this is not a specific Swedish BWR problem.

### BACKGROUND

On July 28, at 05.39 a safety relief valve on the main steam line inside the containment dry well opened inadvertently, 1, reference in figure 1. The reactor was in start up operation after refuelling and the reactor power was < 1% and the reactor pressure was at 30 bar when the relief valve inadvertently opened. The reactor was shutdown, the containment was isolated, ECCS and CS was actuated. The inadvertent opening of the safety relief valve corresponds in size to a small loss of coolant accident (LOCA) (close to medium). The root cause for the valve to open inadvertently was a leak in a pilot valve due to maintenance error.

This specific relief valve is designed to discharge directly into the containment dry-well compartment. The steam beam ripped off surrounding thermal insulation material from piping nearby, 2, (the design aspect of allowing a relief valve tearing off insulation will not be discussed here). This material was transported with the CS flow down to the wet well, 3 & 4. Later on, after 70 minutes, the strainers in the containment spray pump suction lines were "clogged", 5, - high differential pressure alarm was received (CS pump cavitation protection



alarm, high pressure drop over the pump suction line strainers). The strainers were later backflushed to remove the dislodged thermal insulation material from the strainer surface<sup>1</sup>.

Due to earlier design backfitting the event itself had a small risk but the event as a precursor is outstanding. Dislodged insulation material was identified as a significant safety problem already in the 1970's. The existing plants were at that time backfitted with strainers and backflush possibility of intake strainers in the ECCS as well as in the containment spray systems. As a part of plant specific probabilistic safety analysis (PSA) carried out during the 1980's, the manual initiation of backflush operation was studied and an alarm indicating clogged strainers was installed in the control room in Barsebäck. A number of sensitivity studies were carried out by varying the probability of initiating backflush and cleaning of the strainers.

The most critical information revealed by this incident was the behaviour of the insulation material and the timing of the scenario, clogging of the strainers after ~1 hour for a small LOCA. This in turn raised the question whether there would be enough time to meet this situation in the event of a large or a medium size LOCA.

In the procedures for backflush operation it is anticipated that there are 10 hours before any clogging problems will occur. The incident indicates that this time is much shorter for a large LOCA. If the time interval is too short it is impossible to carry out the existing procedure for BFO.

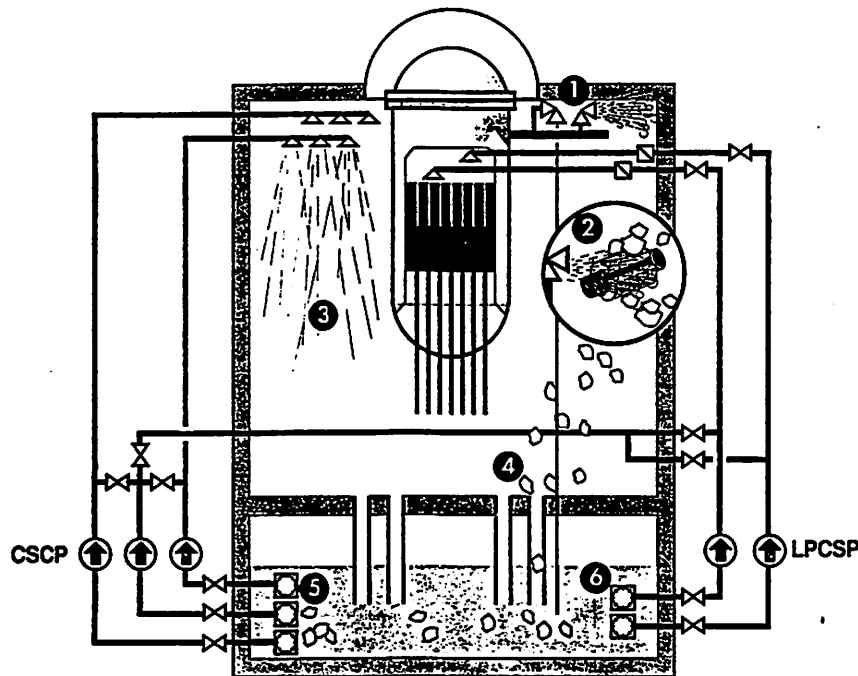


Figure 1. Illustration of the Barsebäck 2 incident.

## THE SHUTDOWN DECISION

The event analysis carried out following the incident focused after some time on the clogging of strainers in large LOCA situations. The original safety analysis estimated the time to clogging of ECCS suction strainers to 10 hours in this case. The event in Barsebäck indicated that clogging was possible much earlier, in the first estimates as early as 20 minutes, later analysis indicated even shorter time frames down to a couple of minutes. The confidence in that estimate was also weak because the precursor highlighted that the original experiments from the 1970's were not correctly designed for an accident condition with heat exposed and thereby aged insulation material. Six weeks after the incident the SKI decided to shut down five of the Swedish BWR's. At this point the complexity of the event and the large range of uncertainties was reevaluated<sup>2</sup>. The incident in Barsebäck 2 showed serious deficiencies in the emergency

cooling systems that applies to the five oldest BWR's in Sweden, which are equipped with small strainers and a backflush procedure. The four remaining BWR's with later design have strainers with larger areas than in Barsebäck, 30 m<sup>2</sup> instead of 1.1 m<sup>2</sup>. The rationale behind the shutdown decision was to a large extent based on probabilistic arguments since it could be expected in a worst case scenario that no means of ECCS and CS would be available following a large LOCA. The implication of the event evaluation was that fundamental safety principles for the design basis accident were violated, i.e. the "30-minute rule" (The reactor safety should not depend on manual actions during the first half-an-hour after an incident) and the single failure criterion.

Besides the violation of basic design principles the safe operation of the plants could not be demonstrated on a probabilistic basis. The core damage frequency increased to the order of the LOCA frequency, from  $1 \times 10^{-5}$  to  $> 1 \times 10^{-4}$ . The periodic safety reevaluation, i.e. the PSA, provided the essential basis for enabling the problem to be identified. The Swedish Nuclear Power Inspectorate defined a minimum set of requirements for continued operation until the refuelling outage in 1993.

- The 30-minute rule should be reestablished.
- Single failures should be eliminated.
- The backflush operation should be assumed necessary at least 3 times per hour in the beginning of a large LOCA scenario.
- The PSA should show risk estimates at about the same level as was the case before the event.

## DETERMINISTIC ANALYSES AND EXPERIMENTS

After the shutdown decision a very intensive period started in order to redesign the plants and the strainers in the condensation pool. First, design criteria had to be determined. Second, design solutions had to be evaluated by carrying out analyses of system availability and man machine issues.

The initial experiments were carried out to answer the following questions; 1-How much of the insulation rips off the pipe when exposed to a steam jet beam? 2-How much of the insulation material will be transported down to the condensation pool? 3-How will the insulation material build up on the strainers? and 4-Can the pressure drop over the strainer be determined for postulated cases? It showed to be very difficult to perform these experiments in a representative way.

It is very intricate to assess the amount of the isolation that rips off the pipes. No tests have included the layout in drywell. The transportation of the isolation material down to the condensation pool is also difficult to estimate, it has now been assumed that all loose material will arrive to the pool. Tests that are representative have not been made.

Table I summarizes parameters having impact on the speed of the pressure drop build up over the strainers. The ageing effect due to heat exposure is important for mineral wool insulation. The scaling factors are arduous to estimate. It is very difficult to build the fibre coating on the strainer in a proper way. The order in which fibers, fines and other granules arrive at the strainer is very important. For example more fibers at the beginning of the build-up leads to lower pressure drop over the coating. The spread of the results indicates that there are parameters that we do not know enough about and probably many of these parameters derive from chemical parameters. In Sweden tests have been done on aged and steam blowed mineral insulation and fibre glass in combination with granules. Experiments with combinations of materials gives a much higher pressure drop.

Relating the results from the experiments performed in Sweden and Finland with NUREG/CR-2982<sup>3</sup> one conclusion is that the method for disintegration of insulation material used in the US experiments is not representative for the scenario following a large LOCA. The experiments carried out now indicate that steam blowed insulation gives much higher pressure drop than insulation that has been teared mechanicly into small pieces. Further, the consequences of steam jet beams in the containment dry well are severely misjudged. Small particles, in combination with fibers, can rapidly increase the pressure drop over the strainers.

Examples of particles are crud, concrete debris, caposil and fines generated from the steam blown fibrous materials. The strainer areas suggested as design basis in NUREG-0897<sup>4</sup> are not sufficient even with BFO possibilities (NUREG-0897 does not include BFO in design basis). The NUREG's are obviously wrong in some important areas and the requirements raised in those reports are not sufficient as a basis for design against this scenario.

Table I. Parameters having impact on the timing of the clogging phenomenon and pressure drop build-up on the strainers.

Parameter	Comments	Impact on pressure drop build up
Material; mineral wool insulation, fibreglass insulation	The tests indicate that pressure drop over glass fiber is lower than the pressure drop over mineral wool.	1.5 to 2 times
Heat-exposure/ageing	Tests have shown that mineral wool disintegrates easier when it has been heat exposed. This causes higher pressure drops over the bed.	Verified for mineral wool. Not verified for glassfiber. Not quantified.
Disintegration	The tests indicate that steam blown insulation gives much higher pressure drop than the teared one.	100 times
Temperature	Finnish test show that a building up of the coating at 40°C instead of 20°C gives a higher pressure drop.	1.5 to 2 times
Small particles "fines"	Tests show that small particles could cause big pressure drops with fibrous materials. Examples of small particles are caposil (calcium silicate armed with asbestos), CRUD, concrete debris and fines from fiber insulation.	Over 100 times
Test set-up	Parameters that can have an influence on the building up of the coating acts differently in different scales. Small scale tests can be misleading.	Verified but not quantified
Flow velocity over the strainer	A high flow rate creates a more compressed bed and will cause increased pressure drop over the bed	Verified but not quantified
Candidate parameters for further investigation		
Microstructure of the insulation material;	Pretreatment of the insulation material, aged steam blown or chopped, gives the portions of fines and grains. The amounts of the different categories of particles are not classified.	
Flocculation and sedimentation	Behaviour in the suppression pool with representative conditions is not investigated.	
Viscosity and chemistry of the water;	Contamination of the water with fenol, borax, concrete debris can change the PH in the water. This could change the electrostatic potential of the fibers and other particles. Small particles can then easier attach to the coating	
Content of nitrogen in the water	Could cause bubbles in the fibrous bed which increases the pressure drop. A similar behaviour has been identified with air bubbles.	

## DESIGN SOLUTIONS

The redesign of the plant was performed with two main problems in hand. First, frequent clogging of the strainers and second, an uncertainty exists as to whether the operators can successfully perform the backflush operation in the short time available. The basis for the redesign was to restore the conditions for the performance of the emergency core cooling systems according to the FSAR without changing operating procedures, i.e. no backflushing needed within 10 hours. The possible solutions in consideration were:

- Improve the thermal insulation by replacing aged mineral wool.
- Enlarge the strainers, originally ~ 1m<sup>2</sup>.
- Provide additional and independent water supply for backflush operation, in the original design containment spray pumps are used to backflush the emergency core cooling pumps

and vice versa.

- Design for automatic backflush operation in order not to need operator actions within the 30 minute time frame.

The new designs now installed in the plants include a mixture of the above solutions<sup>5&6</sup>, figure 2. One pool in the reactor hall provides an independent water supply, 1, and improvements are made in the original backflush arrangement, 2. Automatic backflush operation actuated on the pressure drop over the strainers is in place. The backflush operation is provided by gravity simply by opening one valve connected to the ECCS suction lines. Continuous ECCS flow can be provided during backflushing. The strainers have been enlarged, 3. The areas of the strainers in the ECCS system and CS system at Barsebäck 1 & 2 and Oskarshamn 2 are now 18m<sup>2</sup> per train, a factor 16 in area increase, of which 1,4 m<sup>2</sup> can be backflushed. The Ringhals 1 plant has increased the area by a factor 26. The thermal insulation has been replaced to a large extent with glass fibre or mirror insulation, 4.

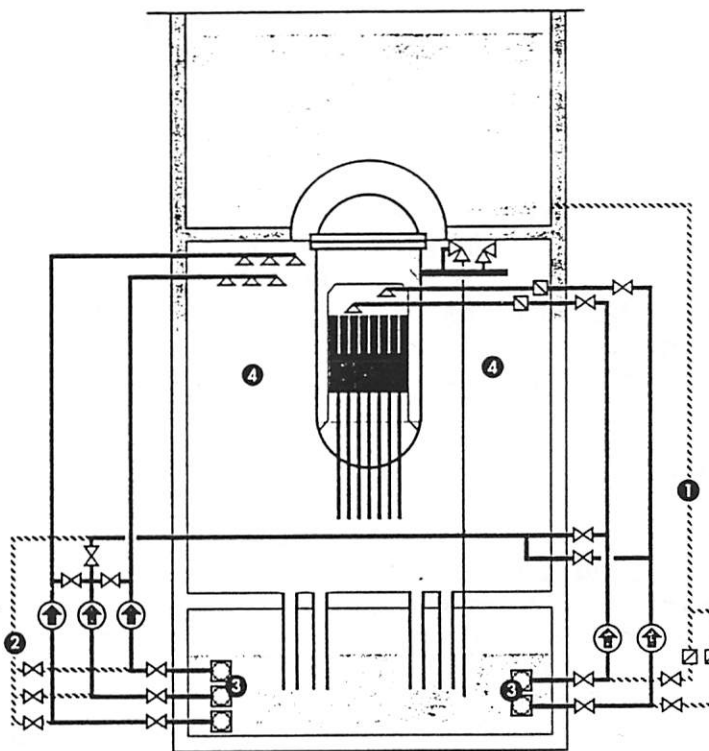


Figure 2. Measures to restore the level of safety.

## REGULATORY SAFETY EVALUATION

The Swedish Nuclear Power Inspectorate (SKI) carried out safety evaluations of the different design concepts suggested. Important aspects in this review were

- 1- the actual design basis, what phenomena are you designing to be able to handle,
- 2- the safety impact of the design solution, was the design functionally reliable and robust against worst case assumptions regarding the clogging phenomena,
- 3- the verification and testing of the suggested design,
- 4- the operator situation and the conditions for securing required operator actions and
- 5- general quality assurance

The licensees showed by analysis that the safety requirements were met with the proposed modifications<sup>7 & 8</sup>.

## CONCLUSIONS

The incident shows that the ability to backflush (i.e. -BFO design -procedures and -an available time window) is critical for the ECCS function. Before the Barsebäck incident the discussion was concentrated on the issue if BFO was needed or not as a part of the design of ECCS. Most LWR plants do not include BFO in design basis and are not equipped with any possibilities to prevent cavitation of pumps in ECCS recirculation mode, due to clogging of suction line strainers. The problem for the Swedish plants was that the time window available to carry out the BFO was much shorter than estimated in the design basis, ECCS operation at a large LOCA was unlikely to succeed.

A large range of experiments were carried out to better understand the clogging phenomena of the condensation pool strainers. It was found to be very difficult to perform these experiments in a representative way. In the experiments the worst case assumptions were not conservative enough in the early experiments, so continued experiments are required to make them more representative by taking into account what has been learned at later stages in this process. The lesson learned from this work that started in July 1992 and continued until March 1993 when four of the plants were restarted, is naturally the ABB-BWR specific insights on how to redesign the ECCS and CS. From a Swedish point of view one can claim that the plants were prepared to handle this situation since the ABB-BWRs are designed or backfitted, due to PSA results, with backflush operation of the condensation pool strainers including instrumentation and operational procedures to handle this situation. However, if the available time frame is too short it is impossible to carry out the procedure.

The clogging phenomenon is a generic problem for all reactor designs based on the concept of recirculation for emergency core cooling from the pressure suppression condensation pool (BWR) or the containment sump (PWR). Our experience indicates that this problem applies to all plants and therefore is not a specific Swedish BWR problem. The NUREG's (-2982 & -0897) are obviously wrong in some important areas and the requirements raised in those reports are not sufficient to use as a basis for design against this scenario.

## REFERENCES

1. NEA/IRS 1294.01, Clogged pump suction strainer in the wet well pool, August 8, 1992.
2. NEA/IRS 1294.02, Decision to discontinue operation due to clogged pump suction strainer in the wet well pool, September 18, 1992.
3. NUREG/CR-2982, Revision 1, "Buoyancy, Transport, and Head Loss of Fibrous Reactor Insulation" D.N. Brocard, Alden Research Laboratory, July 1983, (also Sandia National Laboratory, SAND-82-7205).
4. NUREG-0897, Revision 1, "Containment Emergency Sump Performance", A.W. Serkiz, October 1985.
5. Barsebäck NPP. Application for continued operation after implementation of design changes regarding insulation and strainers, the BOTVID project. Ref:1993-07-12, PQB. Kenneth Zander, 1610.04371. (In Swedish)
6. M. Dellby. Summary report of experiments and analysis of loose insulation material at LOCA conditions. Report SDC 93-1275. ABB-Atom, Västerås 1993-07-05. (In Swedish).
7. L. Hammar. Barsebäck 1&2, Permission to resume operation after measures to ensure safe emergency core cooling and containment spray in cases of a LOCA, NEA/IRS 1294.03, January 6, 1993.
8. L. Hammar. Oskarshamn 1&2, Permission to resume operation after measures to ensure safe emergency core cooling and containment spray in cases of a LOCA, NEA/IRS 1294.04, January 26, 1993.

## **INFERRING SAFETY TREND FROM THE ACCIDENT SEQUENCE PRECURSOR ANALYSIS PROGRAM**

**M. Modarres\***

Center for Reliability Engineering  
Department of Materials and Nuclear Engineering  
University of Maryland  
College Park, Maryland 20745-2115

### **INTRODUCTION**

Accident Sequence Precursors (ASPs) as applied to nuclear plants are those operational events (e.g., incidents) which constitute important elements of accident sequence(s) leading to core damage. Differently said, those events that substantially reduce the margin of safety available for prevention of core damage can be considered precursors to core damage.

The ASP study<sup>1-4</sup> initiated by the Nuclear Regulatory Commission (NRC) in 1979, reviews operational events which are reported in the Licensee Event Reports (LERs) to determine their risk significance. So far LER events of 1969 - 1981 and 1984 - 1992 have been analyzed; LER events of 1982 and 1983 will be analyzed in the future. The NRC's office of Analysis and Evaluation of Operational Data (AEOD) is currently responsible for the ASP program. The AEOD's objective is to identify those LER events that can be considered as significant precursors to severe core damage accidents. The significance of an LER event is measured through its conditional probability that the event leads to a core damage.

The ASP program serves the following functions<sup>5</sup>:

- Search operational events reported in LERs for the elements of potential severe core damage accident sequences.
- Analyze operational events and rank them according to their probability of proceeding to core damage.
- Identify significant or important sequences that, more likely than others, could lead to severe core damage.

Although the process of identifying operational events as precursors to core damage and

---

\* This work was performed when the author was a visiting professor at NRC's Office of Nuclear Regulatory Research.

the subsequent assessment of risk significant of precursors have changed in the past 10 years, the main focus of the ASP study and its methodology has not been changed. This allows its use for studying the safety trend in the operating nuclear power plants. That is, if the number of precursors and their severity as measured by the conditional core damage probability are showing a downward trend, then one can conclude that the nuclear plants are safer than before.

More recently the NRC's office of Nuclear Reactor Regulation (NRR) use the ASP results to identify safety trend in the operating nuclear power plants. On this basis, for example, the NRC staff response to Chairman Selin's request to study industry comments on the trend in core-melt probability concludes that: "The staff notes, on the basis of actual events, that the trend in the sum of the estimated conditional core damage probabilities show an overall decrease since 1970's. This can be used as an indicator of a corresponding downward trend in the probability of occurrence of a core damage."

Most recently, the ASP methodology was the center of discussion in an AEOD-sponsored workshop<sup>5</sup> in which some recommendations for improving the methodology were generated. The use of ASP results to study plant safety trends was a topic of discussion in this workshop. In this paper alternative methods of assessing an overall trend in the safety of operating nuclear power plants from the ASP results is discussed.

## SAFETY TREND BASED-ON PRECURSOR EVENTS

The ASP methodology is based on estimating the conditional probability of core damage given a precursor event by using observed operational events. Although core-damage frequency is not estimated by the current ASP program, earlier precursor analyses (1969 - 1981) calculated an estimate of core damage frequency. Such an estimate is an appropriate indicator of the operating trends and safety. Apostolakis and Mosleh<sup>6</sup> have suggested the following expression based on the use of conditional probability of core damage given a precursor events,

$$\lambda = \frac{\sum_i p_i}{T}, \quad (1)$$

where,  $p_i$  = conditional prob. of core damage given precursor event  $i$ , and  
 $T$  = total reactor-years.

In equation (1), the worth (contribution) of each precursor event  $i$  is counted as its conditional probability,  $p_i$ , that the event would have subsequently led to core damage. Obviously, if the event represents a core damage then  $p_i = 1$ , otherwise  $0 < p_i < 1$ . While  $\lambda$  is not estimated in the precursor study any more, the use of it as an indicator of the safety trend is of much interest in this paper.

A major concern raised with equation (1) is that it is a biased estimator. Namely, it overestimates the effective number of core damages used in the numerator of equation (1). Of course, the amount of overestimation is not exactly known, but one should approximately know it before this estimator can be used as an indicator overall plant of plant safety. Rubenstein<sup>7</sup> first described the nature of this overestimation followed by Cooke et. al.<sup>8</sup> and most recently Abramson<sup>9</sup> has described some approaches to make the estimation of  $\lambda$  unbiased.

While the biased estimation issue with equation(1) is a valid concern, Modarres<sup>10</sup> has argued that the magnitude of overestimation is negligible relative to other potential overestimation or underestimation errors associated with the calculation of the  $p_i$  values. The

later error is often resulted because ASP program uses generic event tree models and because these models are not sufficiently detailed (system level as opposed to train or component level). This is, however, somewhat alleviated by a number ad-hoc adjustments that the ASP program does to correct for this error.

More recently, trends in the number and significance of ASP results have been used as an indicator for the safety of operating plants<sup>11, 12</sup>. For example, NRR has used the sum of conditional core damage probabilities for each precursor as an indicator of plant safety. See Figure 1 for a typical trend representation. Also, the total numbers of precursor events per year and the number of events exceeding various decades of conditional probabilities (similar to Table 1) have also been used as indicators of plant safety. Sometimes the ASP data are scrutinized for apparent differences associated with plant age, size of utility company and type of reactor.

**Table 1. Number of Precursors<sup>4</sup> Ranked by their Significance**

year	pr(cd   precursor i) > 1.0e-4	pr(cd   precursor i) > 1.0 e-5	pr(cd   precursor i) > 1.0e-6
1988	7	21	32
1989	7	18	30
1990	6*	17**	28**
1991	12	20	27

\* including one event at cold shutdown

\*\* including two events at cold shutdown

## PROPOSED SAFETY TREND MODELS

As discussed earlier, the yearly core damage frequency estimated by equation (1) can be used an indicator of safety trend. An alternative method for estimating core damage probability or frequency is to rely on the variabilities observed in the  $p_i$  values. In this case, one can assume that precursor event occurrence follows a Poisson process. Since the  $p_i$  values are obtained from multiplications of other failure probabilities, one can also assume that a random variable representing  $p_i$ 's follows a truncated lognormal distribution (truncated at  $1 \times 10^{-6}$  and 1.0 levels). The truncated form of a lognormal distribution is used since the current ASP program does not consider precursors having less than  $10^{-6}$  conditional core damage probability. The process is illustrated in Figure 2. Suppose core damage is represented by the random variable CD. Accordingly, the probability of a core damage given a set of precursors observed within a fixed reactor-years of experience is

$$\Pr(\text{CD}) = \sum_i \Pr(E=i) \cdot \Pr(\text{CD} | E=i). \quad (2)$$

Where random variable E is the number of significant precursors, and CD is the event of a core damage.  $\Pr(E=i)$  is obtained from a Poisson distribution with a an intensity rate per reactor-year which is obtained from the annual rate of occurrence of significant precursors during the past years.  $\Pr(\text{CD} | E=i) = p_i$  is estimated from a truncated lognormal distribution which best fits the past  $p_i$  values. Accordingly, the problem reduces to estimating the parameters of the Poisson and the truncated lognormal distributions from the past ASP



experiences. Admittedly, errors in estimating  $p_i$  values would still be carried over into the estimation process. However, the biased issue is no longer a concern. Also, the model represents a better and more objective way of studying safety trends.

The proposed model captures both the variability observed in the number of significant precursor events, as well as the variability in the conditional core damage values. That is, both the number of significant events and their severity are modelled. If precursor events are also defined for a particular type of events or category of reactors, for example for shutdown events or for Westinghouse reactors, then equation (2) may be extended to a more general form by replacing the left hand side of equation (2) by  $\text{Pr}(\text{CD}_k)$ . Where the  $k$  subscript shows the contribution to the overall core damage from the  $k$ -th type of precursor events. Also,  $\text{Pr}(\text{CD}_k)$  as an overall safety indicator can be used individually or can be summed over certain types- $k$ .

Of course, similar to equation (2) this model assumes that the precursor data are independently and identically distributed. This crude assumption can be somewhat remedied by using a nonhomogeneous Poisson process for the occurrence of the precursor events. Additionally, one can use a Bayesian updating approach for estimating the truncated lognormal distribution (e.g., updating it yearly).

An alternative but similar model to the one discussed above can be obtained through the extreme value theory. In this model statistics from the severity of precursor events (i.e., yearly  $p_i$  samples of random size) are used to estimate the probability that the number of times that  $p_i=1$  would exceed 1 (i.e., at least one core damage occurs). Several forms of this model are possible. One simple form shows a cumulative density function for the random variable CD representing occurrence of a core damage. This form is developed and sometimes used for estimating the probability of extreme values; for example, probability of major earthquakes, or breaking strength of complex structures under extreme loads when only data are available for small earthquakes, or for small pieces of the structures<sup>13</sup>. The model assumes that precursor events occur according to a Poisson process, the frequency of their severity  $P$  is a random variable with cumulative density function  $H(p)$ . Accordingly, the cumulative distribution of extreme (significant) precursor events in  $t$  reactor-years is given by

$$\text{Pr}(\text{CD}) = \exp\{-\mu t[1-H(p)]\}, \quad (3)$$

where,  $\mu$  = Poisson occurrence rate (occurrence rate of precursors),  
 $t$  = reactor-years,  
 $H(p)$  = cumulative density function for the frequency of the conditional core damage probability  $p$ .

## APPLICATIONS OF THE MODELS

In this section an application of the model described by equation (2) is presented. The process is rather simple. The occurrence rate (intensity rate) of the precursor events are estimated from the past precursor data. Also the parameters of a truncated lognormal representing the variability of  $p_i$  values should also be estimated (remember that estimation of  $p_i$  may carry some uncertainty, but this is not explicitly modeled). Of course one can only calculate point estimates. For example, the occurrence rate of precursors events based on the 1984-1991 precursors is about  $1/3.3 = 0.3$  precursors per reactor-year (using a maximum likelihood estimation). See Table 2 for the data. Similarly, by using a moment matching technique the parameters of a matched truncated lognormal distribution showing the variability of the  $p_i$  values can also be obtained. Finally, from equation 2, the mean of a core damage probability per reactor-year for each year can be calculated. The results are

summarized in Table 2. The results are cumulative in nature. That is, the estimated overall core damage per reactor-year reflects the experience accumulated up to the year of interest. For example, the occurrence rate of precursors for 1991 is 0.3 per reactor-year, and the overall mean frequency of core damage is  $6.3 \times 10^{-5}$  per reactor-year for the same year. For estimating the truncated lognormal distribution a number of well established methods for estimating the parameters of such a distribution are available; examples are: moment matching, probability plotting, or simulation techniques (e.g., Bootstrap method).

While the mean frequency of core damage by the model in equation 2 is a reasonable indicator of an overall safety trend, it would be important to also consider its variability. For example, Figure 3 shows the overall trend based on the mean, and the 95% probability interval of core damage frequency for various years. For calculating the results shown in Figure 3, the concept described in Figure 2 is used along with a Monte-Carlo simulation. While the mean frequency of core damage shows a mild decline, the wide range of uncertainty associated with this estimate reduces our confidence to conclude that a reasonable decline in core damage frequency is observed.

## CONCLUSIONS

The ASP program is a valuable effort to identify important event occurrences in nuclear plants and their significance. The ASP results can be used to infer safety trends in nuclear plants. The methods used by the NRC to show a trend, while in the right direction, should be reexamined. In this paper two models for estimating trends are introduced. The application of one of these models to the 1984 - 1991 ASP data base shows a mild upward trend in the safety of nuclear power plants. However, in light of the variabilities observed and the uncertainties in the estimated conditional core damage probabilities used, the improving trend conclusion should be cautiously used.

Table 2. Analysis of Precursor Data for 1969 - 1981 Period

Year	Number of Significant Precursors	Cumulative Reactor-yrs	Mean Rx-years to a Precursor Event	Cumulative $p_i$	CDF Using Eq. 1	CDF Using Eq. 2
1984	33	82.3	2.5	0.0058	-	$7.1 \times 10^{-5}$
1985	39	172.2	2.4	0.0228	$1.5 \times 10^{-4}$	$1.3 \times 10^{-4}$
1986	19	268.8	3.0	0.0286	$9.9 \times 10^{-5}$	$1.1 \times 10^{-4}$
1987	34	372.2	3.0	0.0327	$9.2 \times 10^{-5}$	$8.7 \times 10^{-5}$
1988	32	479.8	3.1	0.0351	$5.1 \times 10^{-5}$	$7.2 \times 10^{-5}$
1989	29	590.0	3.2	0.0374	$5.3 \times 10^{-5}$	$6.3 \times 10^{-5}$
1990	28	701.6	3.3	0.0412	$4.1 \times 10^{-5}$	$5.8 \times 10^{-5}$
1991	28	809.0	3.3	0.0512	$5.9 \times 10^{-5}$	$6.3 \times 10^{-5}$

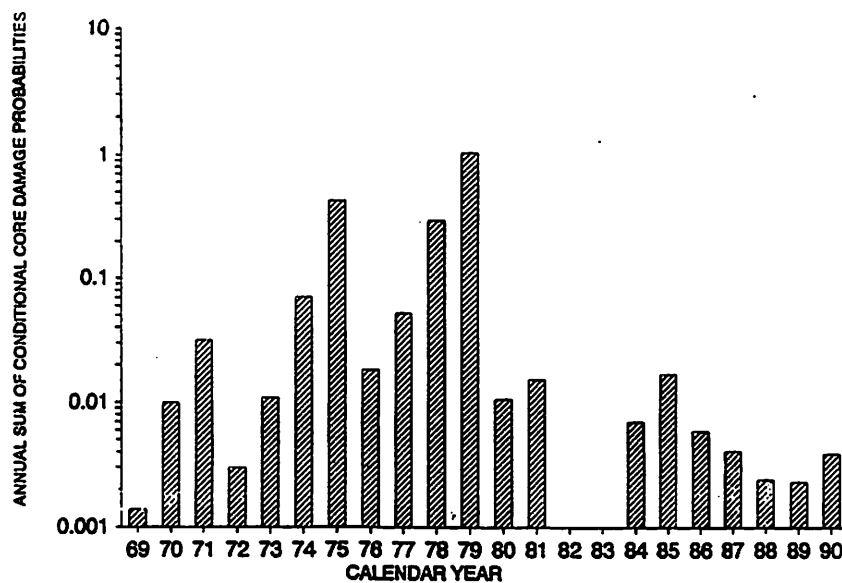


Figure 1. Annually summed ASP conditional core damage probabilities

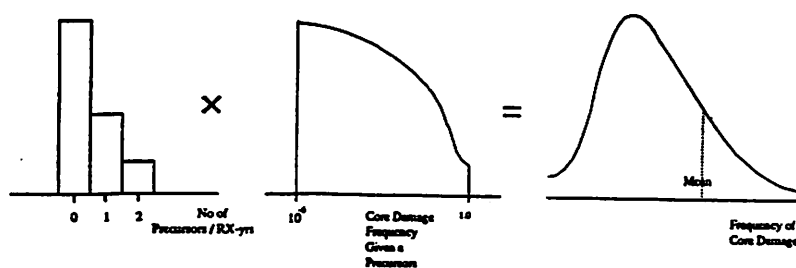


Figure 2. An alternative method for estimating the likelihood of at least one core damage

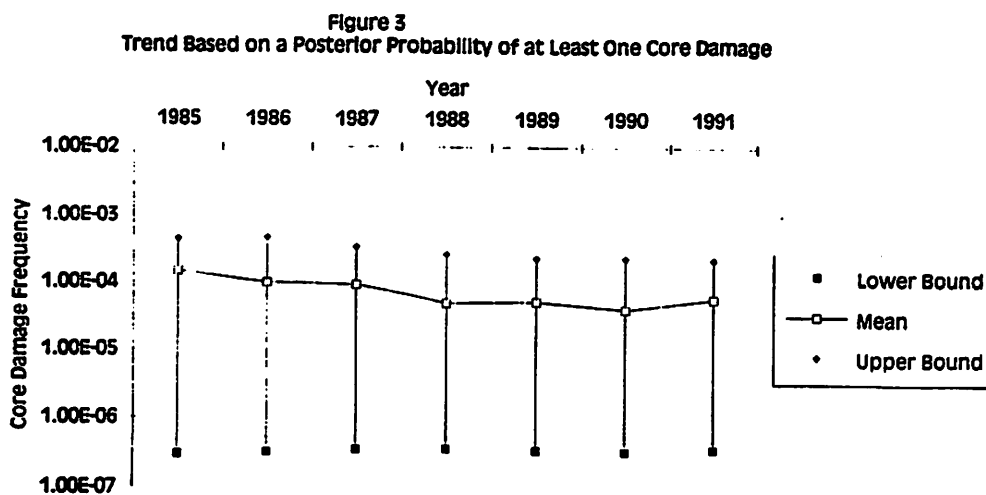


Figure 3. Trend based on a posterior probability of at least one core damage

## REFERENCES

1. Minarick, J.W. and C.A. Kukiella, Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report, USNRC Report NUREG/CR-2497 (1982).
2. Cottrell, W.B., J.W. Minarick, P.N. Austin, E.W. Harris, Precursors to Potential Severe Core Damage Accidents: 1980-1981, A status Report, USNRC Report NUREG/CR-3591, Vols. 1 and 2, (1984).
3. Minarick, J.W. et al., Precursors to Potential Severe Core Damage Accidents: 1984, A Status Report, USNRC Report NUREG/CR-4674 Vols. 1 and 2 (1986). Also Vols. 3-14 are status report for 1985-1990.
4. Minarick, J. W. et al., Precursors to Potential Severe Core Damage Accident: 1991, A status Report, USNRC Report NUREG/CR-4674 Vols. 15 and 16 (1992).
5. Proceedings of the Workshop on the Use of PRA Methodology for the Analysis of Reactor Events and Operational Data, Annapolis, MD, USNRC Report NUREG/CP-0124 (1992).
6. Apostolakis G. and A. Mosleh, Expert Opinion and Statistical Evidence: An Application to Reactor Core Damage Frequency, Nuclear Science and Engineering, 70, pp.135-149 (1979).
7. Rubenstein, D., Core Damage Overestimation, NUREG/CR-3591(1985).
8. Cooke R. M., L.H.J. Goossens, A.R. Hale, J. von der Horst, Accident Sequence Precursor Methodology - A Feasibility Study for the Chemical Process Industries, Technical University of Delft, Delft, The Netherlands (1987).
9. Abramson, L., Private Communications, U.S. Nuclear Regulatory Commission, Washington, D.C.(1992).
10. Modarres, M., The Accident Sequence Precursor Analysis: Review of the Methods and New Insights, Submitted for Publication to Nuclear Science and Engineering (1993).
11. Presentation by T. Murley to the ACRS subcommittee, February 4, 1992 on: Trends in Core-Melt Probability.
12. Memorandum (undated) from J. M. Taylor, Executive Director for Operations, NRC, for the NRC Commissioners, Subject : Status Report on Changes in the Probability of a Core Damage Accident as Inferred from Actual Events Occurring Between the 1970's and Today.
13. Castillo, E., "Extreme Value Theory in Engineering," Academic Press(1988).

## **ESTIMATING THE FREQUENCY OF ELECTRICAL OVERLOAD EVENTS IN SPACE STATION *FREEDOM***

T. Paulos, F. Issacci, I. Catton and G.E. Apostolakis

Mechanical, Aerospace and Nuclear Engineering Department  
University of California  
Los Angeles, CA 90024-1597

### **INTRODUCTION**

Fire events on board the space station are the threats with potentially the most catastrophic consequences.<sup>1</sup> Fire events, such as flaming, smoldering or electrical overheating occurrences, threaten the occupants with heat, toxic gases and smoke.<sup>2</sup> Combustion by-products and extinguishing agents can also contaminate the atmosphere and/or electrical equipment.<sup>3,4</sup> Repeated false alarms due to oversensitive detectors can also reduce a crew's effectiveness due to relaxation tendencies. The fire risk cannot be ignored.

To quantify the risk due to fire threats, a frequency estimate is needed. The purpose of this paper is to estimate the frequency of electrical overload (overheating) events in the U.S. Laboratory Module, a proposed section of Space Station *Freedom*. This estimate is based on past experience, current hardware design and human judgement.

### **Definitions**

Two terms are used almost interchangeably in this paper: shorts and overloads. Although they both refer to electrical overheating events, they are two separate and distinct failure modes. The discerning characteristics are based on magnitude and duration of the electrical event in question. The term overload refers to events in which the current level carried by a wire is greater than its rated capacity or when damage to the wire conductor, such as a "nick," causes a localized hot spot with a temperature sufficient enough to cause the insulation to thermally degrade. The term "short" is used to describe true, sustained dead shorts. These high energy events are power limited by the DC-DC converter and are likely to last only several seconds due to safety features built into the hardware, or due to the wire conductor melting. Shorts can be viewed as extreme overloads.

### **Past Events**

The main fire risk in spacecraft does not appear to be due to flaming fires, but instead from electrical overload and smoldering events. There have been at least five fire events

on Shuttle flights, and all have been due to smoldering and/or electrical overheating events.<sup>5</sup> The first occurred in April 1983 when several wires with Teflon and Kapton insulation overheated and fused together. The second occurred in August of 1989 when a teleprinter cable shorted. In December of 1990, a cooling fan failed which caused a resistor to overheat. In June of 1991, a refrigerator-freezer fan motor failed causing an overload situation to occur. The fifth event occurred in July of 1992, when a blown electrical capacitor caused another electrical mishap. All five events were detected by the crew, not the detectors. In addition, there have also been six false alarms and four smoke detector test failures.

### Expected Events and Critical Locations

These past experiences tend to support the belief that electrical overheating events will dominate the fire risk in future spacecraft, such as *Freedom*. Obviously, there are electrical components just about everywhere on-board a spacecraft, so engineering judgement must be used to evaluate which areas would be more likely to have such an event to occur.

Most fire scenarios that have been examined<sup>6</sup> could be based on incidents originating within a closed compartment termed a "rack," which is essentially a wall drawer.<sup>7</sup> The occupied *Freedom* volumes, or modules, will be constructed of banks of racks surrounding the central core volume on four sides. Most racks will contain electrical equipment; many may also contain flammable solids or fluids. It is felt that the frequency of electrical events in these areas will dominate the fire risk, and hence, these areas must be deemed as critical.

### FAULT TREE

There are two paths to failure, direct and indirect. A direct failure occurs when a component failure initiates a short or overload directly. For example, an aged cooling fan draws more power than the feed wires are rated to carry, and the resulting wire conductor temperature is sufficient enough to cause an overload condition. The fan may also fail by shorting, in which case the power feed wires would be subject to an even greater overload.

The indirect failure path is initiated by a general component failure (the component fails in any mode other than a short or overload) and is completed by a human error that occurs during the maintenance task. For example, a pressure sensor is giving false readings and needs to be replaced. During the maintenance action, a power feed wire gets nicked, and the resulting conductor temperature at the nick is sufficient enough to cause an overload. An error in re-wiring that causes a short may also occur. Figure 1 shows a simplified fault tree depicting the two paths to failure.

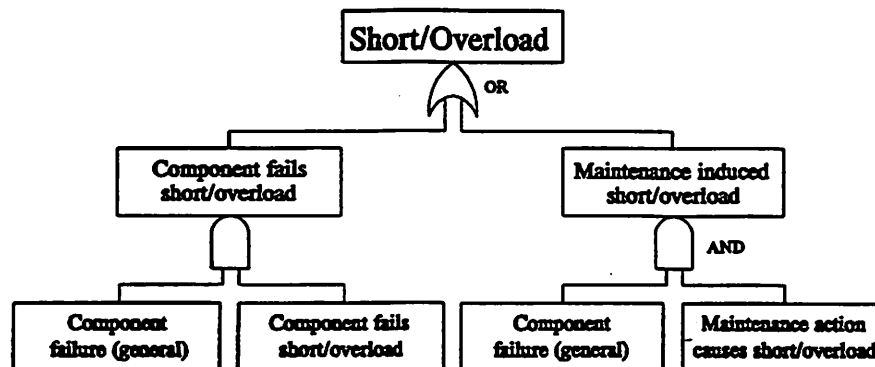


Figure 1. Simplified Fault Tree Showing Two Paths to Failure

## THE U.S. LABORATORY MODULE

In the U.S. Laboratory Module, there are 24 racks--six on each "side" of the module. Several racks are dedicated to various systems, such as the Data Management System, the Temperature Control System, the Fire Detection and Suppression System, or for cabin air delivery. Approximately one-half of the racks are for payload (both scientific and commercial) purposes. Others are used for storage or for workstations.

The rack to be examined in this example is officially designated LAP 6. This proposed rack is dedicated to support the Cabin Air, Crossover and Thermal Control Systems. Twenty-one components have been identified as possible event initiators and/or require periodic maintenance. See Table 1 for a list of rack LAP 6 components that could act as event initiators.

**Table 1. Components in Rack LAP 6**

Components and Abbreviations	
Atmosphere Control System/Temperature Control System (ACS/TCS) N <sub>2</sub> internal rack assembly	Pump package assembly
Circulation fan assembly	Rack Essentials Controller (REC)
Coldplate assemblies (2)	Rack Flow Control Assembly (RFCA)
Connector supply backpane	Remote Power Distribution Assembly (RPDA)
Electrical interface box	Remote Pressure Equalization Valve (RPEV)
Fan group Orbital Replacement Unit (ORU)	System flow control assembly
Flow meter	Temperature Control and Check Valve (TCCV)
Inlet ORU	Water separator ORU
Outlet temperature assembly	Wire harnesses (2)
	Wires

## FREQUENCY ASSESSMENT

This section explains the frequency estimation process. To perform this analysis, several assumptions were made and probability distributions assumed.

### Assumptions

In calculating event frequencies for the entire U.S. Laboratory Module, some assumption as to failure frequencies in other racks needs to be made. For this example, the components in rack LAP 6 are assumed to have similar failure rates compared to components in other racks dedicated to systems support or payloads. Storage racks contain little or no functioning electronic equipment, so the calculation ignores them by reducing the number of racks that are, on the average, in use. This calculation also assumes that component failures due to infant mortalities and extreme conditions, such as high temperature, radiation or humidity situations, is negligible. The IEEE Standard 500<sup>8</sup> Handbook states that these types of conditions may increase a component's failure rate by a factor of two or more, but since these conditions are rare, they are not taken into account.

### Probability distributions

The following aspects of the frequency calculation are better described by probability distributions than as set, distinct values.

**Component failure rate data.** Failure rate data for most of the components in rack LAP 6 comes from Boeing, which is responsible for their design and buildup.<sup>9</sup> This data is given in terms of mean time to failure and duty cycles and is considered to be exponential. The failure rate of the wire insulation and flow meter come from the IEEE Standard 500 Handbook.<sup>8</sup> One component, the Rack Essentials Controller (REC), was assumed to have a failure rate comparable to the Remote Flow Control Assembly (RFCA) and a duty cycle of 100% since no failure data could be obtained.

**Component Fail Short/Overload (CFS/O).** When a component fails, there are many particular modes in which the failure may occur. The probability of a component failing in a specific mode, such as a short or overload, varies from component to component. Extensive real world data is needed to accurately describe this probability. Although sources such as the IEEE Standard 500 Handbook have had years of experience with nuclear plants, industrial plants and manufacturer's reliability data, this data is not yet available for components (in most cases) to be used in the space station. Hence, expert judgement and failure data of similar components from terrestrial applications must be used to estimate these probabilities.

One opinion<sup>10</sup> stated that a conservative estimate of 10-25% be used to describe the percentage of total component failures that are overloads and shorts. Although this may be higher than 40% for some components,<sup>8</sup> a value of 20% was selected for all components. Of this value, an estimation was made that a fail-overload is four times more likely to occur than a fail-short. Assuming a normal distribution, the CFS probability has a mean value of 0.04 and a standard deviation of 0.01. The CFO probability was also given a normal distribution, but with a mean value of 0.16 and a standard deviation of 0.04.

**Maintenance Induced Short/Overload (MIS/O).** The Human Reliability Analysis (HRA) manual has been used extensively in nuclear power plant assessments in the past to determine the probability of human errors occurring in different situations, such as maintenance tasks or decision making under high stress situations.<sup>11</sup> In this example, an initial probability of 0.01 was selected as the probability that a maintenance action would cause a short or overload; however, two other, important factors need to be considered. First, the crew will be considered novices since they will have less than six months "on-the-job" experience, and second, the expected workload will be heavy. The HRA manual recommends a multiplication factor of ten to be used to adjust the given initial probability and that a lognormal distribution with an error factor of five be used. Similarly to CFS and CFO probabilities, it is felt that the probability of a MIO is four times as likely as a MIS. Hence, the MIS probability is a lognormal distribution with a mean value of 0.02 and an error factor of five, and the MIO probability is also a lognormal distribution with an error factor of five, but with a mean value of 0.08.

**Racks in use.** Although there are 24 racks in the U.S. Laboratory, they will, most likely, not all be occupied at any given time. A truncated normal distribution with a mean value of 20 and a standard deviation of one has been selected to represent, on the average, how many racks are in use. The probability distribution has been truncated at 16 and 24 to prevent extreme values from biasing the results: 16 was deemed an appropriate lower limit and at the other extreme, only 24 racks are available.

#### **Spreadsheet calculation**

The frequency calculations were performed using an Excel<sup>®</sup> spreadsheet, and the uncertainty calculations were made using @RISK<sup>®</sup>, an Excel<sup>®</sup> add-in program.



**Frequency estimate.** The spreadsheet calculation determines the expected total number of component failures through the thirty year simulation based upon the mission mean time to failure, which takes into account duty cycles for components. The CFS/O and MIS/O probability distributions are then used to estimate the number of shorts/year and overloads/year that will occur. Finally, this thirty year estimate for one rack is related to a per year estimate for the entire module. The results are presented in the next section.

**Uncertainty propagation.** The @RISK<sup>®</sup> Monte Carlo simulation (10,000 iterations) was used to propagate the uncertainty errors and to develop the probability distributions for both the expected number of shorts/year and the expected number of overloads/year.

## RESULTS

A graphical representation of the expected shorts simulation is in Fig. 2. This distribution represents a mean value of 1.25 shorts/year, a 95<sup>th</sup> percentile value of 2.27, a median value of 1.12 and a 5<sup>th</sup> percentile value of 0.65.

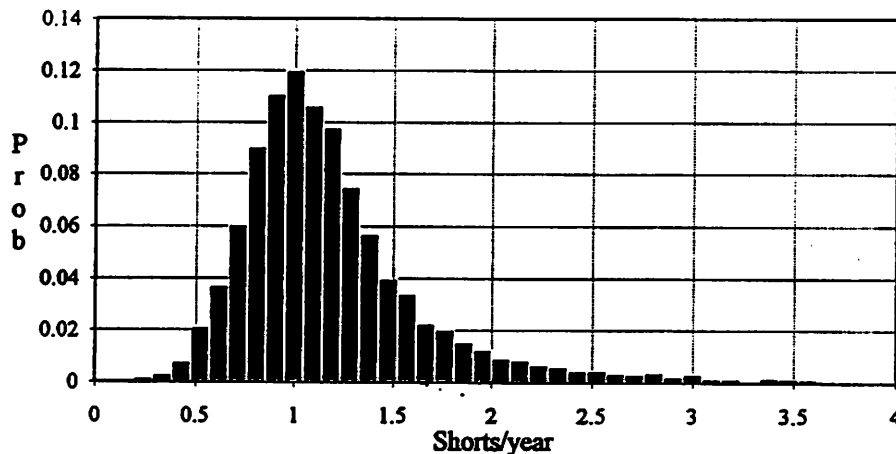


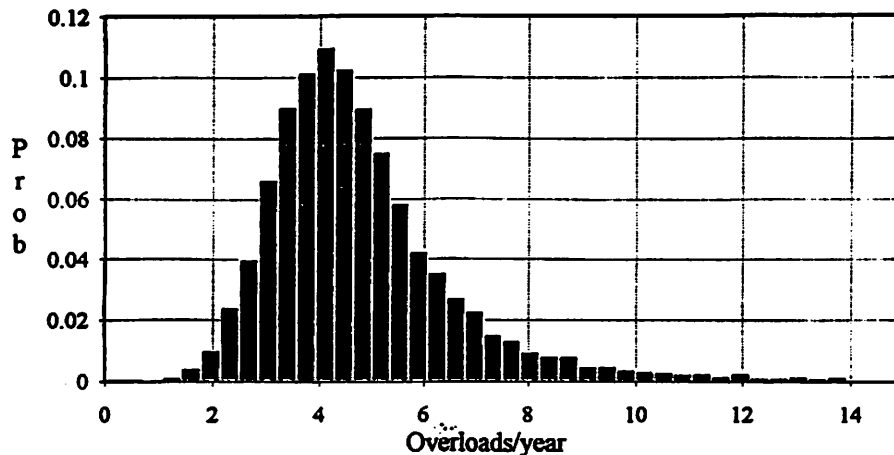
Figure 2. Simulation Results Showing Distribution of Estimated Shorts/year.

A graphical representation of the expected overloads simulation is in Fig. 3. This distribution represents a mean value of 5.00 shorts/year, a 95<sup>th</sup> percentile value of 8.68, a median value of 4.5 and a 5<sup>th</sup> percentile value of 2.77.

## CONCLUSIONS

The results of the simulation show that electrical overheating events are not negligible and cannot be ignored. Applicable microgravity testing needs to be performed and appropriate models developed so that the consequences of these events can be estimated. Risk management strategies also need to be developed to deal with these situations.

The Shuttle, having close to one year of operation time in space, has had at least five events: four overloads and one short. Although the space station and the shuttle are two different platforms, it is interesting to note how the frequency estimate and real world data compare.



**Figure 3.** Simulation Results Showing Distribution of Estimated Overloads/year.

### ACKNOWLEDGEMENT

The authors would like to thank Mr. Robert Friedman at NASA-Lewis (Cleveland, OH) and Mr. Robert Johnson at Boeing (Huntsville, AL) for their continued help and support. This project is supported by the NASA In-Space Technology Experiment (IN-STEP) program under contract number NAS3-25975A031.

### REFERENCES

1. R.L. Peercy, Jr., and R.F. Raasch, "Threat-Strategy Technique: A System Safety Tool for Advanced Design," *J. Spacecraft*, 23:200 (1985).
2. T. Paulos, et al., "Risk-Based Spacecraft Fire Safety Experiments," paper AIAA 93-1153 (1993).
3. R. Friedman and K.R. Sacksteder, "Fire Behavior and Risk Analysis in Spacecraft," ASME Winter Annual Meeting (NASA TM-100944), Chicago, IL (1988).
4. D.M. Karydas, "A Probabilistic Methodology for the Fire Smoke Hazard Analysis of Electronic Equipment," Factory Mutual Research Corporation, Norwood, MA (unpublished).
5. Robert Friedman, plenary speech given the Second International Microgravity Combustion Workshop, NASA Lewis Research Center, Cleveland, OH, Sep. 15-17 (1992).
6. W.R. Fuller and M.W. Halverson, "Space Station *Freedom* Program Risk Model Control Document," PLG, Inc., Newport Beach, CA (1989).
7. "Environmental Control & Life Support System Fire Detection & Suppression," Boeing Corporation, D683-15006-1, WP01 Space Station *Freedom* Program (1991).
8. "IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations," (IEEE Std 500-1984), IEEE, New York, NY (1983).
9. V. Hugo, personal communication (fax), Boeing Corp., Huntsville, AL (1993).
10. R. H. McFadden, personal memo (1993).
11. A.D. Swain and H.E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," (NUREG/CR-1278), Sandia National Laboratories, Albuquerque, NM (1983).

## **100 Reducing Errors through Quality and Design**

*Chair: T.G. Ryan, INEL*

**The Pros and Cons of Using Human Reliability Analysis Techniques to Analyze Misadministration Events**

*L.T. Ostrom (INEL)*

**Construction Error and Human Reliability for Structural Systems**

*M.G. Stewart (U. Newcastle)*

**The Feasibility of Designing Human-Error Backup Systems for Fail-Safe Structures**

*Y. Sato (Tokyo U.); K. Inoue (Kyoto U)*

**A Methodology to Support Space System Designer in Minimizing Human Error**

*M. Ferrante, C. Vivalda (Alenia Spazio); C. Fogli (ESA/ESTEC)*

## **THE PROS AND CONS OF USING HUMAN RELIABILITY ANALYSIS TECHNIQUES TO ANALYZE MISADMINISTRATION EVENTS**

Lee T. Ostrom, Ph.D., CSP

Idaho National Engineering Laboratory  
EG&G Idaho, Inc.  
P.O. Box 1625  
Idaho Falls, ID 83415-3855  
Telephone: (208) 526-2844  
FAX: (208) 526-9152

### **ABSTRACT**

This paper discusses the risk assessment methodologies applied to data collected during investigations of incidents in medicine involving nuclear by-product materials. These are called misadministration events. The risk assessment methodology applied to the data is fault tree analysis augmented with human reliability analysis. The results of the analysis has been beneficial for further elucidating the causal factors of the misadministration event analyzed. The risk assessment methodology did not provide all the benefits desired, however. For example, the methodology did not provide a good quantitative estimate of the risk of future misadministrations.

### **INTRODUCTION**

Medical applications of radionuclides involve both therapeutic and diagnostic procedures. Therapeutic procedures may include the use of relatively intense radioactive sources and have the potential for significant detrimental health effects if mistakes occur. The Nuclear Regulatory Commission (NRC) regulates these medical applications of radionuclides under 10CFR35. In this regulation, misadministration events are defined; licensees are required to report these events to the NRC.

Misadministration events generally involve errors in therapeutic or diagnostic applications resulting in the wrong dose being administered, the wrong site being treated, or the wrong patient being treated. In order to better understand the potential causes of these events, and to help examine the regulatory basis, the NRC Office of Nuclear Materials Safety and Safeguards (NMSS) is undertaking a risk assessment of misadministration events as part of an event investigation activity. This work represents one of the first applications to the safety of medical radioisotope devices of Probabilistic Risk Assessment (PRA) techniques developed to evaluate reactor safety. This paper discusses the methodology used to date, the problems encountered, preliminary insights from this first analysis, and possible future directions of the project.

---

This project was funded by the U.S. Nuclear Regulatory Commission and for the U.S. Department of Energy under DOE Idaho Field Office Contract DE-ACO7-76IDO1570. Views expressed in this report are not necessarily those of the Nuclear Regulatory Commission.

## METHODOLOGY

The methodology applied to the data discussed in this paper was PRA fault tree analysis augmented with human reliability analysis (HRA). The data to conduct the analyses were collected during site visits to facilities that had experienced misadministration events and from visits to facilities that performed similar procedures. These visits were beneficial because they enhanced the understanding of the medical procedures.

The risk assessment methodology dealt only with the top event observed during the event. The three possible top events were:

- Wrong treatment site
- Wrong dose administered
- Wrong patient being treated.

The event discussed in this paper was a wrong treatment site event.

### Description of the Event

This event involved the manual brachytherapy treatment modality. A patient undergoing treatment for cervical cancer received an unintended dose of radiation to her labial skin and the inner aspects of her thighs. This occurred because the technologist selected the wrong sources which were of a smaller diameter than the correct sources. The sources slipped through the opening in the end of a helical spring designed to keep the sources at the end of the source carriers of the Henschke manual brachytherapy applicator used in this treatment. A complete description of this event is contained in Ostrom, Leahy, and Novack<sup>1</sup>.

### Analysis Methodology

The risk assessment methodology used to perform the analysis was a combination of probabilistic risk assessment (PRA) and human reliability analysis (HRA). The process for conducting the analysis involved six steps. These were: 1) developing the process model; 2) developing the fault trees; 3) developing the HRA event trees for specific human action sequences; 4) quantifying the model; 5) generating the cut sets; 6) conducting a sensitivity analysis. The sensitivity analysis (Step 6) involved iterating on Steps 4 and 5 in order to model the process while varying performance shaping factors and postulating changes in the process. The following discusses each of these steps in more detail:

**Process Model.** A process model was developed using functional flow diagram (FFD) techniques<sup>2</sup>. The model basically shows the steps in the process in the order of their performance. The process model was developed using data collected from a misadministration site visit and a visit to a cancer center that performs similar treatments. This model was used as the basis for the rest of the analysis.

**Fault Trees.** There were three fault trees developed using standard PRA techniques. Figure 1 shows an example of the types of fault trees developed.

The human errors shown on the tree were determined in two ways. First, by input from the misadministration investigation site visit and, second, by postulating errors from the process steps shown on the process model. Medical professionals helped postulate these errors. HRA event trees were developed for sequences of human errors, such as the placement of the afterloader.

**Human Reliability Event Trees.** Figure 2 shows an example of the HRA event trees developed from the analysis of the process that existed at the time of the event. This tree was developed using the techniques described in THERP<sup>3</sup>. There were two sequences of human errors postulated. These were the Source Control Sequence (SCS) and the Afterloader Placement Sequence (APS). The SCS shown in Figure 2 depicts the event that was investigated during the site visit. The failure paths on these trees proceed diagonally

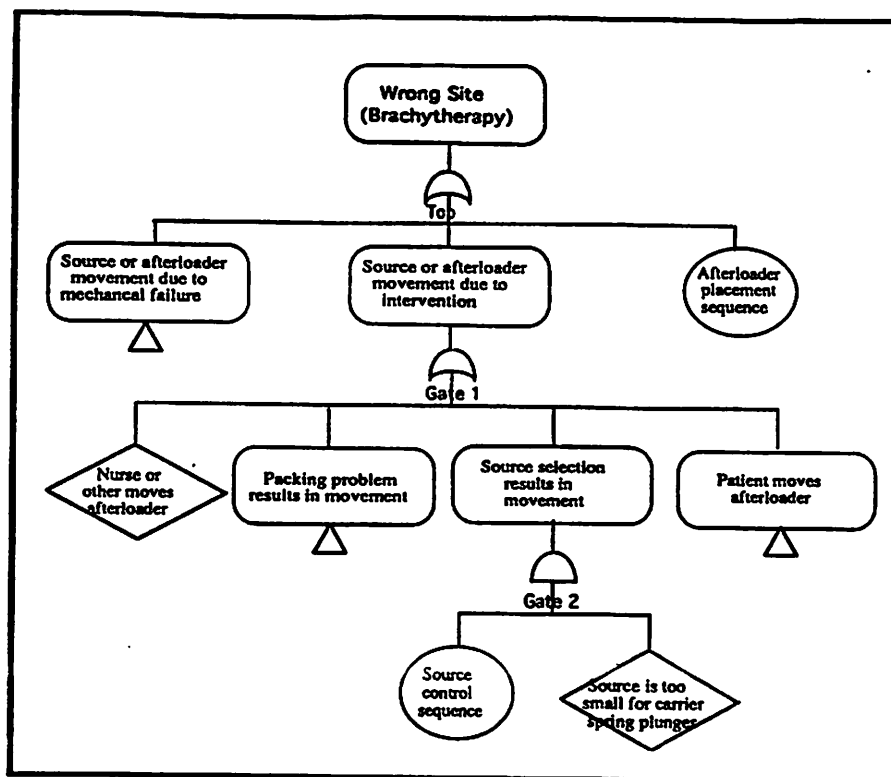


Figure 1. Fault tree developed for the event

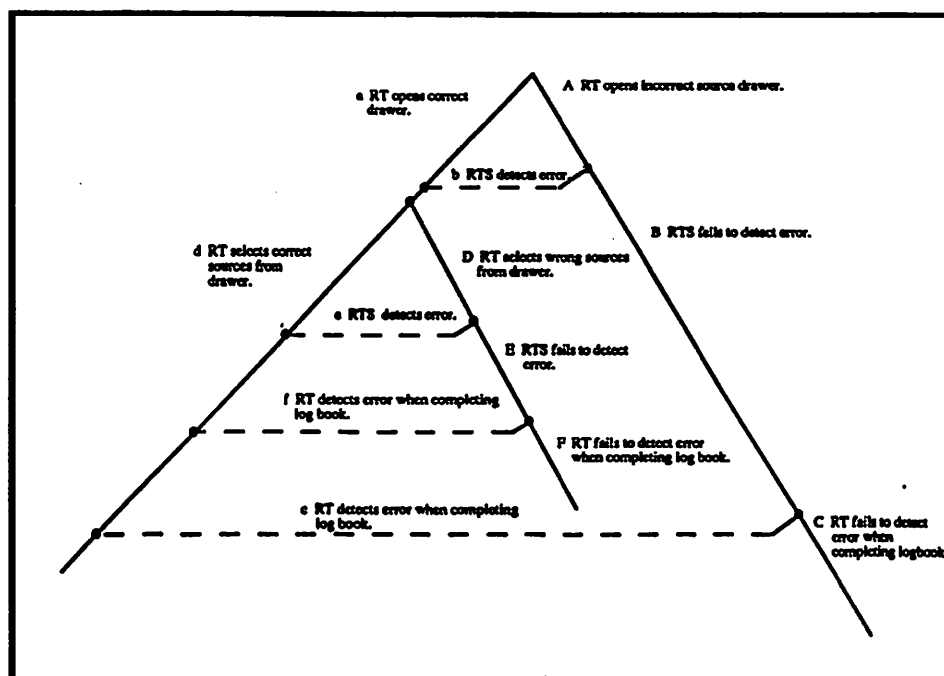


Figure 2. Source Selection Sequence

from upper-left to lower-right. Success paths proceed diagonally from upper-right to lower-left. Recovery paths are dashed lines and proceed from right to left. The capital letters denote errors and the lower-case letters denote successful actions.

There were three failure paths determined in the SCS. These were: ABC, aDEF, and AbDEF. There were also three failure paths in the physician placement sequence.

**Quantifying the Model.** THERP<sup>3</sup>, SHARP<sup>4</sup>, and ASEP<sup>5</sup> methodologies were used to quantify the human error probabilities. The hardware failure data were developed using a generic hardware failure rate of  $1.0E-3$ . This is a screening value and actual failure rates will be sought from the manufacturer. The hardware failure rates are probably high because there is no force placed on the welds and the material the afterloader is made of is high grade stainless steel. High grade pipe has a failure rate on the order of  $2E-5$  failures per hour and springs have failure rates on the order of  $4E-5$  failures per hour<sup>6</sup>.

Factors that were considered during the quantification of the human errors were the Radiation Technologist's lack of training, the poor labeling on the source safe, and the dependencies between the Radiation Technologist and the Radiation Technologist Supervisor.

The Radiation Technologist (RT) and Radiation Technologist Supervisor (RTS) errors were quantified using the data tables and methodologies contained in THERP<sup>3</sup>. Although there were not one-to-one correlations between the errors that were postulated in the model and those listed in the THERP tables, the categories were generally similar. It was assumed that 36% of the Cs<sup>137</sup> sources in the safe were small enough to migrate through the end of the spring. This was calculated by taking the number of 10 mg Cs<sup>137</sup> sources of the diameter used in the event and dividing by the total number of sources in the source safe at the time of the event. This value is an estimate; the exact number would vary depending on the age of the spring and whether the opening was damaged. The physician errors were more difficult to quantify, so SHARP skill-based screening values were chosen. It was assumed that the physician was well skilled; a value of  $5.0E-4$  was chosen as the HEP. This is the middle of the range for a skill-based error, which is from  $5.0E-5$  to  $5.0E-3$ . The patient errors were the most difficult to quantify. These were quantified by using ASEP pre-accident screening values. The value initially used was 0.03; however, this value was postulated to be too high because patients are medicated and instructed not to touch the afterloader. In fact, patients are afraid to touch the afterloader because of the fear of radioactivity. The medical consultant stated that in his twenty years of work in the field he has only heard of one case where a patient got up from bed. In this regard, we reduced the HEP for the patient actions by a factor of ten, which is the error factor, and used the value 0.003. This is the lower tolerance bound. This still made the value conservative, but more realistic. An ASEP screening value of 0.03 was also used for errors involving the nurse and transportation of the patient.

**Generating the Cut Sets.** IRRAS 4.0<sup>7</sup> was used to generate the cut sets.

**Sensitivity Analysis.** The sensitivity analysis involved varying performance shaping factors and postulating changes in the process. These changes were then quantified and an estimate in the change in the overall probability for failure was calculated. Two separate analysis were conducted.

The first analysis involved improving the level of stress of the workers, improving their training level, reducing the dependence between staff members, and adding independent verification steps to the process. The second analysis involved postulating the process with the incorrect sources removed from the source safe.

## RESULTS AND DISCUSSION

The risk assessment was interesting because it highlighted (a) the failure path that lead to the event, (b) the estimated effects of licensee's corrective actions on the failure path, and (c) another failure path that is not only reasonably probable, but could go undetected. The

evaluation process suggested the need for a reliable, independent verification of afterloader placement, to reduce the probability of this failure path.

The analysis process was also beneficial because it clearly showed the sequence of events and how the performance shaping factors at the facility affected the outcome. Also, it give a reasonable estimate of risk reduction after postulating changes to the facilities process.

Lack of a specific human reliability data base that addresses human errors for medical procedures and specific hardware failure rates for medical equipment lead to the methodology producing less than ideal results.

## FUTURE DIRECTION

From these results it has been decided to retain elements of the risk assessment methodologies tried to date, plus orient the data analysis to more of a human factors approach. For example, a process model and event trees will be developed for the events investigated.

The investigation itself will be oriented more towards a human factors approach since the events investigated to date have primarily involved human error. This entails collecting more information about the human factors aspects of the process including:

- Communications
- Training
- Human-machine interface
- Organizational culture.

Also, the possibility of maintaining a data base of all medical procedures using nuclear by-product materials and how many of those result in misadministration in order to get a better understanding of the true risk for misadministrations will be explored.

## CONCLUSIONS

Applying risk assessment methodologies to misadministration events has proven useful because it shows how the system can fail and how changes to the system can help prevent misadministrations.

The risk assessment methodologies tried to date have not provided all the information desired. Therefore, a hybrid risk assessment approach is going to be applied to data collected during future misadministration events.

## REFERENCES

1. L.T. Ostrom, T.J. Leahy and S.D. Novack, "Summary of 1991 and 1992 Misadministration Events," EG&G-2707, NUREG/CR-6088 (1993).
2. D. Meister, "Behavioral Analysis and Measurement Methods," John Wiley and Sons, New York, (1985).
3. A.D. Swain and H.E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, (1983).
4. G.W. Hannaman and A.J. Spurgin, "Systematic Human Action Reliability Procedure (SHARP)." EPRI NP-3583, Palo Alto, CA, (1984).
5. A.D. Swain, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, SAND86-1996, (1987).



6. D.I. Gertman, W.F. Gilmore, W.J. Galyeon, M.R. Groh, C.D. Gentillon, B.G. Gilbert, and W.J. Reece, "Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)." NUREG/CR-4639, EG&G-2458, Vpl. 1, Rev. 1, (1990).
7. K. Russell, et al., "Integrated Reliability and Risk Analysis System (IRRAS)," Version 4.0, NUREG/CR-5813, January (1992).

## **CONSTRUCTION ERROR AND HUMAN RELIABILITY FOR STRUCTURAL SYSTEMS**

Mark G. Stewart

Department of Civil Engineering and Surveying  
The University of Newcastle  
Newcastle, NSW, 2308, Australia

### **INTRODUCTION**

Buildings, bridges, offshore platforms and other structures consist of interconnected beams, columns, walls and other structural elements to form a structural system. Recent statistical reviews have found that construction errors are a dominant cause of structural failures. For example, Eldukair and Ayyub (1991) have estimated that 77% of structural failures are attributed to errors committed by contractors (i.e., poor workmanship by sub-contractors, site staff, foreman and workmen). The principal modes of structural system failure are structural collapse and serviceability problems (e.g., excessive cracking).

The safety of nuclear power and chemical process plants, and other potentially hazardous processes are also influenced by the performance of their structural systems. For example, premature failure of a nuclear power plant containment structure during a degraded core accident (e.g., LOCA) may have catastrophic consequences.

Structural systems are generally continuous event systems; therefore, system failure occurs when loads exceed the resistance. The structural resistance (or strength) may be a beam, column, roof or connection capacity. Loads may comprise of flood, earthquake, snow, wind, dead, and roof or floor live loads. In addition, built facilities for hazardous processes may be subject to accidental loads caused by the latent release of energy (e.g., explosion, overpressure). Estimates of system risk used in structural engineering are currently computed from probabilistic models that tend to exclude the influence of human error. Hence, these estimates of risk are not realistic. For example, these models only include the influence of small variations in material properties and element dimensions. However, it has been observed that estimates of risk obtained from these models seem to be several orders of magnitude lower than those based on statistical surveys of structural failures [e.g., Melchers, 1987]. It therefore follows that design, construction and other errors accounts for this discrepancy. Note that human errors are not all detrimental to system safety; some errors actually increase system reliability.

In the present paper a HRA has been developed to simulate the effect of human error in construction tasks. Consequently, the HRA may provide some understanding of the

influence of construction error and of various error amelioration/control measures on the probability of structural failure. This method utilises event-tree logic where the event-tree is analysed using Monte-Carlo simulation techniques. It is assumed herein that construction errors are those attributed to errors committed by contractors. Unfortunately, there is currently very little human reliability data (i.e., error rates, error magnitudes, and error detection) available for construction tasks. Such data is required for input into a HRA. However, some data has been collected for reinforced concrete construction tasks. Using this data, a HRA has been conducted for the construction of a simple reinforced concrete beam. A description of the data and results of the HRA are presented herein. The proposed HRA method may be applied also to the reliability of existing nuclear power plant structures, this application is also discussed.

Note that the proposed HRA model may be used to estimate the average system risk for (i) "generic" structures (i.e., for a large number of buildings) that includes variations in performance both within and between sites, and (ii) specific building sites. Finally, The HRA methodology proposed herein has been used also to simulate the effect of design error on structural design tasks [e.g., Stewart and Melchers, 1989; Stewart, 1990].

## CONSTRUCTION ERROR

Construction error is defined herein as an outcome that exceeds a construction tolerance as specified by an appropriate code of practice (e.g., depth of beam must be within 5mm of the specified depth). Construction errors are most likely to be caused by slips, mistakes and violations; most of these errors will also be latent. For the present paper it is assumed that construction errors most likely will influence the resistance of structural elements (e.g., undersized beam). Thus, construction errors may either reduce ("detrimental errors") or increase ("conservative errors") the structural resistance.

Brown and Yin (1988) suggest that construction errors committed by contractor are dominated by ignorance, thoughtlessness, and negligence. Such an observation is not unreasonable since construction workers are generally unskilled or semi-skilled, work in unpleasant conditions, have poor motivation, and are often unaware of the consequences of their actions. These are all factors that contribute to poor task performance, and suggests that construction errors are to be expected. For this reason, engineering inspections, supervision and other quality control measures are recognised as important components in the construction process. However, Eldukair and Ayyub (1991) have observed that lack of supervision and control was a factor contributing to 37% of structural failures.

## SYSTEM RISK FOR STRUCTURAL SYSTEMS

### Computation of System Risk

The probability of failure of a structural system may be referred to as a "system risk". The computation of system risk for a structural system requires that probability distributions for loads and structural resistances of each structural element are known. The computation of resistance distributions is of most interest because resistances are most likely to be influenced by construction error.

The resistance or strength of each constructed element is calculated from a predictive model ( $R_{pred}$ ); the model is generally an existing theoretical (or empirical) formulation. The parameters in most predictive models for resistance relate to material and dimensional variables. For example, the actual resistance (bending capacity against collapse) of a reinforced concrete beam is

$$R = ME \times R_{pred} = ME \times A_{st} f_y d \left( 1 - \frac{0.6 A_{st} f_y}{B d f_c} \right) \quad (1)$$

where  $A_{st}$  is the cross-sectional area of reinforcing steel,  $f_y$  is the yield strength of reinforcing steel,  $d$  is the depth to steel reinforcing,  $B$  is the beam width,  $f_c$  is the concrete compressive strength, and  $ME$  is the "modelling error" (see Table 1).

Probabilistic models are needed to describe the variability of these variables. Monte-Carlo computer simulation may then be used to develop a probability distribution of resistance by generating values of the variables from appropriate probabilistic models. It is generally assumed that the material and dimensional variables are independent. However, in practice some variables may well be correlated. For example, it is likely that variability in reinforcement placement and cross-sectional dimensions will all be higher for construction sites with poor supervisory control.

It is important to note that most existing statistical parameters for dimensional and material variables are obtained from direct field measurements made from only a limited number of building sites. It is therefore statistically unlikely that these limited samples would include within them any gross construction errors (i.e., large deviation from construction tolerances). Further, it is unlikely that a single probability distribution can accurately model the occurrence of very low probability/high consequence events (i.e., gross errors). Hence, most probabilistic models of actual resistances currently in use ignore the influence of gross construction errors.

### HRA of Structural Resistance

The HRA method used herein is based on THERP (Technique for Human Error Rate Prediction). The THERP method uses an event-tree logic system to divide a complex system into a number of successive individual microtasks. Each microtask models a human action needed in the sequence of producing a final outcome. It is likely that values of the dimensional and material variables in the finished product is influenced by human actions (e.g., workmanship). It is possible to represent each of these variables as a microtask.

**Human Reliability Data.** The HRA method requires human reliability data (i.e., measures of performance) for each microtask that is prone to construction error; namely:

- (i) error rates: Frequency of error occurrence or Human Error Probability (HEP).  
HEP = number of errors ÷ total number of opportunities for error
- (ii) error magnitude: If an error occurs, the error magnitude ( $m_e$ ) is the direct consequence or outcome of the error.

$$m_e = \frac{\text{outcome} - \text{correct outcome}}{\text{correct outcome}} \times 100\% \quad (2)$$

- (iii) error recovery: The rate of detection and correction of errors (e.g., checking efficiency of inspections).

This data may be obtained for errors of commission and errors of omission that are caused by slips, lapses and violations. It is assumed herein that error rates for individuals (for a specific task) will vary from individual to individual and that this variation in error rates is represented by the lognormal distribution. The mean error rate is usually available from human reliability data (i.e., HEP). A convenient measure of dispersion (i.e., variance) is represented by the "error factor" (EF), see Swain and Guttman (1983) for further details.

In the present case, the distribution of error magnitudes may be modelled by a probability distribution (say lognormal) if the median and some upper bound (say 90<sup>th</sup> percentile) are known. The distribution of error magnitudes can then be converted to a distribution of outcomes by the use of Eqn. (2), if the correct outcome is known. It may then be necessary to truncate the proposed distribution of outcomes at the maximum or minimum allowable construction tolerance, see Figure 1. Error rate, error magnitude and outcome probability distributions are referred to herein as "human performance models". These models may be obtained for "conservative" and "detrimental" errors for each microtask. Note that these human performance models may be influenced by worker experience, inspections, and other performance shaping factors.

**HRA Method.** The main computational tools used in THERP are event-tree logic and Monte-Carlo simulation. The event-tree starts at a convenient point and works forward in time. For each microtask a decision (e.g., "error-free", "conservative error" or "detrimental error") and also the consequences of the decision (i.e., outcome) are made. Error rates for detrimental and conservative errors (HEP1, HEP2) are randomly generated from their respective probability distributions. A uniform random variable [0,1] is then generated (RN). A detrimental error occurs if  $RN < HEP1$  or a conservative error occurs if  $RN < HEP1 + HEP2$ , otherwise the task is "error-free". An outcome is then randomly generated from the appropriate distribution of outcomes. The process is then repeated for subsequent microtasks (i.e., for all material and dimensional variables), an estimate of structural resistance (R) can then be calculated from the predictive model. The entire process is then repeated many times (i.e., Monte-Carlo simulation), a probability distribution of actual resistances can then be inferred. The probability of failure can then be calculated from existing methods [e.g., Melchers, 1987]. However, results obtained from a HRA can provide only an indication of the true nature of the influence of human error on system risk because human behaviour is a complex phenomenon that is difficult to quantify. For this reason, system risks obtained from a HRA are particularly useful for comparative studies; for example, to compare the effectiveness of error amelioration/control measures or other performance shaping functions. See Stewart (1993) for a more detailed description of the above HRA method.

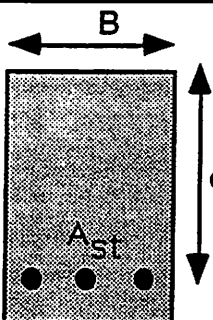
Finally, the HRA method described herein may be applied to a range of other continuous event systems; namely, dams, embankments, foundations, tunnels, and other geotechnical and hydraulic systems.

## APPLICATIONS

### Reinforced Concrete Beam Construction

A preliminary study has been conducted to develop human performance models for the construction of typical reinforced concrete beams and to incorporate this information into a HRA [Stewart, 1992]. The four construction microtasks prone to construction error are given in Table 1. Expert judgements from practising engineers were used to obtain single point estimates for the average error rate for errors committed prior to engineering inspections ( $\bar{m}_0$ ), the checking efficiency of inspections ( $\bar{p}_i$ ), and the average and worst error magnitudes ( $\lambda_{BE}$  and  $\lambda_{UB}$  respectively), for each microtask. The average error rate for errors not detected by inspections and thus included in the finished work is  $\bar{m}_i = \bar{m}_0(1 - \bar{p}_i)$ , see Table 1. Figure 1 shows the distribution of outcomes for microtask E1, for a beam with a specified effective depth of 800mm.

Table 1. Parameters for Human Performance Models ( $\bar{p}_i=0.997$ )

	Microtask	Error Rates		Error Magnitudes	
		$\bar{m}_i$	$EF_i$	$\lambda_{BE}$	$\lambda_{UB}$
	E1 Area of Tensile Steel ( $A_{st}$ ):				
	Detrimental Error	0.00037	10	-14.3	-82.2
	Conservative Error	0.00020	10	15.2	69.2
	E2 Depth to Tensile Steel ( $d$ ):				
	Detrimental Error	0.00051	10	-7.1	-21.1
	Conservative Error	0.00032	10	6.3	16.6
	E3 Beam Width ( $B$ ):				
	Detrimental Error	0.00014	10	-5.2	-14.5
	Conservative Error	0.00014	10	5.2	16.5
	E4 Concrete Mix ( $f_c$ ):				
	Detrimental Error	0.00490	3	-9.6	-38.0

A HRA was conducted using the above human performance models, for a reinforced concrete beam supporting a typical floor and spanning 10m. The structural resistance of the beam is given by Eqn. (1). Figure 2 shows the lower and upper tails of the distribution of structural resistances ( $R$ ) for "error-free" (all microtask error rates equated to zero) and "error-included" construction processes. The lower tail of a resistance distribution has a major influence on the calculated probability of failure. The resulting mean probabilities of failure were  $0.54 \times 10^{-4}$  and  $0.52 \times 10^{-3}$  for "error-free" and "error-included" construction processes respectively. Thus, construction error causes a relative loss of structural safety of approximately an order of magnitude. However, the "error-included" probability of failure may approach the "error-free" value if the efficiency of engineering inspections is further improved or if other error amelioration/control measures are adopted. It is important to recognise that some structures will have probabilities of failure above or below the "mean" probability of failure as a result of variations of workmanship between sites.

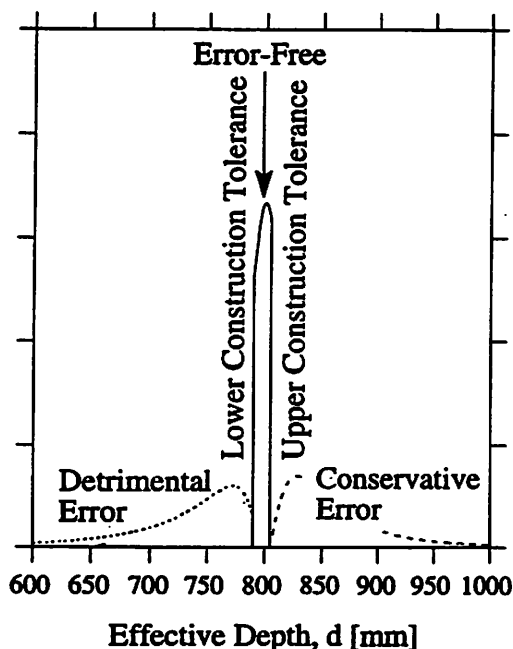


Figure 1.  
Distribution of Outcomes for Error Type E1

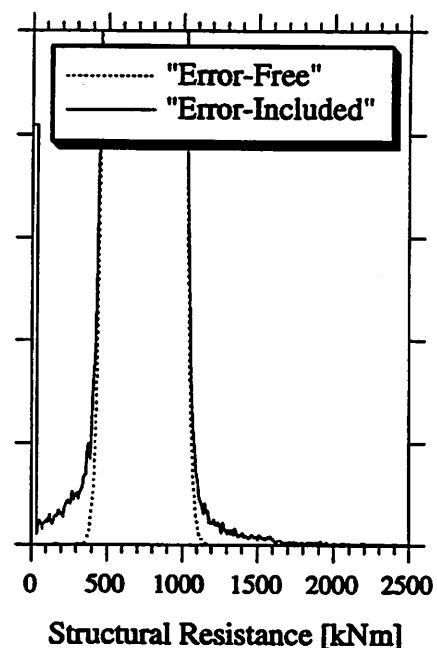


Figure 2.  
Distribution of Structural Resistances as  
Obtained From Monte-Carlo Simulation

## Nuclear Power Plant Structures

It is likely that design and construction errors exist also in nuclear power plant structures such as control room buildings and containment structures [Ravindra, 1986]. The performance of these structures during abnormal loading events such as a LOCA (overpressure) or earthquake (ground acceleration) may significantly influence the reliability of equipment and systems contained within the structure.

Ravindra (1986) reports that the influence of design and construction errors are generally ignored from PRA's. For example, seismic fragility curves are used in a PRA to represent the failure rates of structures, components or systems given the occurrence of a specific peak ground acceleration; these curves are currently developed on the assumption that the design and construction processes are "error-free". However, it is likely that the HRA method proposed herein may be used to assess the influence of construction errors (e.g., incorrect placement of reinforcement) on the peak ground acceleration capacity (i.e., resistance) of a structure. Human reliability data may be obtained from expert opinions in a manner similar to that obtained for reinforced concrete construction tasks.

It should be noted that the "error-free" probabilities of failure for some structures may be quite low; for example, Hwang, et.al. (1987) have suggested that proposed containment structures should have a conditional structural failure probability (given the occurrence of a large pressure due to a LOCA) of  $10^{-6}$  to  $10^{-4}$ . It has been shown by Stewart (1990) that the proportional loss of structural safety due to human error is greater for structural members with very low "error-free" probabilities of failure. Thus, the inclusion of human error into the computation of failure probabilities may significantly increase some existing "error-free" failure probabilities. However, it is unclear if the overall system risk (e.g., risk of core damage) will be sensitive to these increases in structural failure probabilities.

## CONCLUSION

A Human Reliability Analysis (HRA) model has been developed to simulate the effect of construction error on structural reliability. A HRA was conducted for the construction of a simple reinforced concrete beam. The application of the HRA method to the structural reliability of nuclear power plant structures was also discussed.

## REFERENCES

- Brown, C.B. and Yin, X., 1988, Errors in Structural Engineering, *Journal of Structural Engineering*, ASCE, 114(4), 2575-2593.
- Eldukair, Z.A. and Ayyub, B.M., 1991, Analysis of Recent U.S. Structural and Construction Failures, *Journal of Performance of Constructed Facilities*, ASCE, 5(1), 57-73.
- Hwang, H., Ellingwood, B. and Shinozuka, M., 1987, Probability-Based Design Criteria for Nuclear Power Plant Structures, *Journal of Structural Engineering*, ASCE, 113(5), 925-942.
- Melchers, R.E., 1987, "Structural Reliability: Analysis and Prediction", Ellis Horwood, Chichester, England.
- Ravindra, M.K., 1986, Gross Errors, Seismic Margins and Seismic PRA's, in: "Modeling Human Error in Structural Design and Construction", A.S. Nowak (Ed.), ASCE, New York, 113-121.
- Stewart, M.G. and Melchers, R.E., 1989, Error Control in Member Design, *Structural Safety*, 6(1), 11-24.
- Stewart, M.G., 1990, Human Error in Steel Beam Design, *Civil Engineering Systems*, 7(2), 94-101.
- Stewart, M.G., 1992, A Human Reliability Analysis of Reinforced Concrete Beam Construction, *Civil Engineering Systems*, 9(3), 227-247.
- Stewart, M.G., 1993, Human Error and Human Reliability for Building Construction Tasks, in: "Probabilistic Risk and Hazard Assessment", R.E. Melchers and M.G. Stewart (Eds.), A.A. Balkema, Netherlands, 195-205.
- Swain, A.D. and Guttman, H.E., 1983, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, US Nuclear Regulatory Commission, Washington, D.C.

## THE FEASIBILITY OF DESIGNING HUMAN-ERROR BACKUP SYSTEMS FOR FAIL-SAFE STRUCTURES

Yoshinobu Sato<sup>1</sup> and Koichi Inoue<sup>2</sup>

<sup>1</sup>Dept. of Electronic and Mechanical Eng.    <sup>2</sup>Dept. of Aeronautical Eng.  
Tokyo University of Mercantile Marine    Kyoto University  
2-1-6 Etchujima, Koto-Ku, Tokyo 135    Sakyo-Ku, Kyoto 606

### INTRODUCTION

As the reliability of the hardware of production systems, vehicles, etc., has enhanced rapidly, human-error is becoming the main initial cause of injurious accidents. In order to curb the accidents resulting from human error, not only should there be improvement of human reliability but also human-error backup systems (HEBS: the system which prevents damage, given that human-errors have occurred) should be utilized for man-machine systems. For instance, ASVs (Advanced Safety Vehicles) are supposed to be equipped with automated human-error backup mechanisms to avert car collisions. However, if a fault of such mechanisms brings about an accident, the makers can be sued. Thus, the HEBS should be so structured as not to cause damage even when faults arise in itself. Only the well-developed HEBS will be able to meet this safety requirement.

Since a fail-safe system prevents damage by transferring a system from an ordered state to a disordered state (viz., the system transition relies on the laws of nature rather than human intervention), we prefer designing HEBSs for the fail-safe structures. However, the fail-safe structure is not always possible. It depends on the types of hazards produced in the man-machine system and on other system conditions. This complicates the problem of structuring fail-safe systems, and therefore we need to approach it systematically. An HCS (hazard-control system: the system which prevents damage, given that undesirable changes have occurred) involves (inherently) fail-safe and fail-operable system structures. HCSs have been categorized and systematized in terms of an action-change and action-chain (A-C) model<sup>1</sup>. This paper explores the feasibility of designing HEBSs for (inherently) fail-safe structures based on the A-C model.

### Acronyms

A-C    action-change and action-chain

ASV    advanced safety vehicle



**HCS** hazard-control system**HEBS** human-error backup system**Notation**

$X u_{i m} \rightarrow W$  action  $u_i$  ( $i \in 1, 2, \dots, 6$ ;  $u_1=a, u_2=b, u_3=c, u_4=d, u_5=e, u_6=f$ ) is transmitted from element  $X$  to  $W$ .

$Y u_{j' n} \rightarrow X$  dissociation action  $u_{j'}$  ( $j' \in 1, 2, \dots, 6$ ;  $u_1'=a', u_2'=b', u_3'=c', u_4'=d', u_5'=e', u_6'=f'$ ) is transmitted from element  $Y$  to  $X$ .

$(Y g'_{n+1} \rightarrow X) \& (Y g'_{n+1} \rightarrow Y g'_{n+1} \rightarrow W)$  dissociation action  $g' \& g''$  is transmitted from element  $Y$  to elements  $X$  and  $W$ .

$Y_1 u_k'' \rightarrow Y_2$  control action  $u_k''$  ( $k \in 1, 2, \dots, 6$ ;  $u_1''=a'', u_2''=b'', u_3''=c'', u_4''=d'', u_5''=e'', u_6''=f''$ ) is transmitted from element  $Y_1$  to  $Y_2$ .

$Y_1 \underline{u}_l \rightarrow Y_2$  reversal action  $\underline{u}_l$  ( $l \in 1, 2, \dots, 6$ ;  $\underline{u}_1=\underline{a}, \underline{u}_2=\underline{b}, \underline{u}_3=\underline{c}, \underline{u}_4=\underline{d}, \underline{u}_5=\underline{e}, \underline{u}_6=\underline{f}$ ) is transmitted from element  $Y_1$  to  $Y_2$ .

$P_r$

$X u_{i m} \rightarrow / W$  action link  $[u_{i m} \rightarrow]$  ( $i \in 1, 2, \dots, 5$ ) is dissociated by dissociation principle  $P_r$  ( $r \in 1, 2, 3$ ), i.e., the fail-safe dissociation principle.

$P_4$

$X f_m \rightarrow / W$  action link  $[f_m \rightarrow]$  is dissociated by dissociation principle  $P_4$ , i.e., the fail-operable dissociation principle.

$X u_{i 0} \rightarrow W(:)$  damage  $(:)$  arises in element  $W$  by direct causal action  $u_i$ .

$m, n, q$  concatenation order of linkage from a direct causal action link ( $m, n, q=1, 2, 3, \dots$ )

$(x), (y), (z) \dots$  element changes (usually omitted.)

$H$  human system-element     $M$  machine system-element     $M'$  subsystem of  $M$

$B$  human-error backup system-element     $BI$  information processing subsystem of  $B$

$O$  damaged system-element     $C$  systems condition

**Definitions**

**hazard** A situation with a potential for harm in terms of human injury, damage, etc.

**hazard identification** The process of recognizing and defining a hazard's characteristics.

**HCS** A system which prevents damage, given that undesirable changes have occurred.

**HEBS** A system which prevents damage, given that human-errors have occurred.

**Fail-safe system**

In general, we can identify many hazards especially for a complex system. Hazards can be classified into two categories in accordance with these characteristics: hazards which are manifest with undesirable changes when the relationship between any two system elements is in an ordered (relatively small entropy) state; and hazards appearing in a disordered state. Then the relationships among the former and the latter-type hazards, the state of the elements, and hazard control result in the following:

1. We can prevent the former-type hazards from materializing by: (1) controlling and holding the relationship between system elements if it has already been in a disordered state; (2) controlling and transferring it from an ordered state to a disordered one if it is in an ordered state.

2. The latter-type hazards can be prevented from materializing by: (3) controlling and holding the relationship between system elements if it is in an ordered state; (4) controlling and transferring it from a disordered state to an ordered one if it is in a disordered state.

In the cases (1) and (2), a disordered state averts damage in the result although it is not clear if the whole hazard-control process consists of disordered states only; and an ordered state does in the cases (3) and (4). Hence we give the following definitions to the system: the system is a fail-safe system regarding the specified hazards and undesirable changes for cases (1) and (2); and a fail-operable system for cases (3) and (4).

A fail-safe system that controls a hazard rather along the natural course of events than by human intervention must be distinguished from a fail-operable system. If the whole process of controlling a hazard consists of disordered states only, we can define the system as an inherently fail-safe system regarding the specified hazard and undesirable changes.

## HAZARD IDENTIFICATION

The hazard that is initiated by a human-error and brings about damage into system element  $O$  is identified by the following action chain:

$$H(h)u_{i_1} \rightarrow M(m)u_{j_0} \rightarrow O(:) \quad (1)$$

$i, j \in 1, 2, \dots, 6$

$H, M, O$  system elements (see notation)     $u_{i_1} \rightarrow, u_{j_0} \rightarrow$  action links (see notation)  
 $(h)$  a human-error arises in  $H$ .     $(m)$  changes occur in  $M$ .     $(:)$   $O$  is damaged.

We define the hazard as Hazard (1). Accident scenarios corresponding to the hazard are:  
**Example 1.** When a driver has stepped on the brakes hard [ $H(h)a_1 \rightarrow$ ], the car goes into a skid because of locking the brake [ $M(m)$ ] and skids into an object [ $a_0 \rightarrow$ ], and damage arises in the object [ $O(:)$ ].

**Example 2.** Since a personnel did not open a main safety valve after his maintenance of a reactor [ $H(h)f_1 \rightarrow$ ], the reactor explodes due to excess pressure [ $M(m)$ ] and releases poison [ $c_0 \rightarrow$ ], and the surroundings are damaged [ $O(:)$ ].

## STRUCTURING "HEBS"

We can rewrite action chain (1) using a subsystem of  $M$ :

$$H(h)u_{i_2} \rightarrow M'(m')u_{k_1} \rightarrow M(m)u_{j_0} \rightarrow O(:) \quad (2)$$

$i, j, k \in 1, 2, \dots, 6$

System element  $B$ , i.e., an HEBS composes the following control chain and dissociates the action link [ $u_{k_1} \rightarrow$ ] in order to avert damage (see Appendix):

For  $k \in 1, 2, \dots, 5$

$$C(c)u_{l_3} \xrightarrow{P_r} B u_{m_2} \rightarrow M' u_{k_1} \rightarrow M \quad (3)$$

$r \in 1, 2, 3 \quad l, m \in 1, 2, \dots, 6$

For  $k = 6$  (i.e.,  $u_k = f$ )

$$C(c)u_l^n \xrightarrow{P_4} Bg'_{.2} \rightarrow \{(M'f_l \rightarrow M) \& (Bg^n_{.1} \rightarrow M)\} \quad (4)$$

$l \in 1, 2, \dots, 6$

Here, the system is a fail-safe system regarding Hazard (1) and human-error ( $h$ ) for control chain (3), and a fail-operable one for control chain (4).

Examples of HEBS corresponding to the control chains are:

1. an antilock-braking system for automobiles
2. a reactor interlocking system (which detects the blocking of a safety valve and locks up the reactor operation.)

These HEBSs may be able to compose both control chains.

We can induce the following rule from discussions above:

**Rule 1.** A necessary condition for structuring an HEBS as a fail-safe system is that the machine controlled by the HEBS generates one or more ordered-state actions.

If a fault ( $x$ ) arises in the information processing subsystem of HEBS, the control chain is reversed and dissociation cannot occur. For example, for control chain (3):

$$C(c)u_l^n \xrightarrow{P_4} BI(x)u_n \xrightarrow{P_4} B(y)u_p \xrightarrow{P_4} M'(m')u_k \xrightarrow{P_4} M(m)u_j \xrightarrow{P_4} O(:) \quad (5)$$

$n \in 2, 6 \quad k \in 1, 2, \dots, 5 \quad j, l, p \in 1, 2, \dots, 6$

We define the hazard identified by reversal chain (5) as Hazard (2). If the control (dissociation) actions in control chains (3) and (4) are ordered-state control (dissociation) actions and they are reversed, the disordered-state reversal action  $f$  results. Similarly, the reversal of disordered-state control (dissociation) actions result in ordered-state reversal actions (see *Appendix, Theorem 3*). Since the characteristics of reversal actions are the same as the actions in action chains, the action-link dissociation principles apply. Then the reversal link  $[u_n \rightarrow]$  in the reversal chain (5) is dissociated in the following manner and the original action link is dissociated again (*Theorems 5 and 6*):

For  $n=6$

$$C(c)u_l^n \xrightarrow{P_4} BI'g'_{.4} \rightarrow \{(BI(x)f_{.3} \rightarrow B) \& (BI'g^n_{.3} \rightarrow Bu_m'_{.2} \rightarrow M'u_k \rightarrow M)\} \quad (6)$$

$k \in 1, 2, \dots, 5 \quad l, m \in 1, 2, \dots, 6 \quad r \in 1, 2, 3$

$BI'$  redundancy of  $BI$

Here the system is a fail-safe system regarding Hazard (1) and human-error ( $h$ ), and a fail-operable system regarding Hazard (2) and change ( $x$ ).

For  $n=2$

$$FSe'_{.4} \xrightarrow{P_s} BI(x')b_{.3} \rightarrow Bu_m'_{.2} \xrightarrow{P_r} M'u_k \rightarrow M \quad (7)$$

$k \in 1, 2, \dots, 5 \quad m \in 1, 2, \dots, 6 \quad r, s \in 1, 2, 3$

# FS fail-safe mechanism of BI

Here the system is a fail-safe system regarding Hazards (1) and (2), human-error ( $h$ ), and change ( $x'$ ). The structure of HEBS induces the following rule:

**Rule 2.** The necessary condition for designing the information-processing subsystem of HEBS for a fail-safe system regarding its internal faults is that the subsystem is so structured to evoke disordered-state control actions to avert accidents caused by human-error.

An HEBS controls and transfers the state of system elements from a dangerous state to a safer one. We can classify the transition into two categories. One is the ordered-process-type transition, another is the disordered-process one. A typical example of the former is the transition of kinetic energy of an airplane landing safely on a runway under variable winds. The transition of a safety valve from a closing to an opening state is a latter case. Since an HEBS must generate ordered-state control actions in order to materialize ordered-state transition (*Theorems 7 and 8*), the following rule is concluded:

**Rule 3.** The necessary condition for structuring an information-processing subsystem of HEBS for a fail-safe system regarding its internal faults is that HEBS implements disordered-state transition.

Table 1 demonstrates the feasibility of designing HEBSs for fail-safe structures by examples of ASV<sup>2</sup>. Here, an IPS (Information Processing System of ASV) sensing a driver's error, such as looking aside or dozing, automatically brakes in order to avert a car crash.

Each hazard is defined as follows:

**Hazard 1.** regarding human-error and a collision; disregarding a skid

**Hazard 2.** regarding a skid, faults of HEBS for the skid only, and a collision

**Hazard 3.** regarding human-error, faults of HEBS, and a collision; disregarding a skid

**Hazard 4.** regarding human-error, a skid, faults of HEBS for both skid and human-error, and a collision

## CONCLUSIONS

We first define an (inherently) fail-safe and fail-operable system systematically based on an A-C model. Next, systematic methods for studying the feasibility of designing human-

**Table 1.** Feasibility of designing ASV for fail-safe structures

System elements	Hazard 1	Hazard 2	Hazard 3	Hazard 4
Driver	○	○	/	/
Power-source of ASV	○	□	○	□
External sensor subsystem of IPS	/	/	○	○
Internal sensor subsystem of IPS	/	□	/	□
Processor subsystem of IPS	/	□	○	△
Actuator subsystem of IPS	/	□	○	□
Brake-mechanism	△	□	△	□

○ Fail-safe structure is feasible for the whole element regarding the hazard.      △ Fail-safe structure is partially feasible for the element regarding the hazard.      □ Fail-safe structure is not feasible for the element regarding the hazard.

error backup systems for fail-safe structures are proposed. Examples involving information processing systems of ASV demonstrate the new technology.

## REFERENCES

1. Y. Sato, E. J. Henley, and K. Inoue, An action-chain model for the design of hazard-control systems for robots, *IEEE Trans. Reliability* 39:2(1990).
2. Y. Sato, The structure of hazard-control systems for advanced safety vehicles, *Proceedings of Japan-USA Symposium on Flexible Automation*, San Francisco (1992).

## APPENDIX

**Remark 1.** Any damage (and its control process) is modeled by the system-element's changes and propagation of actions (and dissociation, control and reversal actions) among system elements. The changes include not only continuous variables such as voltage or temperature but changes in shape, size, information content, etc. When the state of system elements is in an ordered condition, i.e., having relatively small entropy, ordered-state actions are generated because of energy transfer (kinetic, thermal, etc.), substance transfer, obstruction of necessary supplies, and attributes of shape, force, mass, etc. When the state of system elements is in a disordered condition, disordered-state actions are produced because of the failure of an element to function.

**Remark 2.** Actions (and dissociation, control, and reversal actions) are categorized into: 1. ordered-state actions: a) energy transmission, b) information propagation, c) agent transfer, d) supply obstruction, e) existence form, and g'&g") function substitution; and 2. disordered-state actions: f) function failure (cessation).

**Remark 3.** Dissociations of (reversal) action links are categorized by the following principles: 1. fail-safe dissociation principles: P1 control of an action source, P2 control of an action path, P3 control of an action source and path; and 2. fail-operable dissociation principle: P4 control by substitution for a failed function.

**Theorem 1.** Ordered-state action links are dissociated by the fail-safe dissociation principles, and disordered-state action links are dissociated by the fail-operable dissociation principle only.

**Theorem 2.** Fail-safe dissociation principles are achieved with dissociation actions of types a', b', c', d', e', and/or f', while P4 is achieved with type g'&g" only.

**Theorem 3.** If an ordered-state dissociation (control) action is reversed, a disordered-state reversal action results, while if an f' or f"-type action is reversed, one or more ordered-state reversal actions arise.

**Theorem 4.** If a change occurs in X, and a control action from X is reversed, reversal chains result from X and dissociation can not occur.

**Theorem 5.** Ordered-state reversal action links are dissociated by the fail-safe dissociation principles, while disordered-state reversal action links are dissociated by the fail-operable dissociation principle only.

**Theorem 6.** If a reversal action link is dissociated, the partial control chain is restored and the original action link is dissociated again, provided no other reversal chains exist in the HCS.

**Theorem 7.** A necessary condition for an f' or f"-type link is a single-direction action link.

**Theorem 8.** Suppose there exists an external dual-direction action link L1 whose control depends on a dual-direction action link L2. Then there must be one or more control chains connecting L1 and L2 with dual-direction action links in HCS.

## **A METHODOLOGY TO SUPPORT SPACE SYSTEM DESIGNERS IN MINIMIZING HUMAN ERROR**

*Mario FERRANTE<sup>1</sup>, Claudia VIVALDA<sup>1</sup>, Carla FOGLI<sup>2</sup>*

<sup>1</sup>Alenia Spazio S.p.A. - P.A. Dept.  
Corso Marche 41  
10146 Turin, Italy

<sup>2</sup>ESA/ESTEC - P.A. & Safety Dept.  
P.O.Box 299,  
2200 AG Noordwijk, The Netherlands

### **INTRODUCTION**

The paper proposes a methodological approach to support space system analysts in deriving recommendations for designers. The recommendations aim at avoiding or minimizing human errors arising during, or leading to, hazardous situations or mission degradation.

The methodology represents a way to extend the hazard analysis and the FMECA (Failure Mode Effect and Criticality Analysis) to a more detailed analysis of human errors. Its basis is a **Paradigm for human error minimization**, which provides the RAMS (Reliability, Availability, Maintainability, Safety) and HF (Human Factor) analysts with a set of high level guidelines, called **Archetype guidelines**, to be tailored to specific situations for recommendation identification.

In the following sections a description of the theoretical background upon which the paradigm and the archetype guidelines are based together with the methodological approach are described in detail.

### **THEORETICAL BACKGROUND**

The theoretical research and the available information relevant to the human error occurrence, have identified general rules from which a *structure* for the definition of recommendations to reduce human error can be derived.

This *structure* or general law has been called **Paradigm for human error minimization** and forms the Key issue of the methodology described in this paper.

This Paradigm is based on two main concepts.

The first is the result of research activity conducted in the frame of human error occurrence in nuclear plants and other industries. Experimental results showed that if the time available to perform a task after an initiating event is brief (in the range of seconds to tens of minutes) it becomes the key contributor to the crew failure probability [1].

The second consists of the physical and present understanding of the mental process that considers the brain divided in two halves [2].

In one half pattern matching dominates and it is mainly involved in stimuli-response (S-R) tasks rather than problem solving tasks.

In the other half experience and training dominates and it is mainly involved in the cognitive process with major emphasis on problem solving tasks.

Using the results of the theoretical research in this field, a correlation between available time and brain function can be identified. In fact, when time is short, the stimuli-response process dominates, while in the presence of additional time, the human cognitive process takes precedence over the other one.

The combination of these two concepts leads to the conviction that mental process, time available to perform a task and human error probability [3] are strictly linked. The rules for paradigm development have been inferred by the analysis of this link. In fact, the paradigm recognises that different human abilities are more reliable in different **time regimes** so that human performance tasks should be designed to take that into account. As a consequence, the Archetype guidelines have been developed to facilitate specific human performance.

### Time Regimes and Archetype Guidelines

The archetype guidelines, together with the time regimes are the basis of the paradigm for minimizing human error (Fig. 1).

The *time regime* is a time interval characterized by a specific brain involvement and human performance.

Four time regimes form the paradigm. They are described below, with the related archetype guidelines.

- **Excluded region.** The time available for human response is less than a few seconds and therefore human actions must be excluded (i.e., they must be either eliminated or automated) since the human response capability is very limited.
- **Short time regime.** Less than one minute is available to humans to perform the required task. Due to the short time available, thinking and decision making is difficult. It follows that the operator tasks must be of a *Stimulus-Response* nature and written procedures become irrelevant because the operator generally has no time to read or use them.

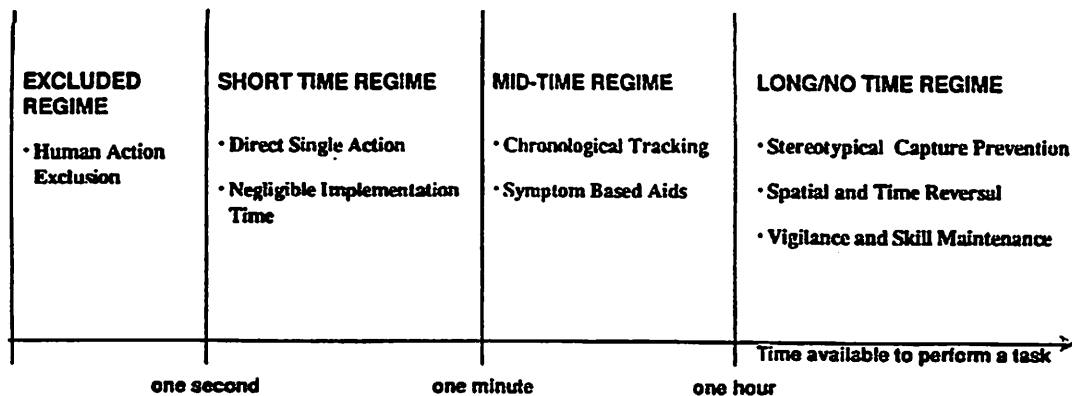


Figure 1 - Paradigm for human error minimization

- **Mid-Time regime.** Several minutes to one hour are available to humans to perform the required task. During this time regime, the operator can evaluate the situation, access some diagnostic tools, and take a decision on the best action to take, even if he is aware that there are limits to the amount of time available to take an action. If decision and diagnosis can be facilitated by flowcharts or effective training, then the likelihood of mistakes can be reduced so that the error probability is characterized by slips.
- **Long/No time dependent regime.** It primarily refers to tasks which are performed while the process or mission is proceeding in a normal fashion. In this regime, the time available presents little or no constraint on the actions that must be taken. Therefore, single slip errors are considered to be the dominant ones in the Long/No time dependent regime, and the guideline recommends that consideration be given to maintaining human vigilance.

The main archetypes guidelines are reported in Table 1.

These archetype guidelines are independent of specific technological systems or environments because they are based on general human behaviour when a man is called on to perform a task. To be effective, each archetype guideline has to be applied to a specific system operational scenario, to reduce or eliminate the well defined error to which it is directed.

**Table 1 - Archetype guidelines**

SHORT TIME REGIME	MID-TIME REGIME	LONG/NO TIME REGIME
<ul style="list-style-type: none"> <li>• <b>Direct Single Action:</b> any task assigned to the operator must be single, clear, unambiguous, whole from the perspective of both the triggering stimulus and the required response.</li> <li>• <b>Negligible Implementation Time:</b> for any task the time required for the response to be enacted and to take effect must either be negligible or must have been previously accounted for or subtracted from the time available.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Chronological Tracking:</b> for multiple tracking S-R tasks which must be perceived and/or performed individually and for diagnostic task, make maximum use of the time available by re-tracking the perceived time to the actual chronological time available.</li> <li>• <b>Symptom Based Aids:</b> for diagnostic tasks introduces symptom based procedures or other aids which effectively convert the diagnostic task into a limited set of S-R tasks.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Stereotypical Capture Prevention:</b> make task cues and response actions as different as possible so that defects in representation are less likely to lead to incorrect responses.</li> <li>• <b>Spatial and Time Reversal Prevention:</b> make the design such that reversal of the sequence of actions and the position perspective of either cue devices or response devices are irrelevant to task performance.</li> <li>• <b>Vigilance and Skill Maintenance:</b> high skill levels and high attention levels cannot be maintained over long period of time and therefore proper countermeasures and training procedures must be implemented.</li> </ul>

## METHODOLOGICAL APPROACH

In the early phases of a space Project, the task of the RAMS Engineering is to define the requirements applicable to the system Architecture in order to prevent or control hazardous or mission degradation situations.

In order to perform this activity systematically, two main analyses are developed: the Hazard Analysis and the FMECA (Failure Mode Effects and Criticality Analysis) [4].

Even if the above techniques follow different approaches (FMECA bottom up, Hazard Analysis top down), the RAMS Engineer identifies the *Failure modes* or the



*Hazard causes* (Hardware failures, software failures, human errors) at the end of the analysis process with the purpose of defining proper countermeasures.

To control the hardware or software failure, specific techniques have been developed (fault tolerant, inhibits etc.). The techniques applied until now to control human errors in the space domain were generally focused on excluding human actions or avoiding human error effects through inhibits but not on minimising human error probability. Only reference to the general application of Human Factor design guidelines or training program is usually made.

Therefore, Alenia Spazio proposes a methodology which provides a way of starting from an identified potential error and a scenario and arriving at a set of specific recommendations to the designer to reduce the likelihood of the error occurrence.

The application of the methodology requires the following inputs:

- the Safety/Operational Hazard Analyses or FMECA, from which it is possible to identify human errors as failure modes or hazard causes of a specific mission degradation or hazardous situation
- the paradigm for human error minimization
- the standards, requirements and guidelines already existing in the space and non-space domains, having the objective to prevent or reduce human errors or improve human performance [5], [6].

Once the human errors are identified from Hazard Analyses or FMECA, the applicable archetype guidelines are selected taking into account the time regimes applicable to the scenario under analysis.

The requirements or recommendations are generated by the tailoring of selected *archetypes* to the particular scenario that considers the Hardware and the Software involved and the dynamic situation in which the human error is generated (i.e. contingency conditions, nominal operations etc.).

In performing this tailoring the existing Human Factors Guidelines and Standards are also used. Typically, the HF guidelines are not linked to the RAMS Analysis but are tailored to a specific subsystem based on Hardware/Environment characteristics or Operational constraints.

With the present methodology the Human Factor Engineer selects from the existing Standards and Guidelines the recommendations more suitable to the *event* (hazardous or mission degradation condition) under analysis. In this way the methodology takes the analyst quickly to those guidelines which fit with the identified error-scenario combination.

As a consequence, instead of having a *Hardware/Environment* oriented approach an *Event* oriented approach is followed, that can be integrated easily with the typical RAMS Engineering methodology.

At the end of this process a set of recommendations resulting from the archetype applications and HF contribution and applicable to the architecture of the Space System under analysis are collected. The process followed to perform the proposed analysis method is shown in Fig. 2 (see following page).

In order to structure the analysis process, a format has been developed to collect all the necessary information and the requirements generated.

Fig. 3 (see following pages) shows the filled format and the application of the methodology to a typical hazardous situation in manned space system in which the *man* is one of cause of the hazard.

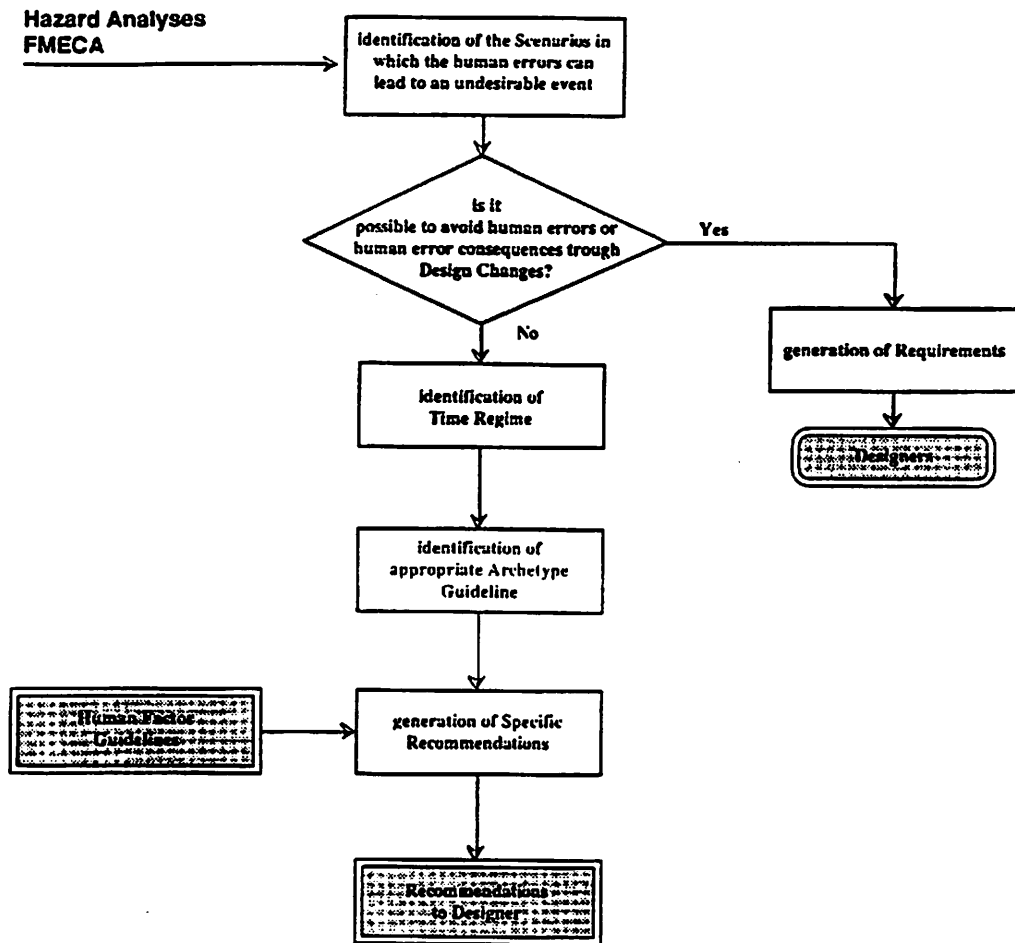


Figure 2 - Methodology flow

## CONCLUSIONS

This work is the result of a preliminary study and other future research activities, to cover the human errors systematically during the overall space project life cycle, are certainly necessary.

The methodology is based mainly on the time constraints issues (time regimes). Presently, considering the information available, it can be considered the more appropriate to reduce the human error in particular situations (hazards etc.) as described in the paper. The proposed approach represents an attempt to cover a missing brick in the overall RAMS activities relevant to the minimization of the human errors. This method can permit the identification of adequate preventions/controls from the early phases of a space project design, in which detailed operational procedures are not available and the trades to decide the involvement of the man in some control or monitoring function are usually performed.

Furthermore, the suggested way to proceed promotes an integration between the Human Factors and RAMS Engineering activities with the common objective to safeguard the crew safety and/or the mission of the Space System.

In following this approach, the human involvement in a predefined *contingent* situation can now be analyzed in an integrated fashion within the overall RAMS activity with the advantages that the analyst is not required to have an in-depth knowledge of psychology, error taxonomies, etc.

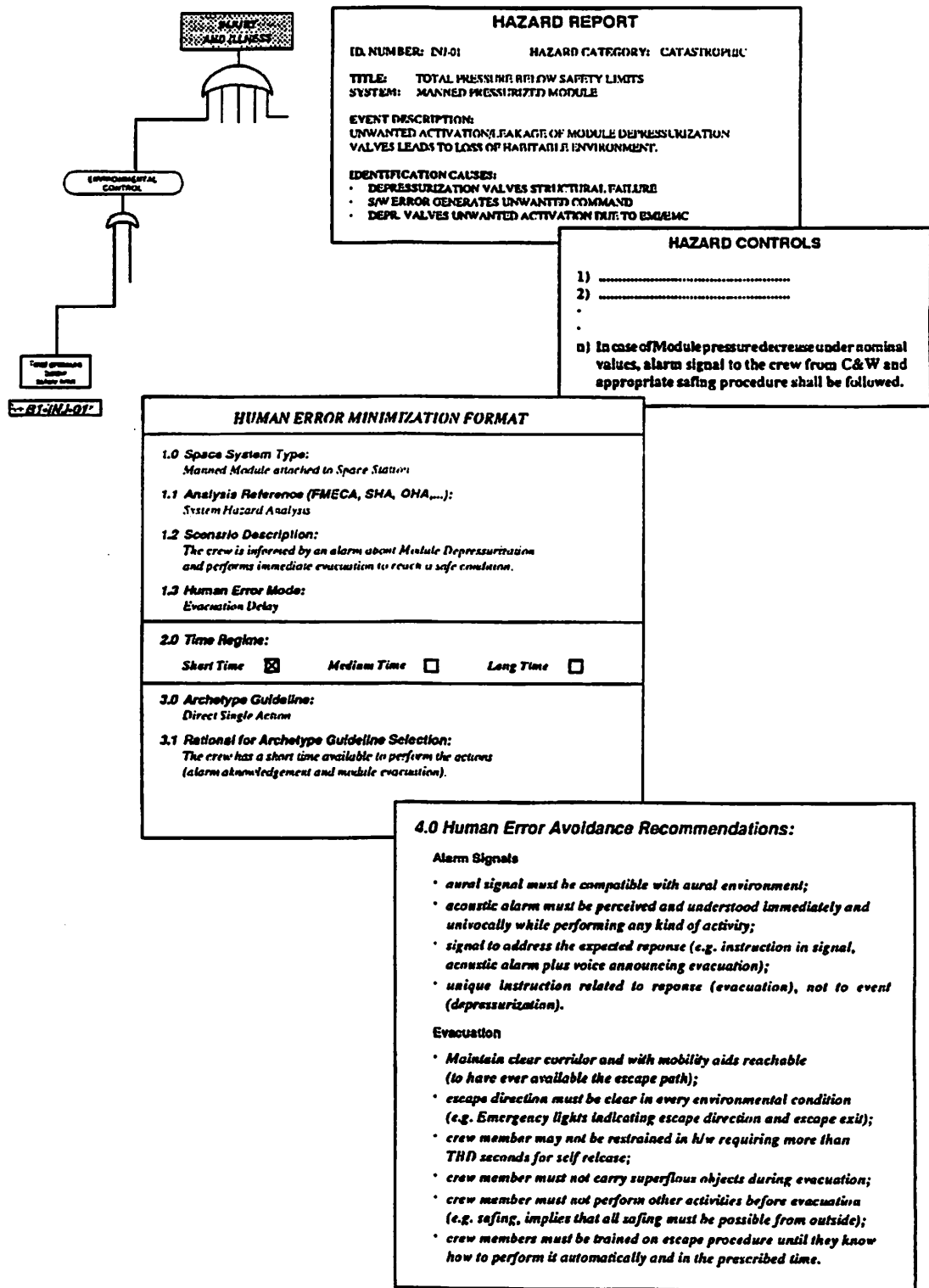


Figure 3 - Application to a manned module

## ACKNOWLEDGEMENTS

The methodology described in this paper is the result of a work carried out under a study commissioned by the PA & Safety Department of the ESTEC-ESA (European Space Research and Technology Centre - European Space Agency) (Contract Number 10143/92/NL/NB(SC)).

The authors would like to thank Mr. J. Fragola from SAIC Corporation, USA, for the support in the development of the paradigm, and Mr. F. Restagno, Alenia Spazio, Italy, for the contribution to the application of the methodology to existing Space Systems.

## REFERENCES

- [1] E.M. Dougherty and J.R.Fragola - *Human Reliability Analysis: A system Engineering approach with Nuclear Plant Applications*, J.Wiley & Sons, New York, 1988
- [2] R. Bergland - *The fabric of minds*, Viking Penguin Publishers, New York, 1985.
- [3] C. Cacciabue, C. Vivalda - *A Dynamic Methodology for evaluating Human error probability*, Proceeding of the international conference on PSAM Beverly Hills, California, US 1991.
- [4] M. Ferrante, D. Foltran - *A Product Assurance Engineering Concept for complex space systems*, Proceeding of ESA Symposium Space Product Assurance for Europe in the 1990s, Noordwijk, 1991.
- [5] NASA - *Man System Integration Standards*, STD 3000.
- [6] W.E. Woodson - *Human Factor Design Handbook*, McGraw-Hill, New York, 1981.

**101 Risk Assessment of Nuclear Waste Storage and Processing**

*Chair: D. Stack, LANL*

**PSA Results for Hanford High-Level Waste Tank 101-SY**

*D.R. MacFarlane, T.F. Bott, L.F. Brown, D.W. Stack (LANL); J. Kindinger, R.K. Deremer, S.R. Medhekar, T.J. Mikschl (PLG)*

## **PSA RESULTS FOR HANFORD HIGH LEVEL WASTE TANK 101-SY**

**D. R. MacFarlane, T. F. Bott, L. F. Brown, and D. W. Stack**

**Los Alamos National Laboratory  
Probabilistic Safety Assessment Section  
Engineering and Safety Analysis Group  
Nuclear Technology and Engineering Division  
Los Alamos, New Mexico 87545**

**J. Kindinger, R. K. Deremer, S. R. Medhekar, and T. J. Mikschl**

**PLG, Inc.  
4590 MacArthur Blvd.  
Suite 400  
Newport Beach, CA 92660-2027**

### **INTRODUCTION**

Los Alamos National Laboratory has performed a comprehensive probabilistic safety assessment (PSA) that includes consideration of external events for the weapons-production wastes stored in tank number 241-SY-101, commonly known as Tank 101-SY, as configured in December 1992. This tank, which periodically releases ("burps") a gaseous mixture of hydrogen, nitrous oxide, ammonia, and nitrogen, was analyzed because of public safety concerns associated with the potential for release of radioactive tank contents should this gas mixture be ignited during one of the burps.

In an effort to mitigate the burping phenomenon, an experiment is underway in which a large pump has been inserted into the tank to determine if pump-induced circulation of the tank contents will promote a slow, controlled release of the gases. This PSA for Tank 101-SY, which did not consider the pump experiment or future tank-remediation activities, involved three distinct tasks. First, the accident sequence analysis identified and quantified those potential accidents whose consequences result in tank material release. Second, characteristics and release paths for the airborne and liquid radioactive source terms were determined. Finally, the consequences, primarily onsite and offsite potential health effects resulting from radionuclide release, were estimated, and overall risk curves were constructed. An overview of each of these tasks and a summary of the overall results of the analysis are presented in the following sections.

### **ACCIDENT-SEQUENCE FREQUENCIES**

The accident-sequence analysis task started with a master logic diagram to identify the potential initiating events, which then were grouped into the 11 categories given in Table 1. These initiator groups included external events, such as earthquakes and airplane crashes, and internal events, such as gas releases (burps) and liquid leaks. Next, event trees, whose

Table 1. Initiating event groups

Initiating Event GROUP		
CODE	DESCRIPTION	EXAMPLE CAUSAL EVENTS
PSB	Primary Tank Shell Breach	Tank Shell Corrosion Drilling Contact with Tank Excavation Contact with Tank
DB	Tank Dome Breach	Vehicle Overloads Dome Water Overloads Dome Heavy Load Dropped over Dome
RVB	Riser or Ventilation Line Breach	Vehicle Impact with Above-Ground Equipment Human Error, Tank Left Open
FB1	Tank Exhaust HEPA Filter Breach	Exhaust Filter Breach Exhaust Filter Blockage
LOTV	Loss of Primary Tank Ventilation	Loss of Power to Vent Fan Vent Fan Failure Ventilation Inlet Blockage
LOSP	Loss of Tank Farm Offsite Power	
WI	Water Intrusion Event	Tank Inundated by Transfer Spill Tank Inundated by Raw Water Leak Tank Inundated by Heavy Precipitation
WT	Waste Transfer	New Waste Transfers from Other Facilities Salt Well Transfers to Collector Tank Liquid Transfers to 242-A Evaporator Slurry Transfers from 242-A to DS Tank Storage
SEIS	Seismic Event	
AIRCASH	Aircraft Crash	
BURP	Bound Gas Release	Waste Turnover Seismic Event Water Intrusion

branches represent chemical and nuclear phenomena, hardware responses, and emergency operator responses, were constructed for the important initiating-event groups. After initiator identification and event-tree construction, accident sequences were built by linking the initiating event for a particular event-tree path with the events on that path. The accident-sequences were linked in a manner that allowed for event-tree top dependencies to be identified. Finally, the accident sequences were quantified using the RISKMAN code<sup>1</sup> by combining initiating-event frequency estimates with the branch point probabilities, or split fractions, for the occurrence of each event on the event-tree paths. An important aspect of this process was quantification of the branch-point probabilities. This was done using a combination of tank farm historical operating databases and occurrence reports, generic component/system failure data, and specific deterministic analyses for Tank 101-SY. All of this effort entailed considerable interaction with Westinghouse Hanford Company (WHC) tank farm operations personnel, as well as analysts at Los Alamos and WHC who had performed other related safety analyses.

## RELEASE SOURCE TERMS

The source-term characterization task involved identifying factors that influence the magnitude and timing of a radionuclide or toxic gas (ammonia) release, as well as defining release categories for accident-sequence grouping. Multiple deterministic analyses were necessary for modeling material release mechanisms for the various accident sequences, thereby providing estimates for the quantity of material and energy involved in each case. Here again, considerable use was made of safety-related analyses performed by others. Recent core-sample analyses for the contents of Tank 101-SY were used to characterize the radionuclide composition of the source terms. To facilitate the comparison of high-frequency/low-consequence accidents with low-frequency/high-consequence accidents and to keep the number of calculations within a reasonable bound, the sequences were grouped into 12 release categories based on the release pathway and radionuclide content (Table 2).

Table 2. HTF PSA release category definition table

RELEASE PATHWAY		RADIONUCLIDE CONTENT	RELEASE CATEGORY CODE
To Atmosphere	Through HEPA	None	TG
	HEPA Bypassed	Low	BPL
	HEPA Breached	Low	HEPAL
	HEPA Breached	High	HEPAH
	Dome Collapsed	High	DCH
	Dome Collapsed	Very High (fire)	DCVH
To Ground	Subterranean Leak	Small	SLK
	Subterranean Leak	Large	LLK
To Atmosphere and Ground	Infiltration/Surface Spill	Small	SSP
	Transfer Failure/Surface Spill (NA 101-SY)	Large	LSP
	Dome Collapse + Small Leak	High	DCSLK
	Dome Collapse + Large Leak	High	DCLLK

Excluding the possibility of an airplane crash, these analyses generally showed that airborne releases are relatively small because of the lack of an energetic dispersal mechanism.

The potential liquid-pathway source terms were classified as small (< 5000 gal.) or large (>5000 gal.), with an upper bound based on both historical tank farm experience and the volume of leakable liquid currently contained in Tank 101-SY. For the purposes of estimating consequences of liquid leaks, the scenario adopted was liquid travel in groundwater to the Columbia River and delayed exposure of down-river populations via drinking water. This obviates the need to develop onsite exposure scenarios based on hypothetical assumptions about future land use. Even though the tank leaks may be large in terms of contained curies, their health effects are less severe because many radioisotopes remain bound to the soil in nonsoluble form, reaching the Columbia River only after a lengthy delay time, during which most of the radioactivity decays away.

## CONSEQUENCES OF RELEASES

The consequence analysis provided estimates of radiological and limited chemical health risks for both onsite workers and offsite residents via the airborne and groundwater pathways. Because of the large onsite worker population in relatively close proximity to the 200 West Tank Farm Area (the location of Tank 101-SY), the airborne dose consequences to this group also were included. The airborne-transport population doses were calculated with AP-RISK,<sup>2</sup> a computer code recently developed at Los Alamos for calculating dose consequences resulting from waste tank accidents. It is based on an integrated Gaussian puff model and includes features for treating large particle settling, as well as modeling discrete population clumps—both refinements needed for the onsite population groups. The code calculates a complete conditional dose distribution function based on a matrix of 576 meteorological conditions of wind speed, direction, and stability class. Plume-rise modeling was included in those cases involving a fire. This result, in combination with the source-term magnitude and distribution, defined the airborne consequences for a particular accident scenario.

The offsite liquid doses were estimated with a modified version of RESRAD,<sup>3</sup> a code developed for planning cleanup and remediation activities by Argonne National Laboratory under DOE sponsorship. In performing the liquid pathway transport analysis, a variety of water infiltration rates were considered that covered the range from current arid climate conditions to a possible future shift to a much wetter climate. Measured properties for the soil layers underlying the 200 West Area were used in the calculations. The conclusion from the analysis was that the river-integrated population doses are independent of the infiltration rate, primarily because the dose is dominated by the isotopes <sup>99</sup>Tc and <sup>129</sup>I, which both move with the groundwater and have very long half-lives, so they do not decay appreciably during the transport delay time to reach the river. The shorter half-life <sup>90</sup>Sr



and  $^{137}\text{Cs}$  are retained more readily in the soils, so they have decayed by the time they reach the river. Although they have long half-lives, the transuranic are retained in the soil and are delayed so long that they do not appear at the river for more than 10,000 yr. Doses occurring this far in the future have not been included in the PSA consequence analysis.

## OVERALL RISK RESULTS

The final results of the risk analysis are the unconditional risk curves, which present the relationship between the frequency of occurrence of the radionuclide release categories (given in Table 2) and the level of damage (radiological doses) caused by the release. Figures 1 and 2 present the mean composite risk curves for onsite and offsite airborne exposures, respectively. The contributions of each of the release categories to the composite curve also are shown. Even though hundreds of accident sequences were quantified, the burp/burn-initiated sequences emerged as the highest contributors to the risk. These accident sequences begin when the hydrogen released by a burp ignites because of the presence of a ventilation system ignition source. The resulting burn then propagates back into the tank, causing pressure loads that are sufficient to cause confinement failure, such as high-efficiency-particulate-air filter failure. A portion of the tank contents then is released directly into the environment and dispersed downwind. Although other sequences are more probable (such as a burp without burn, which releases ammonia gas), they result in essentially no health or environmental effects. Other sequences, such as those initiated by an airplane crash, have more serious consequences, but they are much less likely. Natural phenomena, such as earthquakes, high winds, ashfall, etc., did not prove to be significant risk contributors.

The mean risk (summation of the product of frequencies and consequences for all release categories) represented by the onsite and offsite curves presented in the two figures are 1.5 person-rem/yr [ $7.5 \times 10^{-4}$  additional latent cancer fatalities (LCFs)] and 20 person-rem/yr (0.01 additional LCFs). This is approximately 3 orders of magnitude below the health effects resulting from natural background radiation. Clearly, the onsite and offsite individual risks are substantially below the DOE safety goals, even using 95th percentile results.

The risk curve for the liquid-pathway doses is presented in Fig. 3. For an infiltration rate of 0.2 cm/yr, which corresponds to current climatic conditions, the time to reach the Columbia River is about 2000 yr, and the total dose exposure is accumulated over a time of

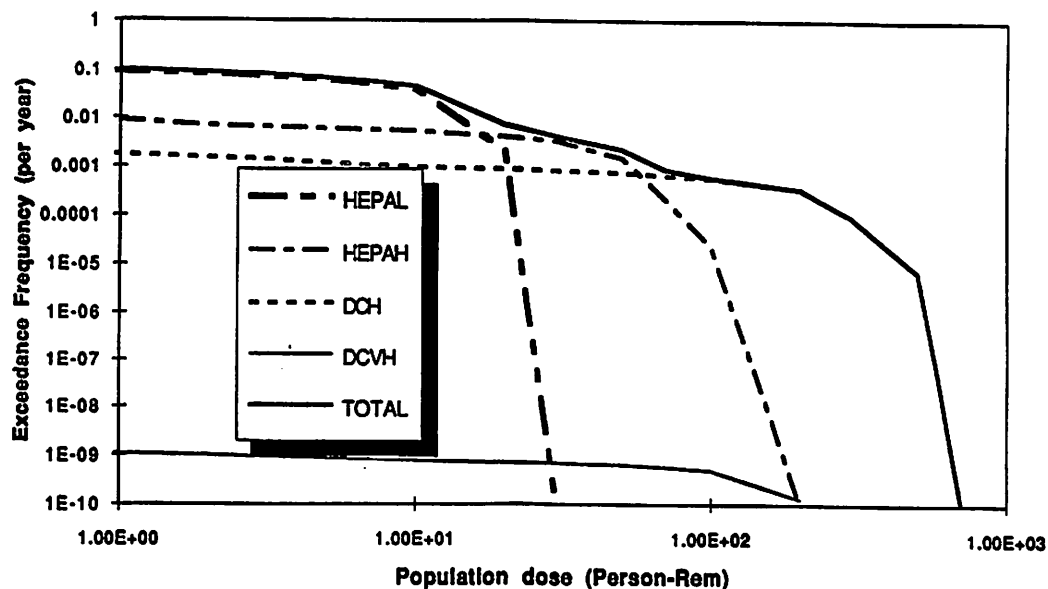


Figure 1. Mean total consequences—onsite.

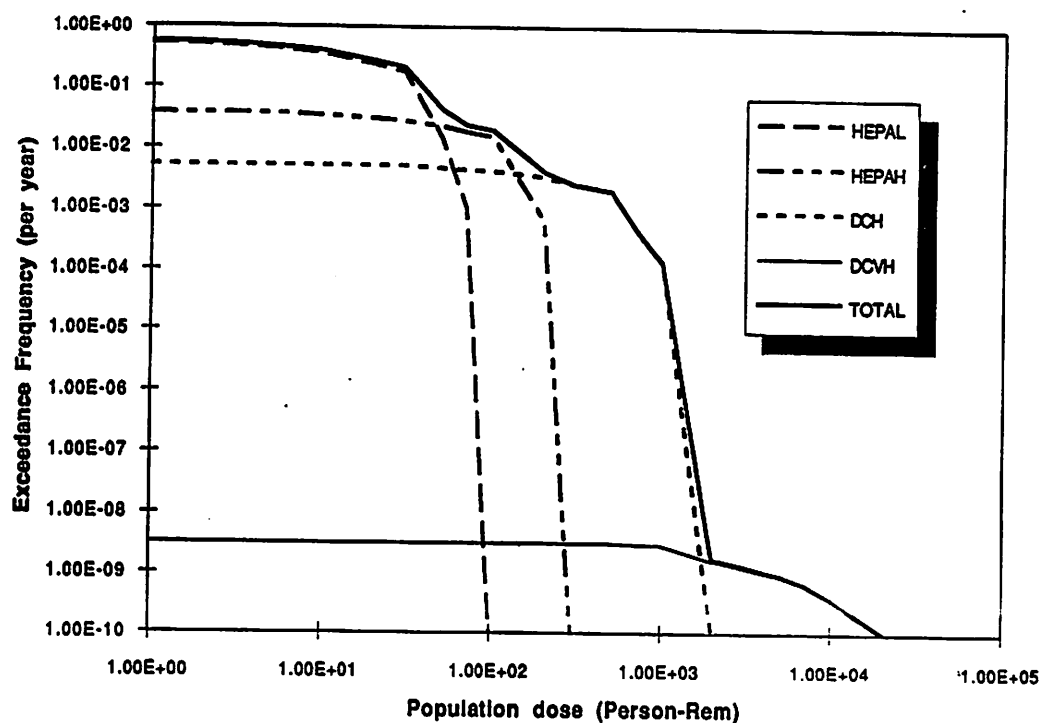


Figure 2. Mean total consequences—offsite.

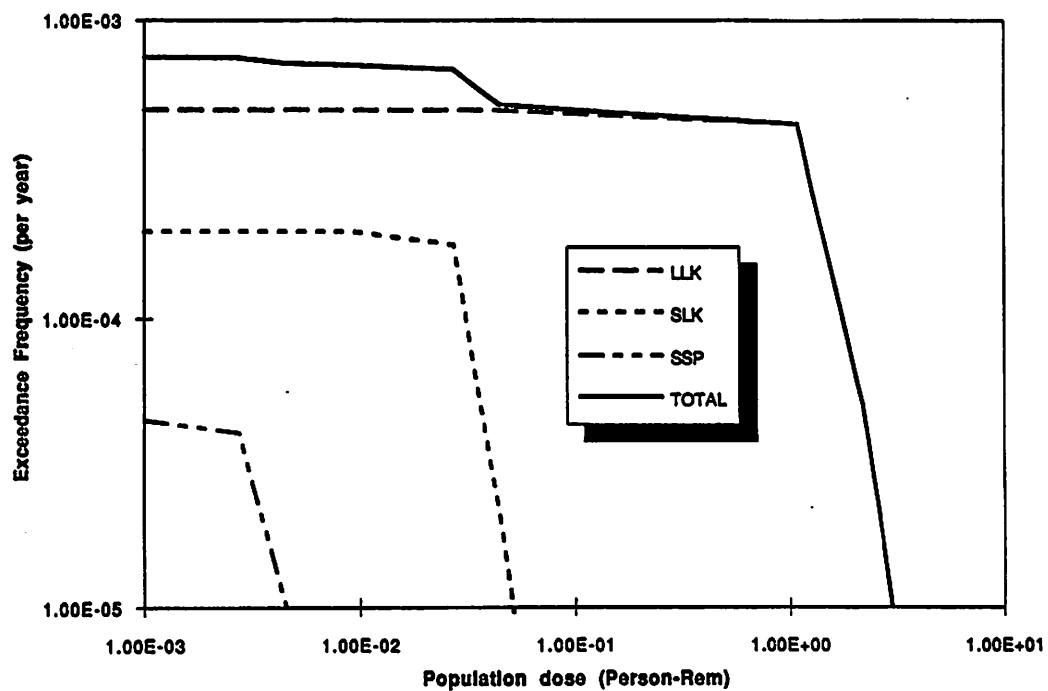


Figure 3. Mean total consequences—offsite liquid releases.

about 300 yr after radionuclides reach the river. The additional LCF corresponding to this exposure is  $2.5 \times 10^{-7}$ .

The conclusions from this PSA for Tank 101-SY may not be valid for other high-level waste tanks, which may have different chemical or radionuclide source terms, or for the whole waste tank farm complex, where common-cause failures, such as earthquakes, may be important. However, the principal consequences of any Tank 101-SY severe accident would be environmental, programmatic, and economic costs. For example, a large leak from Tank 101-SY would be perceived as a significant environmental insult and probably require an expenditure of tens of millions of dollars for containment, clean-up, and disposal operations. Furthermore, alternative storage and other remediation activities, such as construction of a replacement tank for Tank 101-SY, would be viewed suspiciously by the public. Likewise, a Tank 101-SY burp/burn accident, even with limited health effects, would reduce public confidence and jeopardize future remediation efforts.

It is clear that a comprehensive safety analysis is necessary before the initiation of any major project. Such an analysis should quantify risk from past and future operations and compliance, compare remediation effects with the costs and risk associated with continued short- and long-term operations, and evaluate the benefit of proposed remediation work. The results from such analyses will maximize DOE's ability to make long-term decisions regarding operations at the Hanford high-level waste tank farm.

A complete, detailed description of the methodologies and results for this study is given in Ref. 4.

## REFERENCES

1. PLG, Inc., 1992, *RISKMAN—PRA Workstation Software*, User Manuals I–IV, Version 3.0.
2. Y. C. Yuan and D. R. MacFarlane, "AP-RISK: A Computer Program for Calculating Doses and Health Risks from Accidental Release of Radioactive Materials," Los Alamos National Laboratory report in preparation.
3. T. L. Gilbert et al., 1989, "A Manual for Implementing Residual Radioactivity Material Guidelines," Argonne National Laboratory report ANL/ES-160.
4. D. R. MacFarlane et al., 1993, "Risk Assessment for Hanford High-Level Waste Tank 241 SY-101," Los Alamos National Laboratory document LA-UR-93-2730.

**102 Fire Risk**  
***Chair: V. Ho, PLG***

**Development of the Fire Risk Analysis Methodology for Nuclear Power Plants**  
***T. Matsuoka, K. Miyazaki (Ship Res. Inst., Japan); M. Kondo (JAERI, Japan)***

**A Methodology for Quantifying Fire Risk On-Board Spacecraft**  
***K.R. Paxton, F. Issacci, G. Apostolakis, I. Catton (UCLA)***

## DEVELOPMENT OF THE FIRE RISK ANALYSIS METHODOLOGY FOR NUCLEAR POWER PLANTS

Takeshi MATSUOKA<sup>1</sup>, Keiko MIYAZAKI<sup>1</sup>, and Masaaki KONDO<sup>2</sup>

<sup>1</sup>Systems Engineering Division, Ship Research Institute, Ministry of Transport  
6-38-1, Shinkawa, Mitaka, Tokyo, 181 Japan

<sup>2</sup>Risk Analysis Laboratory, Japan Atomic Energy Research Institute  
Tokai-mura, Naka-gun, Ibaraki-ken, Japan

### INTRODUCTION

It has been found out from the plant operating experience that typical nuclear power plants would have three or four significant fires over their operating lifetime. The recent study<sup>1</sup> has shown that the mean values of core damage frequency due to fire were found out to be comparable or greater than those due to internal events. For example,  $1.1 \times 10^{-5}$ /reactor · year for Surry plant, and  $2.0 \times 10^{-5}$ /reactor · year for Peach Bottom plant have been obtained in the NUREG-1150 report. So it is required to develop a fire risk analysis methodology which gives the comparably credible results with those of the analysis for internal event, and does not make an over-conservative estimation.

The Ship Research Institute and the Japan Atomic Energy Research Institute have performed a joint research<sup>2,3</sup> to establish a fire risk analysis methodology since 1989. This paper describes the procedure of fire risk analysis and the brief results of the analysis for a BWR type sample plant.

### FIRE RISK ANALYSIS METHODOLOGY

The fire risk analysis should evaluate the potential contributions to risk of fires anywhere in nuclear power plant. We have formulated the procedure of fire risk analysis as shown in Figure 1. There are six principal steps in this procedure; Plant familiarization, Identification and screening of fire areas, Evaluation of safe shutdown probability, Fire hazard and fire suppression analyses, Re-evaluation of fire occurrence frequency, and Evaluation of core damage frequency.

#### Plant Familiarization

The first and most important step of the analysis is plant familiarization. The general location of components of the principal plant systems could be identified from the general arrangement drawings. A plant visit is made to obtain the more detailed information such as the location of cables, doors, barriers and penetrations. Also the actual situation of fire protection systems and fire fighting procedures are confirmed on a plant visit.

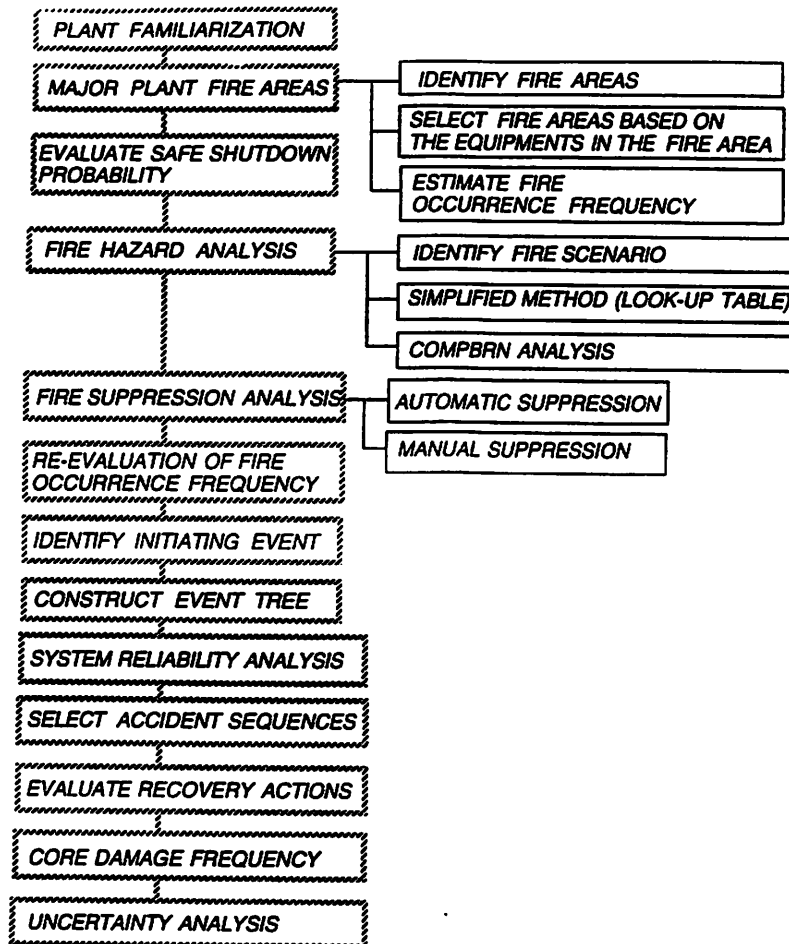


Figure 1. Procedure of fire risk analysis.

### Identification and Screening of Fire Areas

The plant is broken down into fire areas bounded by 2 to 3-hour rated fire barriers. For one hour rated fire barriers, it is evaluated as a fire area boundary based on the possible maximum combustible loading and automatic fire suppression system inside the area. Fire areas have no opening and must be completely surrounded by fire barriers.

Then, some of the fire areas identified above are screened out if there is no component related to the plant operation or any safety system. If there is a possibility for an operator to shutdown the reactor in case of a fire in a fire area, that area is considered significant and kept for further analysis.

The fire occurrence frequency for all the remaining fire area is estimated based on the nuclear power plant fire data<sup>4</sup> compiled by the EPRI. Fire areas which fire occurrence frequency is less than  $1 \times 10^{-6}$ /area  $\cdot$  year are screened out from further evaluation.

It is assumed that all equipments and cables within a fire area are damaged and lost their functions. For each fire area, select the most probable initiating event, and evaluate the safe shutdown probability by utilizing an event tree developed in the internal event analysis. The event tree and the fault trees are modified with the condition the components in the fire area are damaged and inoperable. In this case, the safe shutdown means the reactor could be conducted to the cold shutdown state.

If the product of fire occurrence frequency ( $F_f$ ) and the failure probability of safe shutdown ( $P_{sd}$ ) is less than  $1 \times 10^{-6}/\text{area} \cdot \text{year}$  then the fire area can be screened out from further evaluation.

### Fire Hazard and Fire Suppression Analyses

First, identify some conservative fire scenarios for each fire area by considering the size of fire sources (large/ small), the kind of fire sources (cable fire/ control panel fire/ transient combustible materials/ ...) and so on. Next, it is evaluated whether equipments in the area are damaged or not by the look-up tables in the FIVE methodology<sup>4</sup>. In the FIVE methodology, the fire sources are treated as point source fires. If it requires more detailed analysis, a fire progression analysis is performed by the COMPBRN III or IIIe code.<sup>5,6</sup>

If the equipments are evaluated to be damaged by a fire, it is necessary to estimate the success probability of fire suppression prior to equipment damage. For automatic suppression systems, the fire suppression probability is deduced from the probability of automatic suppression systems being available which is estimated based on a generic industrial data base. For manual fire suppression, the success probability is estimated from the fire suppression model proposed by Siu et al.,<sup>7</sup> or the cumulative curves of fire suppression time<sup>8,9</sup> deduced from the nuclear power plant fire incident data. The total failure probability of fire suppression ( $P_{fs}$ ) is obtained from the product of the failure probabilities by automatic suppression ( $P_{fa}$ ) and by manual suppression ( $P_{fm}$ ).

If no equipment is damaged in the most conservative fire scenario, the fire area can be screened out.

### Re-Evaluation of Fire Occurrence Frequency

The fire occurrence frequency ( $F'_f$ ) is estimated for each specific fire condition identified and survived in the fire hazard and fire suppression analysis. A partitioning method is applied. For example, it is considered the fraction of fire zone to the total room area, in which the target equipments are damaged by a fire.

If the value of  $F'_f \cdot P_{sd} \cdot P_{fs}$  is less than  $1 \times 10^{-6}/\text{area} \cdot \text{year}$  then the fire condition is screened out from further evaluation.

### Evaluation of Core Damage Frequency

After performing the above screening analyses, the evaluation of core damage frequency is conducted for each fire condition. The analysis steps are almost the same as those for internal events. They consist of the identification of initiating events, the construction of event tree, system reliability analyses, the screenings of accident sequences, the evaluation of recovery actions, the calculation of the point estimation of core damage frequency and the uncertainty analysis.

The event trees and fault trees are constructed based on those for internal event analysis with considering fire condition.

If the occurrence frequency of accident sequence is less than  $1 \times 10^{-6}/\text{reactor} \cdot \text{year}$  then this sequence is screened out. The summation of the occurrence frequency of the remaining accident sequences becomes the core damage frequency due to fire events in nuclear power plant.

## SAMPLE PLANT ANALYSIS

The fire risk analysis methodology presented here was applied to the analysis for a BWR type sample plant. The structure and physical arrangements of the sample plant were constructed based on the open documents<sup>10</sup>.

### Identification and Screening of Fire Areas

The sample plant was divided into 145 fire areas, and 99 fire areas were screened out because of containing no component related to the plant operation or any safety system, or the fire occurrence frequency being less than  $1 \times 10^{-6}/\text{area} \cdot \text{year}$ .

### Evaluation of Safe Shutdown Probability

In this step, almost all the fire area were screened out because of the product of fire occurrence frequency ( $F_f$ ) and the failure probability of safe shutdown ( $P_{sd}$ ) being less than  $1 \times 10^{-6}/\text{area} \cdot \text{year}$ . Only two fire areas, control room and switchgear room, were identified as the areas in which fires might significantly contribute to a core damage frequency.

### Fire Hazard and Fire Suppression Analyses

For the control room, we assumed there would be no fire incident produced by transient combustibles, based on the information obtained on a plant visit. So, self-ignited cables in control panels were identified as potential fire sources. In this case, the success probability of fire suppression prior to equipment damage was necessarily presumed zero because these cables were regarded as a target: a component related to a plant operation or a safe shutdown system.

For switchgear room, three fire scenarios were assumed as follows.

- (1) Fire source is transient combustible material (heptane) located on the floor in the center of switchgear room. The fuel size is  $3 \times 3 \text{ m}^2$  with 0.1m thickness, that is 630 kg-weight liquid fuel. The volume of the room is  $820 \text{ m}^3$ . The target is electrical cables located above the switchgear cabinets. The damage temperature was assumed as  $370^\circ\text{C}$ .
- (2) Same as scenario (1), but with the  $0.5 \times 0.5 \times 0.1 \text{ m}^3$  fuel size.
- (3) The fire source is a self-ignited electrical cable inside a electrical distribution panel located on the wall of the room. The target is the electrical cables attached to the top of the distribution panel.

In case (1), it was evaluated, from the look-up tables presented in the FIVE, that the target cables were damaged immediately after the fire ignition. Then, the success probability of fire suppression prior to cable damage was presumed zero.

In case (2), the damage time was predicted as about 80 minutes, which was so long for fire detector's response time. Then the  $P_a$  was estimated as  $5 \times 10^{-2}$  from the unavailability of automatic fire suppression system. The failure probability of manual suppression ( $P_{fm}$ ) was estimated as 0.3 by an engineering judgement in which the fire suppression model, the cumulative curves of fire suppression time, and the information from a plant personnel were considered. Therefore, the failure probability of fire suppression ( $P_a$ ) prior to cable damage was estimated as 0.015.

In case (3), the target cables are attached to the distribution panel and were evaluated to be damaged quickly after the fire ignition inside the panel. Then, the success probability of fire suppression was presumed zero.

### Re-Evaluation of Fire Occurrence Frequency

Fire occurrence frequency in the switchgear room was re-evaluated for each fire scenario assumed in the previous step.

The total fire occurrence frequency in the switchgear room was estimated to be



$7.5 \times 10^{-3}$  /area · year in the step of the screening of fire areas. The ratio between cable fires and heptane fires in the switchgear room was assumed to be equal to the ratio between non-qualified cable fires and transient combustible fires in a whole plant. Therefore, the occurrence frequencies of cable and heptane fires in the switchgear room were estimated to be  $6.2 \times 10^{-3}$  /area · year and  $1.3 \times 10^{-3}$  /area · year, respectively (Figure 2.).

It was also assumed that the size of fire source depended on the fire duration time. We defined the large fire as one of which duration time was more than 30 minutes, and the rest were small fires. The fire incident data<sup>11</sup> indicates that the fraction of fires with more than 30 minutes is 37.5%. The occurrence frequency of heptane fire was divided into the frequencies for small and large fires. They were estimated to be  $8.1 \times 10^{-4}$  /area · year for small fires and  $4.9 \times 10^{-4}$  /area · year for large fires, as shown in Figure 2.

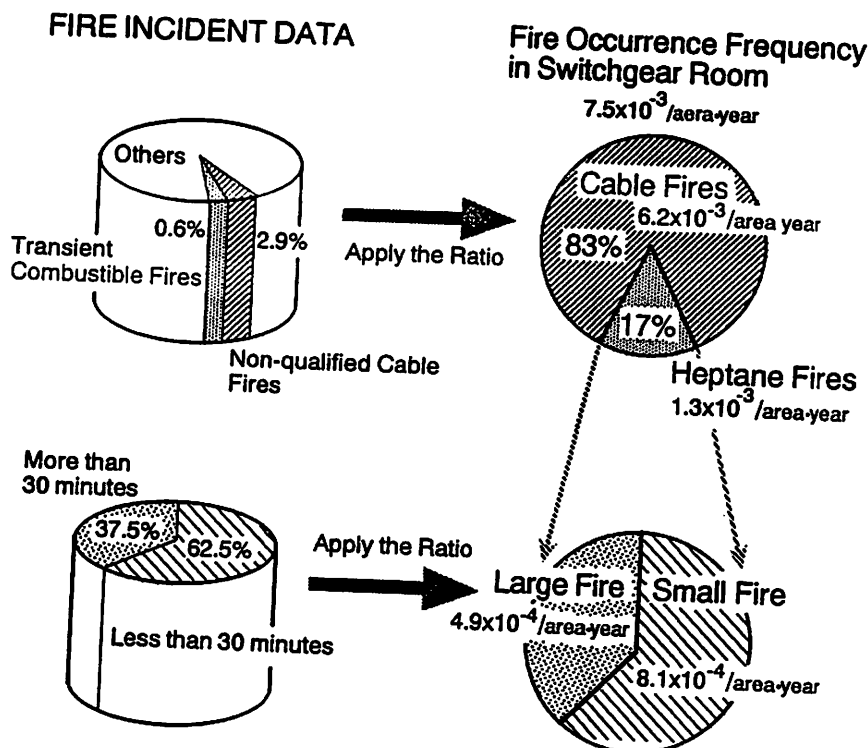


Figure 2. Partitioning method for re-evaluation of fire occurrence frequency in switchgear room.

As for the control room fire, we considered only the cable fires in control panels. The control panels consist of several different kind of function panels such as main control panel, ECCS control panel. The fire occurrence frequency for each panel was estimated by using partitioning method comprised of rationing the area of panels as shown in Figure 3. It was found out that the two largest fire occurrence frequencies were  $3.9 \times 10^{-3}$  /panel · year for the auxiliary control panel and  $2.1 \times 10^{-3}$  /panel · year for the main control panel.

Core damage frequency for each fire condition was evaluated by using the fire occurrence frequency re-evaluated above, and the safe shutdown and fire suppression probabilities. Two fire conditions were survived because of their core damage frequency being greater than  $1 \times 10^{-6}$  /reactor · year. These are the distribution panel fire in the switchgear room and the ECCS control panel fire in the control room. All other fire conditions were then eliminated from further analysis.

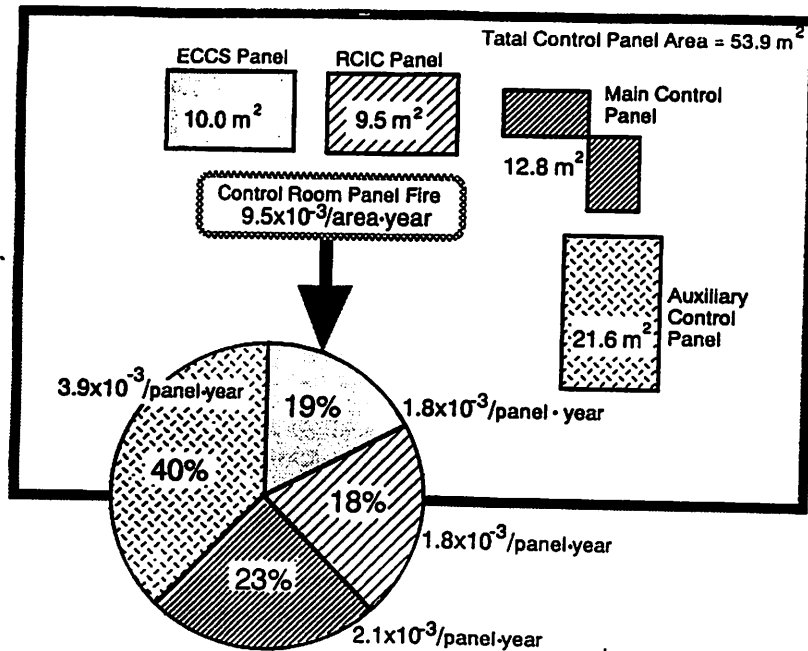


Figure 3. Partitioning method for re-evaluation of fire occurrence frequency in control room.

### Evaluation of Core Damage Frequency

We considered that the distribution panel fire in the switchgear room would lead to loss of offsite power. The LOSP initiated event tree developed in an internal event analysis<sup>2</sup> was used without any modification for this fire condition, because the safety related systems considered in the LOSP event tree would not be directly damaged by the fire restricted in the switchgear room.

In developing the event tree, it is necessary to consider how the ECCS panel fire affects the function of the components controlled by this panel. As for the control room fire, the following assumptions were made in this analysis.

- (1) Operators would manually scram whenever fire occurred in a control room.
- (2) The components in operation keep their functions, but standby components for emergency fail to start.
- (3) Immediately after the ignition of the ECCS panel, systems controlled from this panel become unable to start, that is, the ECCSs are unavailable. The following equipments would remain operable: Safety relief valve for pressure control, FW and RCIC for high pressure injection, and PCS for residual heat removal.
- (4) No credit is taken for operators to recover the malfunctioned systems or to take a back-up from the remote scram panel as well as the main control room panel.

Consequently, it was found that the following were the three dominant accident sequences among those with the occurrence frequency of more than  $1 \times 10^{-6}$ /reactor · year.

- (1) The distribution panel fire in the switchgear room induced LOSP with the failure of all emergency diesel generators.
- (2) The ECCS panel fire in the control room induced manual scram with the failure of power conversion system.
- (3) Same as (2), but with the failures of feed water system and reactor core isolation cooling system.

This paper has presented the fire risk analysis methodology developed by the joint research of the Ship Research Institute and the Japan Atomic Energy Research Institute. An analysis of the fire risk was performed for a BWR type sample plant and its analysis steps were briefly described.

The main characteristics of the methodology presented in this paper are as follows.

- (1) The procedures of screening analysis for fire areas are systematically arranged based on the FIVE methodology.
- (2) Re-evaluation of the fire occurrence frequency is performed for each fire scenario by using partitioning method. The results of fire progression analyses by the COMPBRN code are applicable to this evaluation.

In the present analysis, the following matters were also examined.

- (a) The damaging effects of smoke on high voltage equipment.
- (b) Heat release from a paper stack placed in the control room.
- (c) The possibility of fire propagation to adjacent compartment.
- (d) The effects of combustion of paint on walls and ceiling.

From the execution of the fire risk analysis, the following findings were extracted.

- (I) It is required to develop a more realistic model or analysis technique for fire suppression activity.
- (II) It is desirable to improve the COMPBRN III code to be more transparent for users, that is, models and assumption used in the code could be more clearly described.
- (III) It is also desirable to improve the COMPBRN III code to be applicable to evaluate the possibility of the fire propagation to adjacent compartments.
- (IV) The separation of redundant systems into different compartments is effective to keep the core damage frequency low with the assumption of a single room fire.
- (V) More detailed system reliability analysis is required for some fire scenarios in the Turbine building.

## REFERENCES

1. U.S. Nuclear Regulatory Commission, Sever Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, NUREG-1150 (December 1990).
2. T.Matsuoka et al., Study of External Event Analysis Method (III), Report submitted to JAERI (March 1991) (in Japanese).
3. T.Matsuoka et al., Study of Fire Risk Analysis Method (II), Report submitted to JAERI (March 1993) (in Japanese).
4. EPRI-TR-100370, Fire-Induced Vulnerability Evaluation (FIVE) Methodology Plant Screening Guide, (April 1992).
5. NUREG/CR-4566, ORNL/TM-10005, COMPBRN III - A Computer Code for Modeling Compartment Fires, (July 1986).
6. UCLA-ENG-9016, EPRI-NP-7282, COMPBRN III: An Interactive Computer Codes for Fire Risk Analysis, (May 1991).
7. N.Siu and G. Apostolakis, A Methodology for Analyzing the Detection and Suppression of Fires in Nuclear Power Plants, Nuclear Science and Engineering, 94:213(1986).
8. Philadelphia Electric Company, Sever Accident Risk Assessment Limerick Generating Station, (April 1983).
9. NUREG/CR-5088, SAND88-0177, Fire Risk Scoping Study: Investigation of Nuclear Power Plant Fire Risk, Including Previously Unaddressed Issues, (January 1989).
10. Nuclear Safety Research Association, An Outline of Light Water Power Generating Plants (Revised Edition), (1992) (in Japanese).
11. NUREG/CR-4586, SAND86-0300, User's Guide for a Personal Computer-Based Nuclear Power Plant Fire Data Base, (August 1988).
12. N.Watanabe et al., LOSEP-Initiated Event Tree Analysis for BWR, JAERI-M 89-025, (February 1989) (in Japanese).

## **A Methodology for Quantifying Fire Risk On-Board Spacecraft**

K.R. Paxton, F. Issacci, G. Apostolakis and I. Catton

Mechanical, Aerospace and Nuclear Engineering  
University of California  
Los Angeles, CA 90024-1597

### **ABSTRACT**

Past applications of fire risk assessments to nuclear power plants have only been concerned with the thermal threat. The detection process was treated using empirical data and was thus independent of the damage process. The closed environment of a spacecraft makes the assumptions of only a thermal threat and the independence of the damage and detection processes inappropriate. A revised methodology that incorporates multiple modes to damage and detection is presented in this paper. The new methodology is meant to be based on multiple phenomena-based models that describe the concentration of the damage- and detection-causing elements. This new methodology is not meant to be limited to spacecraft application. It can be used in any situation where multiple modes of damage and/or detection need to be addressed, for example, the assessment of heat and smoke effects on a nuclear-power plant.

### **INTRODUCTION**

The launching of human-crewed spacecraft for long periods of time, such as the Space Station *Freedom*, will usher in a new dawn of space exploration and experimentation. There will be many new scientific and commercial activities aboard these spacecraft during the greatly extended mission life. These new activities can increase the safety hazards, foremost of which is the risk of fire.<sup>1</sup> A spacecraft fire is especially dangerous due to the combination of heat release, weakening of spacecraft structures, release of toxic gases, and possible long term damage to electrical equipment from contamination by airborne fire and suppression products.<sup>2</sup> Probabilistic Safety Assessment (PSA) can be a useful tool to identify the major threats so that steps may be taken to mitigate their contribution to the total risk.<sup>3</sup> However, in order to quantify the PSA, a revised methodology is required. This new methodology must deal with multiple modes for damage and detection to occur. A complete PSA will help to improve the safety of spacecraft.

The probability that a critical component or the crew is damaged can be derived by modeling the damage and detection/suppression processes as competing in time. The frequency that the damage time is less than the detection/suppression time is the probability of damage. Normally, only the thermal threat has been assessed in previous applications to nuclear-power plants. There are multiple threats due to a fire aboard spacecraft. Smoke and toxic fumes pose a threat to the astronauts since there is no egress. Smoke and corrosive gases pose a threat to the sensitive electronic components.<sup>4,5</sup> These are in addition to the threat of thermal damage to the spacecraft and crew. It is important to note that both the fire and the suppression processes can be a threat to the spacecraft and the crew. If too much carbon dioxide is released into the environment, the crew will not be able to survive without some type of safety breathing apparatus. Another possible scenario is an undetected wire overload in a remote location. The released toxic gases could poison a crew member before the threat is identified. A third scenario is that the corrosive gases condense on some critical component's circuitry and subsequently fail the system, possibly resulting in severe consequences. Detection can occur by either a smoke, thermal, or gas detector alarming. There is also the possibility that an astronaut will see some smoke or smell some of the fumes. Even if the astronaut discovers one of these fire signatures, the source may not be evident, thus action may be delayed. In general, the lack of egress and the delicate nature of the circuitry on-board spacecraft requires a new approach to the risk assessment to incorporate the four modes of damage (heat, smoke, toxins and corrosives) and possibly three modes of detection (smoke, heat and gases).

It would appear that in order to quantify the probability of damage, seven damage or detection processes would have to be modeled as competing in time. The methodology of how to deal with these multiple modes is discussed in this paper. The methodology is not limited to spacecraft application; it may also be applied to terrestrial situations. Science is finding that the smoke production during a fire is a serious problem on earth. This methodology is required so that this threat can be incorporated into the terrestrial safety assessments.

## TERRESTRIAL PSA METHODOLOGY

Within any complex industrial plant, there are many different fire scenarios that can lead to severe damage. To find the total risk due to fire, it is necessary to sum the contribution from each scenario. The risk from a single scenario may be quantified as follows<sup>6</sup>:

$$\lambda_{\text{severe damage}} = \lambda_j Q_{k|j} Q_{s.D.|k,j} \quad (1)$$

$\lambda_{\text{severe damage}}$	Frequency of severe damage
$\lambda_j$	Frequency of class j fires (the class is determined by the initial severity and location)
$Q_{k j}$	Fraction of class j fires that lead to damage of the k <sup>th</sup> critical system
$Q_{s.D. k,j}$	Fraction of class j fires leading to damage of the k <sup>th</sup> system that cause severe damage

As mentioned above, the general approach is to model the damage and detection/suppression processes as competing in time. The frequency that the damage time is less than the detection/suppression time is the probability of damage. Mathematically,  $Q_{kij}$  can be described by:<sup>9</sup>

$$Q_{kij} = \Pr\{T_D < T_C \mid \text{fire}\} \quad (2)$$

$\Pr\{T_D < T_C \mid \text{fire}\}$	Probability that the damage time is less than the control time given there is a fire
$T_D$	Damage time (time for the fire to damage the $k^{\text{th}}$ component)
$T_C$	Control time (elapsed time from initiation until the fire is under control)

For the assessment of the control time, the fire does not have to be extinguished, just controlled to the point where it cannot do any more harm. If we view the damage and control as two processes competing in time, then equation (2) simply states that the probability of damage is the probability or frequency that the damage process wins the competition. Note that in the references, the damage and control times are referred to as the growth,  $T_G$ , and hazard times,  $T_H$ , respectively.

The control time may be broken down into smaller time steps.

$$T_C = T_f + T_d + T_e + T_s \quad (3)$$

$T_f$	Time for fire "signature" to reach detectable level at the detector
$T_d$	Detector response time
$T_e$	Elapsed time to initiate suppression from the time of detection
$T_s$	Suppression time

This form for  $T_C$  further emphasizes that the control time is composed of the times required for detection of the fire, suppression to be initiated, and for the suppression effort to bring the fire under control. The time for suppression to be initiated may seem inconsequential, however it may not be. The fire may be detected by a smoke detector, but someone might be sent to the area to corroborate the detector. Another possibility may be that the fire is detected, but the optimal suppression effort is unknown, and thus action is delayed.

In power plant applications, the damage time may be quantified using a computer model such as COMPBRN.<sup>7</sup> This code combines many different models of fire phenomena to calculate the damage time. The code predicts a unique time until damage, given a set of inputs. However, there are large uncertainties associated with the input parameters. Typically, many different realistic combinations of the input parameters are tested and a distribution of the growth time is developed. This can then be used in conjunction with the control time distribution to find the fraction of fires that damage the  $k^{\text{th}}$  component.

- The control time is treated as a random variable whose distribution is derived from data of past events. Precise data are usually easy to work with, however, there is very little precise data on detection because people usually only know when a detector signals and not when the fire began. Usually the detection data are given by some bounds or a distribution. These various forms of data are combined together using Bayes' theorem. A distribution of the control time is thus obtained. For more information on the method and some example data, see Siu.<sup>8</sup>

Once distributions for the damage time and the control time are developed, then the probability of damage can be evaluated. A control time and a damage time are randomly selected from the respective distributions. The frequency that the damage time is smaller than the control time is the probability of damage. One fault with this technique is that it assumes that the damage modes and the control modes are independent of each other, when in fact they are both dependent on the same fire event. This deficiency is remedied in the proposed methodology.

## SPACECRAFT PSA METHODOLOGY

Only the thermal threat has typically been assessed in previous applications to nuclear-power plants, while aboard spacecraft, there are many threats due to the lack of egress and the sensitivity of the electronics to corrosives. The above analysis for determining the fraction of fires that damage a component depends on developed models and detection time data. For microgravity application, there is very little in the way of appropriate models and/or data. The current experimental goal is to develop the phenomena-based models for assessing  $Q_{k|j}$ . These models will give the concentration of the different species (heat, smoke, toxins and corrosives) as a function of time and space. These models along with knowledge concerning the resistivity of the astronauts and the components to the various species can be utilized to calculate the time to damage. The time to detection will simply be the time for the smoke to reach a detectable level at the detector.

Wire shorts or component overloads have been the most frequent fire or fire initiators aboard the Space Shuttle.<sup>9</sup> Thus it is necessary to examine the pyrolysis of the wire in real application scenarios. This is the subject of the current modeling investigation, however the newly developed approach to quantifying the risk is applicable to any fire event, be it flaming or smoldering.

In order to simplify the problem, the fire event is broken down into three processes. These can be described as the *source* of the damage causing element, the associated *transport* process and the *deposition* or *attenuation* process. Since the microgravity test is limited in time (2.2 seconds), the emphasis has been on quantifying the source. The general modeling approach is to characterize the release of the four damage-causing elements as a function of the ohmic heating and then define the subsequent transport and attenuation.<sup>10,11</sup> This leads to concentration models as a function of space and time, which will be used to calculate the control and damage times for each mode.<sup>12,13</sup> The experiment results of the temperature response and mass consumption have been published,<sup>14</sup> along with the smoke production<sup>15</sup> and morphology<sup>16</sup> results.

Since only one mode is required for damage or detection, the damage or detection time is simply the minimum of the respective times from the multiple modes, i.e.,

$$\begin{aligned} T_D &= \min \{T_{D, \text{heat}}, T_{D, \text{smoke}}, T_{D, \text{toxins}}, T_{D, \text{corr.}}\} \\ T_C &= \min \{T_{C, \text{heat}}, T_{C, \text{smoke}}, T_{C, \text{toxins}}\} \end{aligned} \quad (4)$$

Note that for each set of input parameters there is a unique control and damage time corresponding to each mode. However, there is uncertainty in the input parameters, i.e. there is uncertainty in the event location, initial overload current, air flow rates, etc. In order to deal with these uncertainties, a Monte Carlo simulation can be conducted using Equation (2) and parameter distributions. For each pass, a unique set of parameters is picked from the respective distribution. It is then determined if damage occurs or does not occur. This is repeated to cover the ranges of the parameter distributions. This technique forces the control and damage times to be dependent on the same fire event for each pass of the simulation. The characteristics of the fire event are being varied in order to cover the uncertainties in position, current, etc. In previous PSA's, the control time was assigned a distribution that was independent of the fire physics, such as the actual amount of smoke produced. With this new approach, this assumption of independence ceases to exist. The simulation will output a distribution of the frequency of damage. It is important to realize that the distribution is not based on stochastic means, but only on the associated uncertainty of the input parameters.

## CONCLUSIONS

A brief overview of the assessment methods for fire risk in terrestrial applications has been presented. This methodology is limited in that it is only concerned with the thermal threat and it treats the damage and detection processes as being independent events. These assumptions are inappropriate for application to a fire risk assessment aboard spacecraft. Due to the closed environment of the spacecraft, there are multiple threats to the spacecraft and its crew. A revised methodology to incorporate these multiple threats has been presented. Due to the lack of historical data, both the damage and detection processes are to be modeled. This forces the two processes to be dependent on the same fire event instead of being treated as independent events as done in the simpler terrestrial methodology. This revised methodology, while more complex, is more realistic. It should not be limited to spacecraft application, but should be incorporated into all fire-type risk assessment so that the multiple modes to damage and detection can be addressed.



## REFERENCES

1. Raasch, R.F., Peercy Jr., R.L. and Rockoff, L.A., "Space Station Crew Safety Alternatives Study-Final Report," Vol. 2--Threat Development, NASA CR-3855, June, 1985.
2. Friedman, R. and Sacksteder, K.R., "Fire Behavior and Risk Analysis in Spacecraft," NASA TM-100944, 1988.
3. Paulos, T., Paxton, K., Jones, S., Issacci, F., Catton, I. and Apostolakis, G., "Risk-Based Fire Safety Experiments," *AIAA Paper 93-1153*, AIAA/AHS/ASME Aerospace Design Conference, Irvine, CA, 1993.
4. Babrauskas, V., "Toxic Hazard from Fires: A Simple Assessment Method," *Fire Safety Journal*, 20, 1993, pp. 1-14.
5. Tewarson, A., "Nonthermal Fire Damage," *Journal of Fire Science*, 10, No. 3, May/June 1992, pp. 188-242.
6. Kazarians, M., Siu, N. and Apostolakis, G., "Fire Risk Analysis for Nuclear Power Plants: Methodological Developments and Applications", *Risk Analysis*, 5, 1985, pp. 33-51.
7. Ho, V. & Apostolakis, G., "COMPBRN IIIe - A Computer Code for Probabilistic Risk Analysis," *Nuclear Engineering and Design*, 138, 1992, pp. 357-373.
8. Siu, N. & Apostolakis, G., "Modeling the Detection Rates of Fires in Nuclear Plants: Development and Application of a Methodology for Treating Imprecise Evidence," *Risk Analysis*, 6, No. 1, 1986.
9. Friedman, R. & Urban, D.L., "Contributions of Microgravity Test Results to the Design of Spacecraft Fire Safety Systems," presented at the AIAA/AHS/ASME Second Aerospace Design Conference, Irvine, CA, February 16-19, NASA TM 106093, AIAA-93-1152, 1993.
10. Im, K.H., Ahluwalia, R.K. & Chuang, C.F., "RAFT: A Computer Model for Formation and Transport of Fission Product Aerosols in LWR Primary Systems," *Aerosol Science and Technology*, 4, 1985, pp. 125-140.
11. Pagni, P.J., Alvares, N.J. & Foote, K.L., "Defining Characteristic Times in Forced Ventilation Enclosure Fires," *Mathematical Modeling of Fires*, STP 983, J.R. Mehoff, Ed., American Society for Testing and Materials, Philadelphia, 1987, pp. 68-82.
12. Evans, D.D. & Stroup, D.W., "Methods to Calculate the Response Time of Heat and Smoke Detectors Installed Below Large Unobstructed Ceilings," NBSIR 85-3167, 1985.
13. Alpert, R.L., "Calculation of Response Time of Ceiling-Mounted Fire Detectors," *Fire Technology*, 8, 1972, pp. 181-195.
14. Jones, S.T., Issacci, F., Catton, I., and Apostolakis, G., "Temperature and Mass Loss of Overheated Wires in Microgravity", ASME, Fundamentals of Heat Transfer in a Microgravity Environment, Winter Annual Meeting, New Orleans, Louisiana, 1993.
15. Paxton, K.P., Issacci, F., Catton, I., and Apostolakis, G., "Smoke Production from Overheated Wires in Normal and Microgravity", ASME, Fundamentals of Heat Transfer in a Microgravity Environment, Winter Annual Meeting, New Orleans, Louisiana, 1993.
16. Paul, M., Issacci, F., Catton, I., and Apostolakis, G., "Morphological Description of Particles Generated from the Overheating of Wire Insulation in Microgravity and Terrestrial Environments," ASME, Heat Transfer in Microgravity Systems, 29th National Heat Transfer Conference, Atlanta, Georgia, 1993.

### **103 Risk-Based Regulation (III)**

*Chair: F. Rahn, EPRI*

**Where Do We Go from Here in U.S. Nuclear Safety Regulation?**

*V. Joksimovich (Accident Prevention Grp.)*

**The Use of Probabilistic Risk Assessment in Satisfaction of the Nuclear Regulatory Commission's Maintenance Rule**

*R.M. DuBord, M.W. Golay (GE Nuclear Energy); N.C. Rasmussen (MIT)*

**The Beneficial Use of Risk Analysis in the Regulatory Process**

*M.V. Bonaca, D.A. Dube, S.D. Weerakkody (Northeast Utilities Serv.)*

## WHERE DO WE GO FROM HERE IN U.S. NUCLEAR SAFETY REGULATION?

Vojin Joksimovich

Accident Prevention Group  
16980 Via Tazon, Suite 110  
San Diego, CA 92127

### INTRODUCTION

This paper contains excerpts from the APG's Report #28 (Joksimovich, 1993) which was presented to the NRC Staff, ACRS, included into the NRC's Regulatory Review Group Report and presented to many nuclear utilities.

The principle objectives of the report were to: a) Share the concerns about the uncompetitive state of the nuclear industry and b) to search for solutions. The uncompetitive generation costs of the bulk of the nuclear power plants are best illustrated by EPRI (Rahn, 1993).

### A HISTORICAL PERSPECTIVE

The industry worldwide has been preoccupied with the hardware (machine), QA/QC and engineering aspects (assurance of machine), almost to the point of obsession. As a good illustration, in the aftermath of the TMI accident, which was not so much with the hardware as with how the hardware was employed or not employed, thousands of hardware changes were proposed and many, of peripheral and even irrelevant public risk reduction impact, were implemented, costing the rate payers billions of dollars. One of the conclusions of the Kemeny report (Kemeny, 1979) was that the fundamental problems were people-related problems and not equipment problems. The TMI action plan even applied to HTGRs. Nuclear safety expertise was pretty much equated with knowledge of structures, systems and components.

Although the landmark Reactor Safety Study (RSS) or WASH 1400 was completed in 1975 and unambiguously demonstrated that the bulk of risks associated with operation of nuclear power plants (NPPs) were associated with severe accidents, i. e., beyond design basis, a regulatory emphasis on severe accidents was painfully slow to phase in. Until TMI, the findings of the study were practically dismissed by the NRC. Even in the aftermath of TMI, plant-specific PRA studies were only requested for high population sites in order to establish risk significance of some exotic hardware solutions such as core ladles. The utility industry embraced PRAs primarily in order to contest such non-meritorious, expensive backfits, which would have shut down many plants, and certainly the Big Rock Point (BRP). PRA Study (Blanchard, 1985) presents a remarkable display of rationality and transparency, for uses of PRA in the regulatory process. The plant continues to run, and it is planned to run through the year 2000. The NRC's severe accident policy was not promulgated until 1985 and the generic letter for plant-specific PRAs or IPEs was not issued until 1988.

Despite the fact that NPPs now generate in excess of 20% of the nation's electricity, and despite

the fact that PRA is now a mature discipline (with accompanying abuses, of course), we have not been able to sufficiently factor risk perspectives either into nuclear regulation or NPP operations. The industry has not coordinated a concerted effort. Fire drills and immediate "provide what I want to prove" approaches result in replication rather than collaboration. The "compliance mindset" coupled with PRA experts oversell of PRA capabilities, in particular when it comes to validity of bottom line values, resulted in a stalemate.

A smooth transition from traditional design and construction activities to operations has not been made yet. As David Ward has eloquently stated, "When there is a disconnect between what is needed and what we know how to do, the latter wins. A man with a hammer sees everything as a nail." (Ward, 1992).

Plant operations have to be seen as a collection of systems, human actions and process requirements in a highly interactive mode, as opposed to individual rule compliance's or non compliance's. Making this, what appears to be a revolutionary change from binary (OK-Not OK) compliance thinking to a highly interactive systems performance perspective, and its associated reduction in variability's seems to be the underlying cultural hurdle the nuclear industry must overcome.

#### **A Perspective on Status of Nuclear Safety**

One can safely state that there is a general consensus amongst nuclear safety experts that there is more than sufficient hardware in existing NPPs. The plants are well designed to withstand natural phenomena such as earthquakes. In fact, they are over-designed. The Shoreham study (Shoreham, 1985) discovered that, with the exception of ceramic insulators, beyond the control of a NPP, the first component to fail required an earthquake four times safe shutdown earthquake (SSE). Fire protection despite recent thermo lag issue, but in view of Appendix R attention, is adequate. All in all, the existing hardware is good enough suggesting that hardware freeze is appropriate. Only marginal further gains could be made in this area, despite apparent imbalances in the design. Any appreciable gains can only be achieved with advanced designs like ALWRs and HTGRs. Many PRAs/IPEs corroborate this conclusion. Of course, this may not be necessarily true for every single plant in the country, but the existing IPE process should reveal major outstanding design inadequacies.

Since TMI, readiness of operating crews to respond to complex accident scenarios has been greatly enhanced. Simulator training and emergency operating procedures are probably the most instrumental in this success story. However, there is no room for complacency and more needs to be done, not in terms of quantity, but quality of training. Current training demands are excessive. The simulator offers much more before it reaches its full potential.

The measurement techniques developed and applied in EPRI funded projects such as Operator Reliability (ORE) (EPRI NP-6937, 1990) and other projects contain a potential for answering conclusively fundamental safety questions regarding operator readiness, training effectiveness; optimal crew composition on case-by-case basis to safely manage the plant, etc. Regretfully, institutional obstacles and inertia associated with reluctance to accept measurements rather than educated guesses, have thus far prevented wider use of these techniques for both training and PRA/IPE applications. As a result, PRAs/IPEs typically employ generic operator action guesses rather than the simulator data. Paradoxically, ORE style data collection has been completed at the PAKS VVER simulator in Hungary, and is being interpreted for use in the PAKS PRA.

What is not good enough is our understanding of plant operations and operational risks. We are reluctant to apply plant operational risk models capable of simulating NPP risks vs. time, despite existence of the basic technology (Vesely, 1993). The models that we do have show that core damage frequencies (CDF) can undergo large changes over time due to changing plant hardware configurations. Most

dramatically, there appears to be a strong correlation between many high risk configurations and precursor events (Vesely, 1992). The drifts in CDF attributable to human reliability and organizational factors considerations are not even modeled yet. On the other hand, we are aware that essentially a single competent and committed individual in an executive position can make a vast difference in fostering a safety culture, as exemplified at Turkey Point (O'Neill, 1992).

The bottom line is that our understanding of the safety culture, not to mention the nuclear risk culture is inadequate. This should be examined using perspectives derived from analyses of catastrophic accidents (such as Chernobyl, Bhopal, Challenger, Amoco Cadiz, Piper Alpha, Exxon Valdez), which show that these accidents may be characterized by four broad categories of root causes (abbreviated as "4M"):

- Machine (design with its basic flaws)
- Milieux (natural phenomena, operational conditions, political environment, commercial pressures, etc) providing triggering events, and
- Man (operating crew response)
- Management (basic organizational safety culture flaws)

Strong management can minimize the contribution of machine, milieux and man to nuclear operational risks. One way management can have this powerful positive influence is through establishment of a proper safety and risk culture (Joksimovich, 1992).

## REPERCUSSIONS

Rising O&M costs, largely attributable to regulatory requirements and how the utilities have responded to them, are driving the industry right into the ground. A reduction of 20% or so is imperative to keep many plants viable. To quote from the 1989 Regulatory Impact Survey: "NRC so dominates licensee resources through its existing and changing formal and informal requirements that licensees believe that their plants, though not unsafe, would be easier to operate, have better reliability, and may even achieve a higher degree of safety, if licensees were freer to manage their own resources." The nuclear utilities cannot economically compete with fossil fuel plants and other sources of electricity. Permanent shutdowns of Yankee Rowe, San Onofre Unit 1 and Trojan clearly signal the magnitude of the problem. The crisis boils down to an issue of how to maintain or enhance (where it might be appropriate) nuclear safety at sustainable reduced costs in an acceptable regulatory framework. This leads to Risk Based Regulation (RBR) and Integrated Risk Management (IRM).

## RISK BASED REGULATION

RBR, i.e., a compendium of regulatory implementation guides should be explicitly based on risk analyses which are traceable and scrutable. It needs to be, however, pointed out that even if the regulators and licensees were completely competent in the practice, risk quantification is still an art as well as a science, and the general public's lack of appreciation of relative risk concepts is an unfortunate impediment to the pace with which progress can be expected in public understanding. Nonetheless, we can achieve a goal of rational and transparent regulation if we devote appropriate resources to exploiting the full potential of PRA techniques which are by and large currently available, but are only in limited use both by the regulator and the nuclear utilities. Vesely has convincingly illustrated existence of a technology consisting of ten NUREGs (Vesely, 1993) summarizing the work performed over eight years.

Like EPRI-sponsored human reliability technology and IAEA sponsored safety culture literature referred to earlier, this NRC-sponsored technology is virtually untapped.

Regulatory requirements should be distributed according to risk significance. Herschel Specter has illustrated how it could be applied in the maintenance rule case (Specter, 1993). In another paper (Specter, 1992) he illustrated the example of costs associated with various non-safety vs safety related components such as with high ratios such as: \$242.44 vs \$4,447.00; \$29,000 vs \$66,800; \$207.00 vs. \$7,548, \$1.35 vs \$21.12, etc. New York Power Authority paid \$313.00 for a single hex socket set screw which can be bought in a local hardware store.

In addition, I advocate that greater self-reliance and more self-regulation through instillation of enhanced safety and risk culture via advanced self-assessment programs should also be a key ingredient of RBR, which may or may not be a part of the license similar to integrated living schedule, which is a part of BRP's license. A good example for an advanced self-assessment is an integrated risk management program (IRMP).

#### **IRMP**

Risk management is defined as the decision making process to minimize potential losses. Typically, risk management is accomplished by virtue of exercising a risk model of a specific plant and weighing the costs, benefits and risks of available options for achieving risk control. Degree of success is dependent on the quality of the risk model. If the risk model is geared towards the plant hardware aspects only, then its usefulness is confined to identifying plant configuration vulnerabilities, but is not necessarily successful for all plant operational considerations. For the latter, the risk model has to be capable of simulating NPP risks vs. time and be capable of accommodating human reliability and organizational factors, e.g., safety and risk culture.

A number of utilities have developed risk management programs primarily geared to hardware considerations. Hence, I would not call them integrated since they represent a sub optimal case. To my knowledge, Yankee Atomic has probably the most advanced program in the industry (Yankee, 1991). A striking example was the use in closure of NRC's severe accident policy issues, i.e., IPE, IEEE, Containment Performance Improvement (CPI) and Accident Management (AM). Northeast Utilities is another industry leader and a staunch advocate of using living PRA in decision making (Bonaca, 1991).

IRMP's framework and principal elements are described in the above mentioned reference (Joksimovich, 1993)

The utilities cannot successfully manage nuclear risks independent of common business issues. It is imperative that a more holistic view of plant management responsibility be seen. Land and Sancic's paper (Land, 1990) reflects realities of plant decision making. Plant managers must successfully balance public safety, personnel safety, economic performance, personnel productivity and regulatory impact. The scope of IRMP takes this imperative to account.

#### **Corollary - Ten Assertions**

1. No other industry has invested more resources in public safety than the nuclear industry. O&M costs largely attributable to regulatory requirements and how the utilities have responded to them, have escalated to unacceptable levels and are driving competitiveness of nuclear utilities right into the ground. Long-term sustainable and cost reductions are imperative for saving the nuclear option.
2. For this large investment, the industry has achieved a remarkable safety record. Nevertheless, there is no room for complacency; the level of safety achieved has to be maintained and continuously looked to be enhanced.

3. The nuclear industry worldwide has been preoccupied with the hardware to the point of obsession. TMI action plan alone resulted in thousands of hardware changes costing the rate payers billions of dollars. As a result, existing hardware is good enough and hardware freeze is appropriate.
4. Since TMI, readiness of operating crews to respond to complex accident scenarios has been greatly enhanced. Simulator training and emergency operating procedures are probably the most instrumental. However, more needs to be done, not in terms of quantity, but quality of training. The simulator offers much more before it reaches its full potential.
5. With almost all NPPs operational, the emphasis has to shift from traditional engineering considerations into entirely operational ones. In order to maintain and enhance the existing level of safety, our understanding of operational risks has to be vastly expanded. Plant operations have to be seen as a collection of systems, human actions and process requirements in a highly interactive mode which requires a cultural change in the industry. The "4M" aspects, discussed briefly in this paper, should receive due attention. Core damage frequencies can undergo large changes over time due to changing plant hardware configurations, human reliability and organizational factors.
6. Full benefits should be derived from currently under-utilized and sufficiently in-depth researched disciplines such as PRA in both integral and time-dependent mode, human reliability and safety and risk culture.
7. Risk-based regulation and risk management, as advocated in this paper, is an answer. Greater self reliance and more self regulation through instillation of enhanced safety and risk culture via advanced self assessment programs should be key ingredients. A good example for an advanced self assessment program is the Integrated Risk Management (IRMP).
8. Risk technology applications as proposed by the NRC's Regulatory Review Group represent a step in the right direction. Subsequently, the NRC should gear up its resources to respond expeditiously to nuclear utility initiatives. Furthermore, a regulatory culture reform will be needed to reflect some points made above.
9. Regulatory culture reform should address two fundamental issues: the proper role of the regulator, i.e., cooperative, like in many European countries vs. competitive, and change of binary (OK/Not OK) compliance thinking to a highly interactive systems performance perspective and its associated reduction in variability's.
10. A massive instillation of risk education in the whole industry via management and personnel training has to be initiated, and the sooner the better. In addition, rule-based culture has to be substituted with knowledge-based culture. Regulatory and utility-sponsored research must continue with emphasis on the human and organizational factors in particular.

## REFERENCES

- [Blanchard, 1985] Blanchard, D., "PRA and Regulation", USIR/NRR Seminar, September, 1985.
- [Bonaca, 1991] Bonaca, M.V., Editor, Living Probabilistic Safety Assessment for Nuclear Power Plant Safety Management, NEA, 1991.
- [EPRI NP-6937 1990] Spurgin, A.J., et al., "Operator Reliability Approach Using Power plant Simulators, Volumes 1, 2 and 3, EPRI NP-6937 and EPRI NP-6937L, Electric Power Research Institute, Palo Alto, CA, 1990 and 1991.
- [Joksimovich, 1992] Joksimovich, V., "Safety Culture in Nuclear Utility Operations", 1992 IEEE Fifth Conference on Human Factors and Power Plants, Monterey, CA, June 1992.
- [Joksimovich, 1993] Joksimovich, V. "Where Do We go From Here In US Nuclear Safety Regulation? A Personal Perspective," APG Report #28, June 1993.
- [Kemeny, 1979] Kemeny, "The Need for Change: The Legacy of TMI", October 1979.
- [Land, 1990] Land, R.E., and Sancic, D., "Value Ranking System for Nuclear Plant Modifications", Nuclear Plant Journal, Sep-Oct 1990.
- [O'Neill, 1992] O'Neill, "Thanksgiving at Turkey Point, Nuclear Industry, Third Quarter 1992.
- [Rahn, 1993] Braun, C, Ziegler, E.J. Rahn, F.J. "O&M Cost Reduction Due to Application of Risk Based Regulation - Top Level Estimate: ANS
- [Specter, 1993] Specter, H., "PSA, Calculus and Nuclear Regulation", PSA '93, Clearwater, FL, January 1993.
- [Specter, 1992] Specter, H, "Shifting the Regulatory Paradigm", NYPA, 1992.
- [Shoreham, 1985] Joksimovich, V. and Orvis, D.D., "Major Common-Cause Initiating Events Study -- Shoreham Nuclear Power Station", February, 1985.
- [Vesely, 1992] Vesely, W., Private Communication
- [Vesely, 1993] Vesely, W. "Risk-Based Regulation and Risk-Based Aging Management", The Second International Conference on Nuclear Engineering, San Francisco, CA, March, 1993.
- [Ward, 1992] Ward, D., "Do We Need Advanced Humans?", Remarks at conference luncheon, 1992 IEEE Fifth Conference on Human Factors and Power Plants, Monterey, CA, June 1992.
- [Yankee, 1991] Yankee Atomic Electric Company, "Applications of Probabilistic Risk Assessment" EPRI NP-7315, Electric Power Research Institute, Palo Alto, CA, 19914.



## **THE USE OF PROBABILISTIC RISK ASSESSMENT IN SATISFACTION OF THE NUCLEAR REGULATORY COMMISSION'S MAINTENANCE RULE**

Renée M. DuBord,<sup>1</sup> Michael W. Golay,<sup>2</sup> Norman C. Rasmussen<sup>2</sup>

<sup>1</sup>GE Nuclear Energy, San Jose, CA 95125

<sup>2</sup>Massachusetts Institute of Technology, Cambridge, MA 02139

The research was performed under appointment to the Nuclear Engineering/Health Physics Fellowship program administered by Oak Ridge Institute for Science and Education for the U.S. Department of Energy.

### **INTRODUCTION**

Maintenance and inspection at nuclear power plants consumes a large portion of a utility's resources, making resource allocation for such procedures vital. The NRC's Maintenance Rule, due to be implemented in July of 1996, requires utilities to select systems, structures, and components (SSCs) important to safety and to develop a monitoring program to ensure that these SSCs are capable of fulfilling their intended functions.

In light of these concerns, two ratios were developed to compare the risk significance of individual components with the amount of plant staff time, or burden, associated with inspecting the component. These risk/burden ratios point out existing disparities between current inspection practices and safety concerns. These ratios can be used to develop new inspection schedules constituting a more equitable risk to burden distribution.

The New York Power Authority's Fitzpatrick plant (Ref. 2-4) was used as an example for this study. The Fitzpatrick IPE was used to select two systems for examination in order to illustrate the relationship between risk significance and surveillance practices. Safety significance can be ranked by minimum cutset frequencies, risk reduction importances (RRIs), or risk increase importances (RIIs). The risk reduction importance (RRI) is a measure of the decrease in the value of the CDF that occurs if the basic event (component failure in this case) is eliminated by setting its probability of occurrence equal to zero. Risk increase importance (RII) is a measure of the increase in the value of the CDF that occurs if the probability of the basic event is set to unity. One risk significant and one risk insignificant system were examined to illustrate the differing surveillance needs

between the two. In this study only the events leading to core damage were investigated. A level 2 analysis would be necessary to identify less obvious SSCs.

The emergency service water (ESW) system was selected as the example risk significant system for several reasons. First, the ESW system components have very high cutset frequencies, meaning the system is extremely pervasive and comes into play in many of the core damage frequency (CDF) dominant scenarios. The system's components also have very high risk reduction importances: of the fifteen highest RRI's, eight of them involve components in the ESW system. NYPA performed a sensitivity analysis on the change in CDF when an entire system's unavailability is changed. A doubling of the ESW system's unavailability led to an approximately 130 percent increase in the CDF, much higher than that of the other systems investigated.

The core spray system, designated as LCS (Low Pressure Core Spray System) was selected as the example risk insignificant system. Only four basic events involving LCS are present in the set of the CDF cutsets, and each occurs only three times in the set of all CDF cutsets. The four LCS basic events have a total RRI of only  $3.2\text{E-}9$ , whereas the top four ESW basic events have a total RRI of  $7.18\text{E-}7$ . The ESW and LCS systems also serve as good comparisons because both have straightforward configurations and both contain similar components known to require maintenance.

## TESTING AND SURVEILLANCE REQUIREMENTS

In order to assess the inspection needs of a system, the dependent components in the system must be separated by the amount of surveillance and testing that they require. Individual system components that show up as high in risk reduction importance can derive the most benefit from a strong testing and surveillance program. Conversely, components with low risk increase importance values become candidates for reduced testing and surveillance, since overall plant risk, as measured by CDF, should not increase if a risk insignificant component is allowed to run to failure before undergoing repair. However, it is important to compare the benefits gained from testing procedures to the possibly increased system unavailability that such testing may cause.

Several things should be looked at to assess surveillance requirements, including: inspection schedules, routine repair and preventive maintenance schedules, special attention paid to certain components, required recalibration, required system realignment, and scheduled tests. It is important to note that other considerations, such as maintaining high operational availability, may also modify the policy actually applied.

Both the ESW and LCS systems have scheduled tests and surveillances. Because of the safety functions of each of these systems, most time-consuming intrusive preventive maintenance is performed only while the reactor is not operating at full power. Maintenance performed while the reactor is not at full power was not considered in the Fitzpatrick IPE as contributing to system unavailability, and is not considered in this study. Furthermore, it is important to differentiate between the amount of effort expended to ensure the reliability of a system, and effort that is required to keep the system operable. Certain components may be designed for a finite lifetime, after which they require either reworking or replacement. This type of work is a necessity and is not subject to change resulting from competition for resources. However, much of the time and effort expended upon a system is devoted to ensuring the reliability of the system, and to catching unexpected system failures. This is the type of time burden that is of interest here. It is reasonable to link the degree of reliability desired to the risk significance of the system.

## ESW AND LCS RESOURCE ALLOCATION PER COMPONENT

It is necessary to measure in a quantitative way the amount of available plant resources expended on different systems. Such a measure is hard to quantify accurately with the available plant data. This is because only routine surveillance and testing work can be easily accounted for, as it is difficult to estimate the amount of effort expended on individual components during the additional testing that corrective maintenance might require. There is very little plant data available regarding such unanticipated work. However, from a knowledge of routine plant procedures an estimate can be made as to the amount of effort expended per system, which can then be extrapolated to individual components.

The staff time burden evaluated here deals only with testing and surveillance procedures that are performed to ensure system reliability. Routine preventive maintenance required to maintain the basic operation of system components was not included. Of course, in the two example systems selected very little preventive maintenance is required because both of the systems are of the standby type, designed for high reliability.

From a detailed study of the routine ESW and LCS system procedures an estimate of the amount of time expended per component can be derived. First, each procedure was reviewed to determine which components were tested or inspected during the procedure. Two different actions were each considered to constitute a test: that of forcing a required response to occur or of perturbing a component in order to produce a system alignment which would permit a test. Forcing a required action to occur involves cycling (opening and closing) a valve, or simulating a signal to turn on a pump. However, some tests require having a system in a certain configuration, usually involving isolating part of the system. Perturbing a valve setting in order to create a desired system test configuration and then returning the valve to its original state after the procedure is also considered to constitute a component test.

An estimate of the number of workerhours required is difficult to obtain. The Fitzpatrick Nuclear Power Plant staff generally does not keep data on workerhours expended per system or per procedure. Furthermore, the actual start and finish times for each procedure may not be representative of the actual amount of time spent working on the system. During outages when the system is not required to be on-line, a system may not be worked on continuously due to the increased resource demands elsewhere.

In conjunction with Mr. K. Vehstedt, Senior Engineer at NYPA (Ref. 5), estimates have been developed for the amount of effort, or burden, required by each procedure. These time estimates were then broken down by component. The time per test is multiplied by the procedure frequency to obtain the total time expended per 18 month plant refueling cycle. It should be emphasized that the values shown are only estimates. A plant program to record the amounts of time expended in actual procedures would be required to attain more accurate numbers. However, an estimate is sufficient to illustrate the methodology presented here. The final time burden results for the ESW system RRI's are given in Table 1. Calculations relating to the LCS ratios have not been included to conserve space.

## RISK/BURDEN RATIOS

In order to measure whether current testing and surveillance procedures are well balanced with regard to the risk significance of the system to which they apply, ratios of the staff time burden to the component's risk reduction and risk increase importances were

calculated for each significant component in the ESW and LCS systems. By comparing the ratios corresponding to different components, disparities between risk significance and the staff time expended while inspecting various components will become evident. These ratios should also be calculated using each component's percent of core damage frequency (Fussell-Vesely index), but this data is currently unavailable from NYPA.

Several of the more important components have more than one basic event associated with them, corresponding to different failure modes. For these components the total risk reduction or risk increase importance is the sum of all the possible different failure modes. This sum was used to calculate the final risk/burden ratios. In this way all possible modes of failure of a component are accounted for in the final ratios.

The final RRI versus time burden ratios for the ESW and LCS systems are shown in Figures 1 and 2. Ideally, these ratios should be reasonably constant from component to component and from system to system. An equitable risk/burden ratio distribution would produce a uniform circle. However, as can be seen from the disparity between the ratios for the ESW system and the LCS system, and even between components within each system, this is currently not the case. These ratios present a quantitative way to measure whether surveillance practices are reasonable with respect to the risk significance of the system, and could be used to reorganize surveillance schedules on a risk importance basis.

From a risk standpoint, the best use of plant resources should lead to a relatively uniform distribution of risk/burden ratios. In order to smooth the ratios between the different ESW system components, and between the ESW and LCS system, a new maintenance and surveillance schedule should be developed that focuses more on those components with high values of the risk/burden ratio. This group would include the ESW pumps, ESW MOV 102, and the ESW manual valve 3. The information embodied in these ratios also provide justification for decreasing surveillance on the LCS system in general, and increasing surveillance on the ESW system.

All of these actions might seem to be obviously required from inspection of the risk significance of these two systems and examination of the cutsets relating to ESW system failure. However, when dealing with other plant systems having less pronounced differences in risk significance, the risk/burden ratios may point out more subtle relationships between the systems. A full analysis of all of the plant safety systems would be necessary in order to establish reasonable values of the risk/burden ratios to use as goals in allocating resources for surveillance and maintenance procedures.

It is hoped that these ratios could play a part in developing a maintenance and inspection program designed to satisfy the NRC's Maintenance Rule. However, there are uncertainties present in these ratios that must be taken into account. The PRA techniques used to rank system and components from a safety standpoint are associated with numerous uncertainties, and there has been considerable regulatory reluctance in the past to use PRA data in a quantitative way. In addition, accurate data regarding the staff time expended on individual procedures is not available. Studies should be done in this area in order to gain a more accurate picture of where plant resources are being spent.

When developing a plant-wide inspection schedule, considerations other than risk must be taken into account. Plant operating criteria must also be considered, as steady, consistent operations are also a vital part of proper resource allocation. However, the risk/burden ratios do represent both a departure from past inspection scheduling practices and an important criteria to consider when developing more efficient schedules.

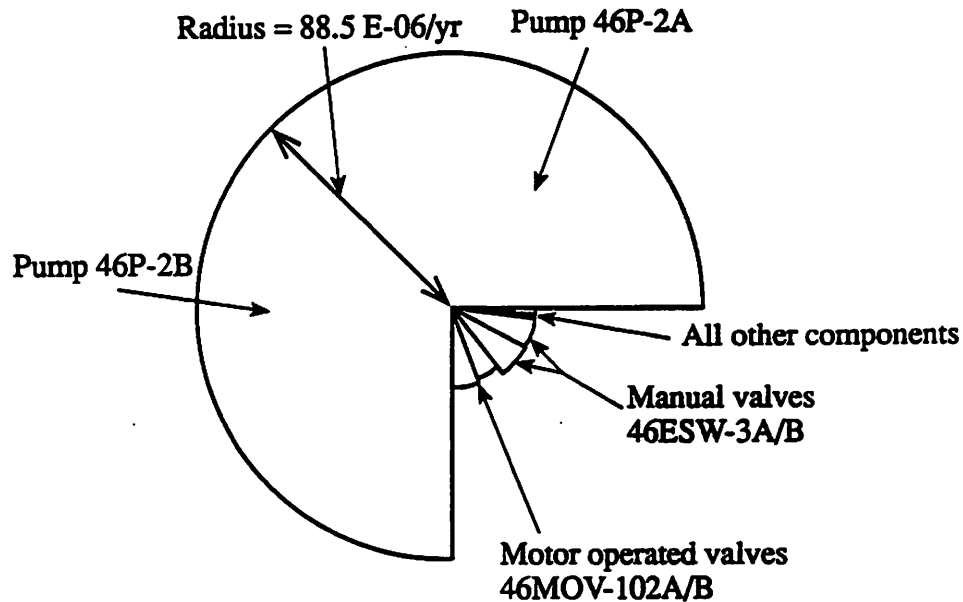
TABLE 1

**ESW SYSTEM COMPONENT RISK REDUCTION IMPORTANCE VERSUS  
TIME BURDEN**

Component	Related Basic Event	$\Sigma$ Risk Reduction Importance ( $\text{yr}^{-1}$ ) (summation over all failure modes)	18 Month Time Burden All Procedures - hours (Time Burden $\text{yr/yr}$ )	$\Sigma$ (RRI) Time Burden ( $\text{E-06 yr}^{-1}$ )
46P-2A pumps	ESW-CCF-FR-PUMPS ESW-MCP-FR-P2A ESW-CCF-FS-PUMPS ESW-RCK-NO-P2A ESW-XHE-RE-P2A ESW-MDP-FS-P2A  All Events	1.78E-07 1.48E-07 9.76E-08 3.36E-08 1.73E-08 2.98E-09  4.77E-07	31.5 (5.39E-03)	88.5
46P-2B pump	ESW-CCF-FR-PUMPS ESW-MDP-FR-P2A ESW-CCF-FS-PUMPS ESW-RCK-NO-P2A ESW-XHE-RE-P2A ESW-MDP-FS-P2A  All Events	1.78E-07 1.41E-07 5.76E-08 3.09E-08 1.57E-08 2.61E-09  4.66E-07	31.5 (5.39E-03)	86.46
46MOV-102A motor op. valve	ESW-RCK-NO-102A ESW-CCF-OO-102AB ESW-MOV-OO-102A  All Events	3.36E-08 1.64E-08 4.39E-09  5.44E-08	13.5 (2.31E-03)	23.55
46MOV-102B motor op. valve	ESW-RCK-NO-102B ESW-CCF-OO-102AB ESW-MOV-OO-102B  All Events	3.09E-08 1.64E-08 3.82E-09  5.11E-08	13.5 (2.31E-03)	22.12
46MOV-101A/B motor op. valve	minimum importance*	4.57E-11*	7.5 (1.28E-03)	0.036
15MOV-175A/B motor op. valve	minimum importance*	4.57E-11*	7.5 (1.28E-03)	0.036
46ESW-3A manual valve	ESW-XHE-RE-ESW3A ESW-XVM-PQ-ESW3B  All Events	9.64E-08 6.92E-10  9.71E-08	24 (4.11E-03)	23.63
46ESW-3B manual valve	ESW-XHE-RE-ESW3B ESW-XVM-PF-ESW3B  All Events	8.95E-08 3.90E-10  9.01E-08	24 (4.11E-03)	21.92
46ESW-10A/B manual valve	minimum importance*	4.57E-11*	3 (0.51E-03)	0.089
46ESW-23 manual valve	minimum importance*	4.57E-11*	3 (0.51E-03)	0.089
46ESW-30B manual valve	minimum importance*	4.57E-11*	3 (0.51E-03)	0.089
46ESW-1A check valve	ESW-CKV-CC-ESW1A	2.18E-09	18 (3.08E-03)	0.71
46ESW-1B check valve	ESW-CKV-CC-ESW1B	1.86E-09	18 (3.08E-03)	0.6
46ESW-6A check valve	ESW-CKV-CC-ESW6A	2.18E-09	18 (3.08E-03)	0.71
46ESW-6B check valve	ESW-CKV-CC-ESW6B	1.86E-09	18 (3.08E-03)	0.6
42C-1ESWA03 relay	ESW-RCI-FE-A42C	3.13E-09	3 (0.51E-03)	6.1
42C-1ESWB04 relay	ESW-RCI-FE-B42C	2.74E-09	3 (0.51E-03)	3.34
63A-1ESWA04 HFA relay	ESW-RCS-OO-A63A9 ESW-RCS-FE-A63A  All Events	8.04E-09 3.13E-09  1.12E-08	3 (0.51E-03)	21.82
63A-1ESWB04 HFA relay	ESW-RCS-OO-B63A9 ESW-RCS-FE-B63A  All Events	7.13E-09 2.74E-09  9.87E-09	3 (0.51E-03)	19.23
15PS- 122A/B/C/D Pressure sensor	minimum importance*	4.57E-11*	6 (1.03E-03)	0.046

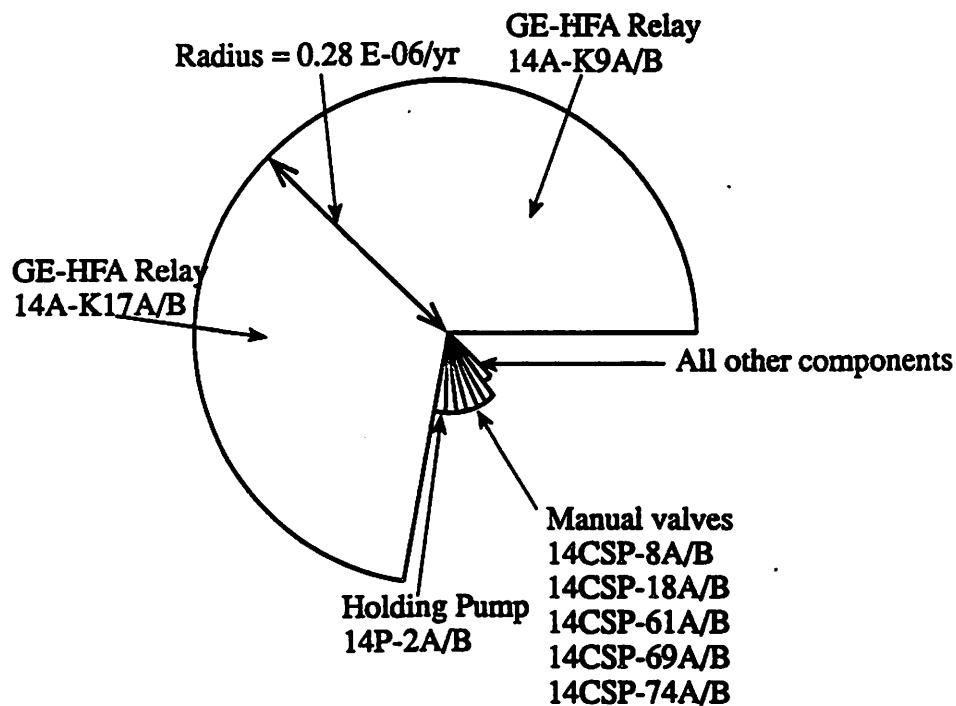
\* Basic event involving the component is not important enough to show up in Fitzpatrick's sensitivity studies. The smallest risk reduction importance value that does show up in the study was used, as this would represent a maximum value for any less-important RRI.

**FIGURE 1**  
**DISTRIBUTION BY COMPONENT OF THE ESW SYSTEM RATIO**  
**OF RISK REDUCTION IMPORTANCE TO TIME BURDEN**



The subtended angle is the component's percentage of total RRI associated with the system.  
 The radius is the component's RRI/Time Burden Ratio.

**FIGURE 2**  
**DISTRIBUTION BY COMPONENT OF THE LCS SYSTEM RATIO**  
**OF RISK REDUCTION IMPORTANCE TO TIME BURDEN**



The subtended angle is the component's percentage of total RRI associated with the system.  
 The radius is the component's RRI/Time Burden Ratio.

## REFERENCES

1. R.M. DuBord. "The Use of Probabilistic Risk Assessment in Satisfaction of the Nuclear Regulatory Commission's Maintenance Rule," Massachusetts Institute of Technology Nuclear Engineering Department MS/BS thesis, Cambridge, MA (May 1993).
2. New York Power Authority. "James A. Fitzpatrick Nuclear Power Plant Individual Plant Examination. Vol. 1 & 2," White Plains, NY (August 1991).
3. NYPA JAF Nuclear Power Plant. "Operations Surveillance Test Procedures:
  - ST-3A Core Spray Pump and Valve Operability Test
  - ST-3B Core Spray Simulated Automatic Actuation
  - ST-9B EDG Full Load Test and ESW Pump Operability Test
  - ST-8D ESW Pump Flow Rate Test
  - ST-8E ESW Logic System Functional Test and Simulated Automatic Actuation Test
  - ST-3J Core Spray Initiation Logic Functional Test
  - ST-1R Reactor Building Closed Loop Cooling Containment Isolation AOV Exercise".
4. NYPA JAF Nuclear Power Plant. "Instrument Surveillance Procedures:
  - ISP-23 Emergency Service Water Lockout Matrix Instrument Functional Test/Calibration
  - ISP-175A Reactor and Containment Cooling Instrument Functional Test/Calibration
  - ISP-275A Reactor Pressure (ECCS) Transmitter Calibration and Channel Functional Test
  - ISP-276A Reactor Level (ECCS) Transmitter Calibration and Channel Functional Test".
5. K.J. Vehstedt, Private communication, New York Power Authority, White Plains, NY (1993).

## THE BENEFICIAL USE OF RISK ANALYSIS IN THE REGULATORY PROCESS

M. V. Bonaca, D. A. Dube, S. D. Weerakkody

Northeast Utilities Service Company  
P. O. Box 270  
Hartford, Connecticut 06141  
U.S.A.

### INTRODUCTION

Over the past several years, we have witnessed an increasing number of varied applications of risk technology in support of nuclear power plant management. The multiple examples documented in the literature demonstrate successful application in almost every area of operation and engineering support, well beyond the identification of plant vulnerabilities which has, traditionally, been the first and often only use of nuclear plant PSAs.

To date, the success of risk analysis in modifying or eliminating current regulatory requirements shown to be unnecessary has been uneven. Some pioneering programs, such as the Northeast Utilities ISAP, which dates back to 1985, represent early application of PSA in the regulatory process. But in general, the regulatory use of PSA has been focused on identification and elimination of plant vulnerabilities, and on developing the insights necessary to develop and support a severe accident management program.

The recent initiative of the Regulatory Review Group on Risk Technology Application opens a new era for the use of PSA in regulatory applications. PSA uses are being encouraged that relax or eliminate unnecessary requirements, or support a "graded" approach to implementation of regulatory requirements. ISAP represents a precursor to the use of PSA for this purpose and provides valuable examples of successful applications.

The benefits of the NRC initiative to the industry are commensurate with the depth and quality of the supporting PSA program, which provides the bases for the proposed modification of compliance. But since even the simplest IPE may be capable of supporting initiatives to relax regulatory requirements, the future focus of PSA programs may be on the potential short term payback from existing programs, limited though they may be. This could actually prevent further development of living PSA programs, with the resulting loss



of the benefits such programs can provide. The experience of Northeast Utilities with PSA technology shows that it pays to develop a living PSA program, capable of supporting effective applications in the regulatory area.

Furthermore, without established industry standards of application, this narrow use of the technology may lead to inadvertent abuses and loss of credibility. The known limitations of PSA require careful use and sound expertise to support credible applications. Therefore, it is essential, at this juncture, that the industry take proactive initiatives to develop standards of application and to build the credibility of PSA by avoiding abuses and pursuing uses that do not degrade, but enhance safety.

#### INTEGRATED SAFETY ASSESSMENT PROGRAM (ISAP)

Northeast Utilities has successfully implemented the Integrated Safety Assessment Program (ISAP) at three of its operating nuclear units, with plans to expand the application to all units. The Integrated Implementation Schedule, an important element of ISAP, is a license condition at the Connecticut Yankee and Millstone Unit #1 nuclear power plants. Through ISAP, NU has evaluated the costs and benefits of several hundred major projects at the nuclear units, and successfully implemented utility-initiated improvements and regulatory-driven backfits on a prioritized basis. Under ISAP, key design changes initiated by NU to address severe accident vulnerability concerns have been given high priority, as is appropriate. Several regulatory driven modifications to address fire protection/Appendix R also were placed on fast-track for implementation based on the calculated high benefit. However, many backfits have been assigned lower priority and extended implementation schedules based on the assessed low safety benefit and/or high cost.

Recently, the NRC staff provided a safety evaluation addressing the acceptability of deviations from the requirements of the General Design Criteria (GDC) for the containment isolation system at Connecticut Yankee (Ref. 1). NU, on behalf of the Haddam Neck Plant, provided deterministic as well as probabilistic based analyses as to how the containment penetrations met the intent of the GDCs, and how further design modifications would be marginal to safety. Altogether, some 39 penetrations were evaluated. The NRC staff concluded that "for most of the penetrations, the valve configuration does meet the intent of the GDCs 54 through 57. In addition, based on the low risk indicated by the licensee's PSA studies, the staff agrees that conformance with the GDCs 54 through 57 would provide minimal safety improvement to the plant." Only two penetrations will require further modification, and those changes are modest (providing a blank flange during operating modes 1 through 4).

Needless to say, the potential costs of meeting not only the intent, but the full letter of the GDCs, would have been in the multi-millions of dollars.

Also recently, NU submitted a probabilistic analysis under ISAP which concluded that the overall benefit to public health and safety from the installation of a redundant containment hydrogen monitor system at Millstone Unit #1 was minimal. Core damage frequency reduction of  $4.5 \text{ E-7}$  per year and risk reduction of less than 2 man-rem per year were assessed. The NRC staff accepted the deterministic and probabilistic analyses performed by NU, and granted relief from regulatory requirements in their safety evaluation (Ref. 2).

The potential cost of installing a redundant containment hydrogen monitor would be in excess of 2 million dollars, including power supplies and meeting electrical cable separation requirements.

#### NEED FOR STANDARDS IN PSA APPLICATIONS

While the applications of PSA have expanded to important areas in plant risk management over the past several years, the PSA application technology has not grown rapidly enough to provide sound scientific basis for PSA based conclusions in these new areas. That is, even for crucial applications, there is potential for subjectivity and ambiguity in PSA based conclusions. Although rapid advances have been made in computer software and hardware that support the PSA technology, the major impact of those advances has been the capability to execute the PSA models extremely quickly to allow timely inputs to plant operational issues. Some fundamental weaknesses of PSA technology that are relatively difficult or impossible to grasp using quantifications or computers are yet to be adequately addressed.

A major weakness in the PSA application area is lack of a scientific method to recover the impact of crucial risk related information which gets lost as a result of the major assumptions, approximations, and limitations on scope of PSA models. At present, there are no standards or proven methods to recover the impact of crucial risk related information which may have a significant bearing on the PSA based conclusion. As a result, PSA based conclusions are viewed with caution, and suspicion at best, not only by discipline experts outside of PSA, but also by different segments of the PSA community. In light of the above, standards are needed to guarantee proper application of PSA methods in order to preserve the long-term credibility of PSA technology.

One standard application method that fits all PSA application cases is nearly impossible to generate due to the wide spectrum of approaches that a PSA analyst has to choose from. For example, quantifications may have been performed using hand calculations, personal computer based PSA models, or using engineering judgement. The best quantification method will depend upon characteristics such as level of detail of PSA model, mode of operation impacted (shutdown or power), type of plant response impacted (internal event or external event initiator).

Therefore, to assure accuracy and reasonableness of PSA based decision making, standards or guidance must be generated using a philosophy that recognizes that:

- o Expertise in PSA is knowledge-based in that cumulative knowledge in many areas is needed to derive accurate PRA insights.
- o The key areas of that knowledge base are expertise in PSA techniques, expertise in overall plant operation, and familiarity with all intimate details of the PSA model such as assumptions, approximations, and truncation values.
- o State of the art has not grown to a point where the above expertise can be structured and computerized.

Considering the current state of technology, the above philosophy can be implemented by bringing together people with the above key areas of expertise to perform brain-storming sessions. During the brainstorming session(s), which may be called "formulation of problem" phase of the application, the following problem attributes should be decided upon:

- o What are the major assumptions and approximations that can impact the risk evaluation and how can that impact be recovered into the analysis?
- o What risk elements (initiators, systems, operator actions, containment features) are impacted?
- o Is the PSA model on PC detailed enough to perform calculations to support the particular application?
- o What type of calculations will be necessary?
- o Is generic data adequate or is plant specific data necessary? Should additional data sources be revisited?
- o Do known PSA methodology limitations have a major impact on the result? For example, during some applications, over-estimated common cause failure rates or assumptions regarding constant failure rate for standby components lead to overly conservative or non-conservative conclusions.
- o What are the anticipated results? (Forming an opinion on the expected results based on engineering judgment helps to highlight the assumptions that must be revisited during PSA quantifications).

Guidelines or standards would be an effective way to assure that the PSA based decision process completely addresses the above issues.

In addition to standards on what to consider in PSA applications, standards are needed to address: (a) the level of quality assurance in the evaluation, (b) the documentation of the assessment, (c) the consistent treatment of operator recovery actions, (d) uncertainty analysis, or sensitivity analyses and (e) the criteria for acceptable risk or core melt frequency determination.

In short, the process of performing risk-based assessments is as important as the content of the assessment itself, and these should be addressed in standards.

#### BENEFITS OF LIVING PSA ON PLANT SAFETY

Currently, NU maintains "living" level 2 PSAs for four nuclear power plants. A living PSA means not only to maintain the PSA current with the plant design and operational experience, but to also use it as an integral part of the design change process and overall risk management (Ref. 3). The goal that NU has set forth, which has been achieved for nearly all the units, is to have an updated PSA model within six months. Such a goal can be resource intensive, requiring nearly one full-time equivalent staff member per plant to update the models and reliability data. These requirements are exclusive of staff necessary for PSA applications.

Through the living PSA process, NU has pursued a process of continuous improvement in the reliability of key plant systems and components. In essence, results of the PSA have been fed back into the design and operations of each nuclear unit.

For example, the Millstone Unit #1 PSA found the failure of the emergency gas turbine generator to be the single most contributor to core melt frequency. The reason for this high importance was, in fact, due to the relatively low reliability of the gas turbine. Subsequently, a detailed reliability analysis performed by the in-house PSA organization identified improvements in the speed control unit as the most cost-effective measure. Since implementation of the design change, measurable increase in reliability of the gas turbine has been observed, as tracked by the living PSA program. The consequence is a continued improvement in overall safety as measured by the projected core melt frequency (CMF).

Similarly, NU has had an extensive program of safety improvements at its Connecticut Yankee plant. Several dozen design changes motivated primarily to address severe accident vulnerabilities and reduce the core melt frequency have been implemented.

Table 1 illustrates the dramatic improvement in plant safety as measured by the CMF for internal events. The nearly 10-fold decrease came at relatively modest expense in comparison to regulatory-driven requirements which, if fully implemented, would have had a marginal effect on CMF. Similar improvements in CMF for external events, such as fire, have also been observed.

TABLE 1

## Results of Safety Improvements at Connecticut Yankee

	<u>CMF (internal events)</u>
Prior to implementation of immediate corrections, 1985-1986	1 E-3 / yr. (est.)
As published in the Probabilistic Safety Study, 1986 (did not credit interim ECCS modifications to address small-LOCA vulnerability)	5.5 E-4
With interim measures to address small-LOCA vulnerability	4 E-4
Following implementation of single failure modifications, 1989	3.25 E-4
IPE report, 1993 (Following completion of new switchgear building, AFW improvements, improved plant operations, enhanced operator training, and other initiatives)	1.8 E-4
Following Cycle 17 Refueling Outage (electrical separation mods, 120 V vital AC buses A and B, MCC-5 ABT testing)	1.3 E-4 (est.)

REFERENCES

1. Letter from A. Wang (NRC) to J. F. Opeka, Haddam Neck Plant - Systematic Evaluation Topic V1-4, "Containment Isolation System", (TAC No. M51935), Docket No. 50-213, dated July 26, 1993
2. Letter from J. W. Andersen (NRC) to J. F. Opeka, Millstone Nuclear Power Station, Unit 1 - NUREG-0737, TMI Action Plan Item II.F.1.6, Post-Accident Hydrogen Monitors (TAC No. M83986), Docket No. 50-245, dated September 7, 1993
3. Living Probabilistic Safety Assessment for Nuclear Power Plant Management - Nuclear Energy Agency, OECD, 1992

## **104 Industrial Risk Management - An EEC Perspective**

*Chair: D.M. Karydas, Factory Mutual Res. Corp.*

**Industrial Risk Management: An EEC Perspective**

*A. Amendola (CEC-JRC, Ispra)*

**Plant Level Hazard Identification Based on Functional Models**

*J. Suokas (VTT, Finland)*

**Decision Making in Process Design - Assessment of Total Safety by Aggregating the Safeties of the Subparts of the Process**

*R. Koivisto (VTT, Finland), V.J. Pohjola, M.K. Alha (U. Oulu, Finland)*

**Short Cut Risk Assessment**

*G. Wells (U. Sheffield, UK); S. Allum (Bowring Marsh & McLennan, UK)*

## **INDUSTRIAL RISK MANAGEMENT: A EEC PERSPECTIVE**

Aniello Amendola

Commission of the European Communities  
JRC-ISEI  
21020 Ispra (Va), Italy

### **INTRODUCTION**

The paper describes the new trends of the EEC regulation to control the risk of major accident in the process industry. After the experience of the first ten years of application, the so-called Seveso<sup>1,2</sup> Directive is being revised. The proposal presently under discussion includes provisions for land use planning with respects to accident hazards; for "whole site" safety assessment instead of focusing on single installations; and for the adoption by the site operator of safety management systems (SMS), as the underlying causes of most of the accidents notified to the EEC Commission have been provoked by management faults<sup>3,4</sup>.

A broader perspective is therefore being established as far as risk management of storing/processing dangerous substances is concerned: a perspective which on the one hand involves society as a whole, and on the other hands goes a step forwards towards incentives for a better environmental management.

### **PRINCIPLES OF THE CONTROL OF MAJOR ACCIDENT HAZARDS WITHIN EEC**

Risk management is the process which is established to control the risk and its implementation. At its highest level it is a social process. The "Seveso" Directive and its amendments<sup>5,6</sup> identify the relevant parties: public authorities, industry and public.

The major accidents that stressed the need for a Directive regulating hazardous industry (e.g. Seveso, Flixborough) had in common the features that local authorities did not know what chemicals were involved and in what quantities; they did not know enough about the processes to understand what chemicals/energy could be produced or released under accident conditions; and there was a lack of planning for emergencies. With this background, the Directive is largely concerned with the generation and the control of a correct information flow among the different actors in the risk management procedure. It applies to industrial activities involving process

or storage of substances capable in the case of an accident to provoke major toxic releases or fire & explosion events. Nature and inventories of such substances are specified according to classes or nominal lists.

The principal requirements of the Directive can be summarised as follows:

- Each Member State must appoint a Competent Authority (CA);
- At any time the manufacturer shall prove to the CA that major hazards connected with the installation have been identified and adequate safety measures have been taken to prevent accidents;
- When dangerous substance inventories exceed specified thresholds, the manufacturer shall provide the competent authority with a written safety notification (which has been more or less identified with the obligation for safety reports) on the installation hazards, shall prepare an internal emergency plan, and give the information needed by the CA for the preparation of off-site emergency plans;
- Major modifications shall be notified to the CA;
- CA shall provide for external emergency planning;
- Member States shall ensure that people liable to be affected by an accident be 'actively' informed of the safety measures and how to behave in the event of an accident;
- The manufacturer shall report to the CA any major accident which occurs, the national authorities should notify major accidents to the Commission;
- The Commission shall keep a register of accidents so that Member States can benefit from this experience for prevention purposes.

After the implementation experience, the principles on which its revision is being based stress the socio-organisational aspects of the control policy, as discussed in the following.

Firstly, the concept of "site" (characterised by the presence of dangerous substances) is introduced instead of that of "industrial installation". This has two major consequences:

- on the one hand, the control is extended on a larger number of activity types: even temporary storage (f. i. marshalling yards, dock) might be covered. This will certainly affect the interfaces between transportation systems and industrial installations, introducing new parties among the actors of the control process;
- on the other hand, if more than one company is operating on a "site", to ensure that a coordinated effort exist to prevent major accidents, some common actions, and therefore new organisational structures will be needed. This also will emphasise analysis of Domino effect scenarios over an industrialised area.

Secondly, the introduction of the obligation for a land use policy with respects to major accident hazards also will have a twofold socio-organisational consequence:

- on the one hand, a broader body of authorities will be involved, as especially the local urban - planning authorities have to decide about the compatibility of new developments with respects to existing land use;
- on the other hand, the public will participate in the decisional process. In this way the public, which until now had the right to be informed about the risks and on the how to behave in the case of an accident<sup>7,8,9,10,11</sup> and, subsequently, had the right of access to environmental information<sup>12</sup>, will exercise a more active role in the overall risk management policy.

Finally, the socio-organisational aspects within the companies will be strongly affected by the introduction of the obligation for formal SMSs.



## IMPLEMENTATION

Directives establish objectives and basic principles to be complied with by all Member States of EEC: each State must transpose them into its own national legislation. This allows various cultural traditions, institutional structures, and regulatory styles to be accommodated<sup>13,14</sup>; on the other hand, this also may result in a variety of criteria and procedures, which can contradict the ultimate goal of the harmonisation of the national approaches. Therefore the action of the Commission and of the national competent bodies is called to monitor constantly the implementation process towards a substantial convergence.

The Commission organises periodic meetings of the Committee of Competent Authorities (CCA), during which questions concerning the Directive and its implementation are discussed so that common approaches can be adopted, and the experience gained with the implementation can be used to ameliorate the Directive itself.

Furthermore working groups have been established with the objective to produce non prescriptive guidance for the implementation of the more relevant requirements. The JRC-ISEI is supporting the activities of the working groups which are constituted by representatives nominated by authorities, industries and control organisations.

Finally the Commission has organised the Community Documentation Centre on Industrial Risk (CDCIR)<sup>15</sup>, located at Ispra, which collects, classifies and diffuse information on published accident investigations, regulations, safety codes of good practices, risk studies etc. The Centre is generally accessible, and the information is diffused by bulletins generally available. It also promotes publications of studies performed or sponsored by the Commission on the technical aspects of the Directive application in the Member States. This action which also contributes to an increased transparency on all questions concerning the risk, provides policy makers and safety analysts with a wide basis of knowledge on national practices and therefore accelerates and improves the harmonisation process.

It is worthwhile to refer the reader to the CDCIR publications already appeared. These cover:

- the Major Accident Reporting System<sup>4</sup>, operated at ISEI, Ispra;
- review of accident case histories<sup>16 to 19</sup>;
- safety reports and codes of practices<sup>20 to 22</sup>;
- information of the public<sup>9</sup>; and,
- emergency preparedness and response<sup>23 to 25</sup>.

The studies on lessons learnt from accident management have been extended to cover all other EEC countries and will be published in the next few months.

The principles of the Directive are finally implemented within national legislation, which in certain cases already includes provisions for land use planning control<sup>25 to 27</sup>.

## ROLE OF THE STAKE HOLDERS

According to the principles stated in above, the roles of the parties participating to the risk management policy can be seen as follows.

### Role of the Public:

- at national level to participate in the elaboration of the risk management policy, i.e. in the definition of the principles which should guide

the sustainable development (benefits from the industrial activities vs. public safety and environmental protection). This should result indirectly from the debate provoked by the public participation on land use decisions;

- at local level participation in the decision on land use planning, and emergency preparedness, consistently with the national policy principles.

#### **Roles of the competent authorities:**

- To exercise control to guarantee the society that industry fulfils its duty, that is the industry has implemented a risk control policy (obligations like identification of the risk, safety reports, in-site emergency plans, SMS etc. are all included within the broad concept of risk control policy).
- to issue operation permit (and or licensing), to permit siting of new activities, to control the land use around existing hazardous sites;
- to promote information and participation of the public in the decisional processes;
- to plan and respond to off-site emergencies;
- to structure the process of information retrieval for preventing accidents and to improve preparedness and response.

**Roles of the Industry:** as the hardware is increasingly improving: safety depends first on management factors, secondly on human factors, if the two categories can be distinguished. Therefore the industry has to realise (and many facts prove that this awareness is growing up at least in major companies) that safety management can only be achieved via the assimilation of the safety culture within the corporation culture. The adoption of SMSs shall help in creating this culture and shall encompass all management steps, both in preventing accidents and in managing them:

**prevention** ⇒ **management at less stringent time constraints**, which includes:

hazards identification at the design stage  
 hardware and administrative countermeasures  
 operating procedures with involvement of the operator skill and experience  
 design modifications  
 maintenance, work permits  
 inspection and supervision  
 training of operators and information of the workers  
 retrieval of operating experience, debriefing of near misses  
 safety audits and performance measurements  
 planning and training for on site emergencies  
 use of the safety report as an important tool to guide this overall process  
 cooperation with authorities for information of the public

**mitigation:** ⇒ **management at stringent time constraints**

implementation of the in-site emergency measures  
 cooperation and coordination with public authorities and other resources (proximate industries) for external emergency measures.

#### **CHALLENGES FOR R&D**

Under the above perspective two major aspects might be of interest for risk management researchers:

- **Risk Assessment and Decision Making:** especially for land use planning the use of risk assessment might be useful. PSA is however still confronted with the problem of the uncertainties<sup>29</sup>. The use of quantitative goals has been adopted in the Netherlands<sup>27</sup> and in UK<sup>26</sup>. However even countries like France<sup>28</sup> which assumes

reference scenarios as the basis of the land use policy, are confronted with the subjectivity of the scenarios adopted. There is a need for improving consistency of PSA analysis procedures and on the same time to make people aware of the limitations existing for probabilistic decision theory. A larger effort should be devoted to propose Multi-Attribute, Multi- Objective decision making models. Indeed such models would have the advantage to make the multiple factors to be transparent in a decision process involving multiple actors (these can indeed take into account multiple economic factors, as well individual and group risk figures, and environmental protection values);

**Safety Management Systems:** in addition to social science research to incorporate the safety culture into the company culture and sharing this culture at all level within the organisation, performance measurements via performance indicators<sup>30</sup> have to be developed and validated.

#### A CONCLUDING REMARK

Focus of public decisions on safety control has moved in the time from standards and norms on single components towards higher levels of aggregations: complex technical systems (system analysis); complex technical systems including man (risk analysis, human factors); and, finally, Safety Management Systems in which the focus is on the safety control itself. At the same time decisions about safety and environment have been made more and more open to public participation. To avoid that the new measures envisaged to control risk will only lead to increased formal burdens or to never ceasing public debates, a cultural change<sup>31</sup> is needed not only in the companies, but even in the relations public - industry - administrations.

#### REFERENCES

1. Council Directive of June 24, 1982 on the major-accident hazards of certain industrial activities (82/501/EEC). Official Journal of the European Communities L230, Vol. 25, August 5, 1982.
2. A. Amendola: The EEC Directives on Environmental Hazards. Proceedings of the EURO COURSE on Environmental Impact Assessment (ed. A. G. Colombo). Kluwer Ac. Pub. (1992)
3. G. Drogaris: Learning from Major Accidents Involving Dangerous Substances. Safety Science, 16 (1993) 89-113
4. G. Drogaris: Major Accidents Reporting System. Lessons Learned from Accidents Notified. CDCIR, Elsevier Publisher 1993.
5. Official Journal of the European Communities, L 85, March 3, 1987.
6. Official Journal of the European Communities, L 236, December 7, 1988.
7. B. De Marchi: Public Information about major accident hazards: legal requirements and practical implementation: Industrial Crisis Quarterly 5(1991) 239-251
8. A. Amendola. Implementation of the art. 8: information of the public " 10th Anniversary of the Seveso Directive" Seminar organised by CEC and the French Ministry of Environment. Cayenne 21-25 Sept. 1992
9. B. Wynne: Empirical Evaluation of Public Information around Major Hazards Sites. CDCIR., EUR 14443 EN. 1992
10. H.B.F. Gow and H. Otway (eds.): Communicating With The Public About Major Accident Hazards. Elsevier applied science publisher. London. 1990.
11. B. De Marchi and E. Rota: Risk Information Needs of Communities near Seveso Sites. A Pilot Study. EUR 12887 EN. 1990

12. Council Directive (90/313/EEC) of 7 June 1990 on the freedom of access to information on environmental matter. Official Journal of the European Communities. L 158/56. 23 June 1990.
13. H. Otway and M. Peltu (eds.): *Regulating Industrial Risks: Science, Hazards and Public Protection* (Butterworths, London 1985) (see in particular T.O'Riordan contribution pp 20-39)
- 14 H. Otway and A. Amendola: "Major Hazard Information Policy in the European Community: Implications for Risk Analysis" *Risk Analysis*, Vol. 9, No 4, 1989 ,505-512.
15. K. Rasmussen and HBF Gow: The importance of information on industrial risk: A new documentation centre. *Journal of Hazardous Materials*, 30 (1992) 355-359
16. P. Lindgaard-Jorgensen and K. Bender: *Review of Environmental Accidents and Incidents*. CDCIR, EUR 14002 EN. . (1992)
17. G. Drogaris: *Review of Accidents Involving Chlorine*. CDCIR, EUR 14444 EN (1992).
18. G. Drogaris: *Review of Accidents Involving Ammonia*, CDCIR, EUR 14633 EN (1992).
19. G. Drogaris: *Review of Accidents Involving Unexpected Run-away Reactions* CDCIR. EUR 14634 EN (1992)
20. A. Amendola, S. Contini: *National Approaches to the Safety Report. A Comparison* CDCIR , SP-I.91.07, CEC- JRC, ISEI (1991)
21. S. Harris et al.: *Comparison of LPG Related Regulations*. CDCIR, EUR 13699 EN (1991).
22. S. Harris et al.: *Comparison of selected LPG Related Codes and Standards*. CDCIR, EUR 14636 EN (1992).
23. G. Drogaris (Editor) "Lessons Learned from Emergencies after Accidents in the Federal Republic of Germany Involving Dangerous Substances, CDCIR, SP-I.91.23, (1991).
24. E.J. Smith and G. Purdy: *Lessons Learnt from Emergencies After Accidents in the United Kingdom Involving Dangerous Substances*. CDCIR, EUR 13322 EN (1990)
25. B. Brette, B. Lequime and JC Besnard: *Lessons Learnt from Emergencies after Accidents in France Involving Dangerous Substances*. CDCIR, EUR 15059 EN (1993)
- 26 HSE "Risk Criteria for Land-Use Planning in the Vicinity of Major Industrial Hazards" (1989)
27. CJ. van Kuijen "Risk Management in The Netherlands: A Quantitative Approach" in B. Segerstahl and G. Kroemer (eds.) *Issues and Trends in Risk Analysis*. IIASA, Laxenburg(A). WP-88- 34, pp. 41-57.
28. J. Mansot . The case of Lyon. OECD workshop on the role of the authorities in research into major hazards and land use planning (London, 19-22 February 1990)
29. A. Amendola, S. Contini and I. Ziomas: *Uncertainties in chemical risk assessment: Results of a European benchmark exercise*. *The Journal of Hazardous Materials*. 29 (1992) 347-363
- 30 S. Schreiber: *Measuring Performance and Effectiveness of Process Safety Management*. EEC seminar on Safety Management in the Process Industry. Ravello (Sa) Italy October 7/8, 1993
31. M. Schüz: *Risiko und Wagnis: die Herausforderung der industriellen Welt*. Gerling Akademie, Verlag G. Neske, Pfullingen (1990)

## **PLANT LEVEL HAZARD IDENTIFICATION BASED ON FUNCTIONAL MODELS**

Jouko Suokas

VTT  
Safety Engineering Laboratory  
Tampere, Finland

### **INTRODUCTION**

The basis of risk management is the identification of hazards and the evaluation of their contributory factors. The assessment of risks, and the planning of measures to reduce or to control risks are based on the information about hazards and their contributors. Therefore, it is most important to assure that the hazards have systematically been identified and evaluated.

There are currently a number of techniques which are employed for the identification of potential failure scenarios for major hazards assessments on process plant. These techniques may relate to

- the technical system: comparative methods such as checklists and hazard indices (eg. the MOND and DOW indices), preliminary hazard analysis, hazard and operability study (HAZOP), failure mode and effect analysis (FMEA), fault tree
- human tasks: methods of human error analysis - for example, action error analysis, several probabilistic methods such as THERP, etc.
- management and information system: there are several auditing methods and rating systems, such as for example five stars, and other methods such as management oversight and risk tree (MORT) for a more detailed investigation of an accident or the function of an organisation.

Hazard identification is based on two main subjects - the search strategy of the employed method/methods and the description of the system to be studied. The search strategy defines the types of hazards to be covered, and the description of a plant or an

activity the systems/subsystems to be included and the level of detail of the identification. In some cases the plant description is rather clear and systematic. This is the case, for example, in HAZOP-studies and in FMEAs. However, these methods typically investigate a plant at rather detailed level resulting often to a situation where the study is time-consuming and costly to implement. Therefore, there is a clear need for the development of

- systematic methods and tools for the description of plant functions and subsystems
- methods for systematic identification of major hazards based on plant level description
- methods which can integrate the investigation of technical, human, and management factors as the contributors to hazards.

This paper describes the development done in the TOMHID-project in the EC research programme STEP and some other complementary results and experiences in the development of hazard identification at plant level and in the development of knowledge-based tools for the hazard identification.

## THE TOMHID PROJECT

HAZOP is perhaps the most widely applied method for the identification of hazards in process industry. HAZOP, however, suffers for some problems and deficiencies. HAZOP does not cover all types of hazards and all types of their contributors. The limitations of HAZOP have been evaluated in a few studies, eg. (Suokas 1985, Taylor, 1981, Taylor 1986).

The other major problem with HAZOP relates to the level of details in the study. HAZOP is typically carried out on the basis of pipe and instrumentation diagram (PID) which is appropriate for small processes. However, when studying a large process plant there is a clear need to make the study first on a more general level.

The TOMHID-project focuses on both of the afore mentioned problems. The aim of this project is to develop an overall knowledge-based methodology for hazard identification. The methodology will have the following features:

- The description of process plant as a sociotechnical system for high level studies of hazard and risk.
- The use of high level screening tool as a first stage in the hazard identification process. This will identify critical areas and the need for further analysis using other complementary approaches.
- The choice of various fundamental methodologies such as eg. HAZOP, and the development of new intermediate methods where appropriate to modern information technology.
- The use of other features such as checklists and possibly human error analysis.

The project is funded by the EC research programme STEP (Science and Technology for Environmental Protection). The scientific co-ordinator of the project is VTT from Finland, and the participants SRD and Sheffield University from UK, Tecsca and JRC from Italy, Risø National Laboratory from Denmark, and CIEMAT from Spain.

The project covers a critical review of the existing hazard identification methods and an interview of the user needs for this kind of new methodology and supporting computer tools. The development of new methods and tools can be divided into the following tasks

- functional modelling of process plants
- concept hazard analysis of a plant
- screening of identified hazards
- identification of technical and management factors contributing to the hazards
- tools to support the construction of plant description and the identification of hazards.

### FUNCTIONAL MODELLING OF A PROCESS PLANT

Plant description forms the basis of hazard identification. In large plants there is a need to first carry out the hazard identification on a general level before starting detailed studies such as HAZOPs on the basis of PIDs. There are a number of methods which have been used in plant level hazard identification. Examples of them are potential problem analysis, preliminary hazard analysis, concept hazard analysis, and checklists. One of the main problem in plant level studies has been the plant description. This may have been in the form of lay-out drawings, lists of inventories and main process installations, etc. Even if these descriptions cover the main parts and subsystems of a plant there is lacking a systematic link between the plant description and the search procedures employed in the identification methods. Therefore, one may present doubts about the systematics of plant level hazard identification and the coverage of the results.

A plant function can be described by several ways. There are also formalised methods supported by software tools to aid the construction of functional models. Perhaps the best known method is the Structured Analysis and Design Technique (SADT) which originally has been developed to support software specification and development (Yordon 1989). Here, the functions have been defined as consisting of three main objects: intent, constraint and methods. Figure 1 illustrates the graphic and logic representation of a function.

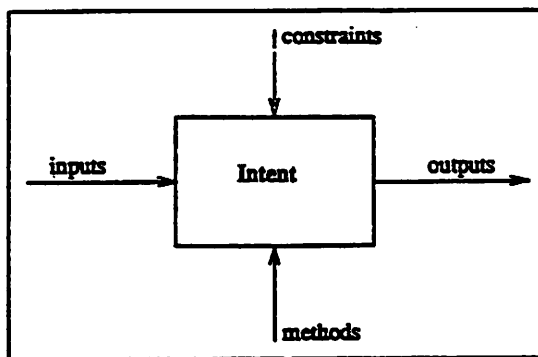


Figure 1. A function is composed of the intent, inputs and outputs, and methods and constraints (Conceptual... 1993).

The driving mechanism of the functional decomposition is the intent (goal) of the functions in question. The basic internal structure is to link the intent of a function with the constraints that are necessary to control or restrict the intent, and the methods that are used to carry out the intent. The plant model, hence, contains objects that can be classified as follows (Rasmussen et al. 1993):

- intents representing the functional goals of the specific plant activities in question
- methods representing items (hardware) that are used to carry out the intent or operations that are carried out using the hardware
- constraints that describe items (work organisation, control systems) established to supervise or restrict the intent.

The advantage of functional description is that it can be applied to any kind of system. A functional description of a plant can be done in a very early stage in design, well before any selections on hardware has been made. This makes it possible to carry out the first safety studies in an early design phase and to use their results in the selection and specification of hardware. Another advantage is that in existing plants there are large numbers of documents resulting to a difficulty to see the forest from the trees. Functional model allows also the integration of technical and management factors in the same plant model, i.e. the description of a plant as a sociotechnical system.

Figure 2 shows an example of the functional description of a part of a phenmediphan (PMP) production plant which has been the first case to test the ideas of functional modelling in the TOMHID project. The PMP plant and a methanator section of a hydrogen plant have also served as the first cases to test the ideas of hazard identification.

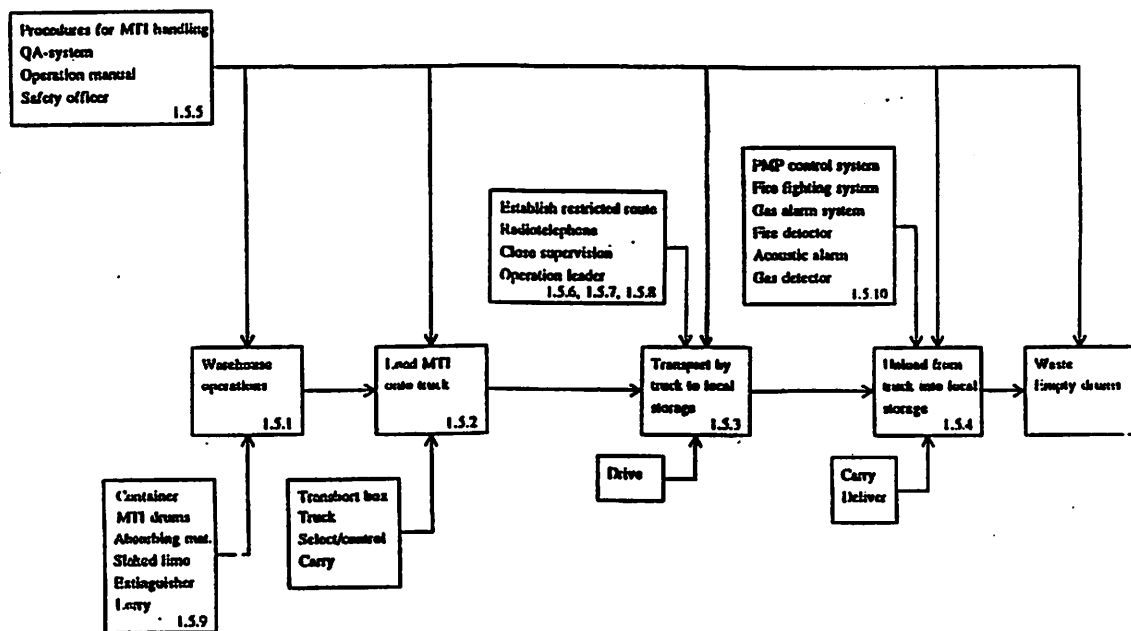


Figure 2. Functional description of a part of a phenmediphan plant. The function "provide MTI chemical" has been broken down in the figure (Rasmussen et al. 1993).



## HAZARD IDENTIFICATION BASED ON FUNCTIONAL MODEL

Hazard identification is made on the basis of the functional description of a plant. The main methods evaluated and further developed in the project have been concept safety review, critical examination of system safety, concept hazard analysis, preliminary consequence analysis, and preliminary hazard analysis (Concept...1993, Wells et al. 1992). These methods were tested the first time on a methanator section of a hydrogen plant. The methods mentioned above are intended for the identification of hazards and their immediate causes. The aim of TOMHID is to support the identification of sociotechnical factors contributing the occurrence of hazards and their consequences. Therefore, a new checklist based method for the investigation of management factors has also been developed. The structure of hazard identification process is described in figure 3 showing the inputs and outputs of the different phases.

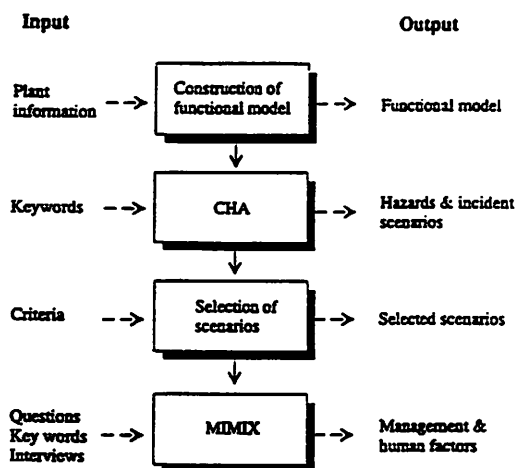


Figure 3. The hazard identification process based on the use of functional model of a process plant.

On the basis of the findings made in concept hazard analysis, a number of hazard scenarios are selected for further studies. The selection of scenarios is based on the potential consequences, and the potential human and management involvement. When the scenarios have been selected one carries out the investigation of management factors. For this purpose a set of questions supported with list of key words are under development. The questions are applied in two phases. In the first phase, persons directly involved in the scenario or the tasks related to the scenario are interviewed. Then, on the basis of the findings the supervisory and senior level persons who are responsible in the tasks concerned are interviewed. The method is called MIMIX (Method to Investigate Management Impact to Causes and Consequences of Specific hazards).

So far, the methods have been tested with small cases based on the experience of the research team. These tests have given valuable information about the applicability of the methods and indicated areas where further development is needed before full scale tests can be carried out. This year the methods are applied on a large existing installation in order to evaluate their applicability in plant level hazard identification.

## REFERENCES

Conceptual study of hazard identification and risk reducing methods. 1993. STEP-TOMHID-project. Report of work package 2.

Rasmussen B. et al., Hazard identification based on functional plant modelling. Risø National Laboratory. (to be published 1993).

Suokas, J. 1985. On the reliability and validity of safety analysis. VTT, Publications 25, Espoo. 69 pp. + app. 8pp.

Taylor, J.R. 1981. Completeness and discrimination of hazard analyses. Roskilde, Risø National Laboratory, Risø-M-2306. 19 pp.

Taylor, J. R. et al. 1986. A design review approach to safety analysis. 5th International Symposium "Loss Prevention and Safety Promotion in the Process Industries". Cannes 15 - 19 Sept. 1986. Paris, Société de Chimie Industrielle, pp. 11.1 - 11.

Wells, G., Wardman, M. & Whetton, C. 1993. Preliminary safety analysis. Journal of Loss Prevention in Process Industry, 6, 1, pp. 47 - 60.

Yordon, E. 1989. Modern structured analysis. Englewood Cliffs, Prentice-Hall. 672 p.

## ACKNOWLEDGEMENTS

The author wants to express his acknowledgements to the EC STEP-program for the financial support received, and the project team for innovative work and many inspiring discussions during the project.

## **DECISION MAKING IN PROCESS DESIGN - ASSESSMENT OF TOTAL SAFETY BY AGGREGATING THE SAFETIES OF THE SUBPARTS OF THE PROCESS**

**Raija A. Koivisto<sup>1</sup>, Veikko J. Pohjola<sup>2</sup> and M. Katariina Alha<sup>2</sup>**

<sup>1</sup> VTT, Technical Research Centre of Finland  
Safety Engineering Laboratory  
B.O. Box 656  
SF-33101 TAMPERE, FINLAND

<sup>2</sup> University of Oulu  
Linnanmaa  
SF-90570 OULU, FINLAND

### **ABSTRACT**

Process design is a very complex activity including three typical problem solving stages, synthesis, analysis and evaluation. By using these three basic elements the tasks in the process design project can be described: synthesis refers to process structure design and optimisation, analysis to process state definition and optimisation and evaluation to process performance assessment. In conventional process design most decisions concerning safety are being made in the evaluation phase. The new methodology suggests that safety should be included in the synthesis phase already. To make this possible, process, safety and process design were defined and described by using object hierarchy (Pohjola et al., 1993a and 1993b). This paper describes how safety can be taken into account during the process design in its every phase by defining process and safety in the same object hierarchy and by associating safety with process on the lower level of this hierarchy. Thus, safety will be included in every decision making point during the design and the total safety can be assessed by aggregating the safeties of the subparts of the process. Safety balance has been introduced (Pohjola et al., 1993b) to aid the evaluation. This paper describes theoretically the use of the developed methodology in the process design.

### **INTRODUCTION**

Process design can be seen as generation of alternatives, selection between those alternatives and decision-making about acceptability - or goodness - of the selected alternative. To be able to select the best alternative there must be a good understanding about criteria applied and about the mutual importance of the applied criteria. An experienced designer

has a system built ready in his/her mind. However, there can be subjective preferences and unconscious human behaviour which have a strong influence in the decisions. Quite often, especially in early design phases, safety assessment and judgement are based on subjective experiences rather than on objective and systematic considerations.

When thinking the life cycle of a process, the most important decisions concerning safety are being made when defining the strategic design constraints and strategic safety constraints, especially. Most often these constraints are in the linguistic form. Even if they have been given quantitative values, it does not help the designer very much: the safety requirement has been expressed as a certain risk due to the whole installation which is difficult to translate into some realistic value for the detailed design target, e.g. for a valve or a pump. Such a constraint can also be for example 'as safe as possible', 'as safe as reasonably achievable', 'as cheap as possible', 'as simple as possible', 'standard level is enough', 'maximum availability', 'maintenance takes care of the problems' etc. However, the question of acceptable safety still remains unsolved.

How do a designer deal with acceptable safety then? From the safety point of view there are three levels to take safety into consideration during the design (Koivisto & Reunanen, 1993): the adherence to good practice, the safety analysis and the safety-driven process design. The adherence to good practice consists of observing the rules and regulations, meeting the requirements of the accepted standards, and of following the practices that have proven to be best during the years of experience with the same processes, the same plant designs and requirements, and the same operating and maintenance procedures. The safety analysis is a systematic examination of the structure and the functions of a process system aiming at identifying potential accident contributors, evaluating the risk induced by them and finding the risk-reducing measures. There are several safety analysis techniques available, but the general problem in the process design, especially in its early phases, is that there is not sufficient information on the process available to apply these techniques. The safety-driven process design methodology will be described more detailed in this paper.

Formal methods in the comparison of different design alternatives are used very seldom by process designers. Life cycle analysis technique is one mean to help in comparison of different alternatives and it has been generally used in the product design nowadays (see for example Thurston and Blair, 1993). Formal decision making aids can also be found on the strategical level, which produces the first safety requirements.

The aim of this study is to associate safety with process design, thus, allowing the safety to be taken into account every time, when decisions on the process are being made. The association becomes possible on the lower hierarchical level when process and safety have been defined and explicated. The new process design methodology uses the Performance Driven Strategy (Pohjola et al., 1993a) to specify the decision making during the design. This methodology is based on the object oriented description of the process and the safety, and on the task based description of the process design.

## **ASSOCIATION OF 'SAFETY' WITH 'PROCESS'**

### **Definitions**

To be able to build an object hierarchy we need to know what is meant by process and safety. Pohjola et al. (1993a) have defined process to be

"(Chemical) Process is Control of (physico-chemical) Phenomena for a Purpose"

and safety (Pohjola et al., 1993b) to be

"Safety is quantified by Probability that Control of Phenomena is lost and by Consequences."

### Object Hierarchy

By using these definitions as starting points an object taxonomy (Virranto, 1993 and Pohjola et al 1993a) was built which defines process as an object having structure, state and performance as its attributes. Process can be said to be completely defined when the values of these three attributes are fixed. The unit structure of process consists of boundary which separates interior from exterior, and of interactions through this boundary. Different abstraction levels are formed by aggregating and disaggregating the process structure, state and performance. Through disaggregation the object can be described more detailed as a topology of objects of its own kind i.e. belonging to the same class.

The object taxonomy was built by explicating the key concepts - phenomena, control, purpose, probability, consequences - of the definitions further. *Phenomena* are spontaneous physico-chemical phenomena. Control and purpose make phenomena a process; phenomena are allowed to take place only in a certain interior where the rate and the extent of the phenomena are being controlled to realize a certain purpose. *Control* is put into practice by the boundary and the interactions (mass flow, energy flow, information flow, etc.) through this boundary. Loss of control means breaking of the boundary or the malfunction of the interaction. *Purpose* is composed of functional specifications and performance constraints. The former refers to the expectations on the material input and on the desired material and energy outputs through the process boundary and to the desired phenomena for carrying out the conversion in the process interior. The latter, performance constraints, refers to the criteria and requirements for process performance (goodness) evaluation.

### Association of Safety with Process

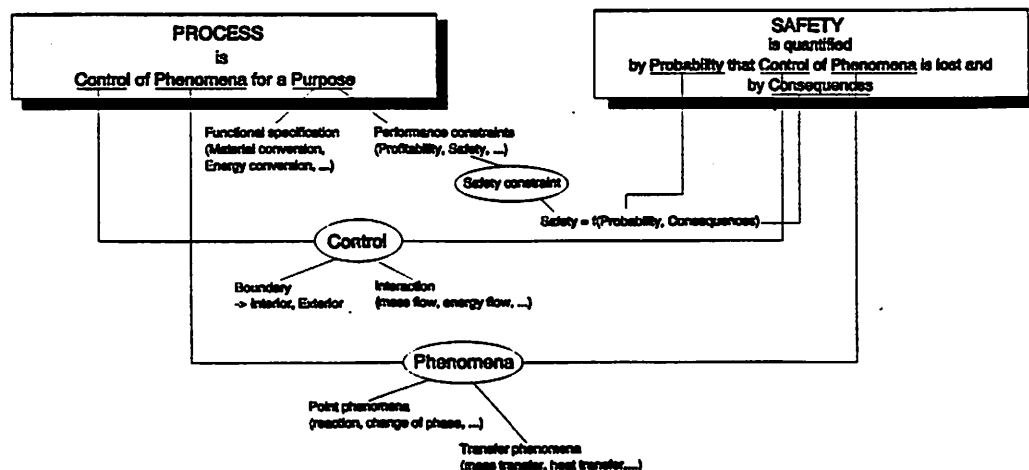


Figure 1. Conceptual association of safety with process.

The association of Safety with Process is difficult on the general level. However, when defining the concepts based on the definitions earlier, it is evident that safety can be linked

to process as presented in Figure 1.

The *Probability* that control of phenomena is lost means either a subjective probability distribution or a statistical frequency distribution on the time axis depending on the available knowledge (van Steen and Gerlings, 1989). Actually, probability is a relation between probability and time. The object 'relation' has the attributes structure, state and performance. Furthermore, the probability that control of phenomena is lost has two contributing factors: the phenomenon which is the object of the control, and the boundary and interaction which are the means to control. The value of the probability is dependent on the structure (type of the distribution function) or on the state (parameter values in the distribution function) of the probability relation object. This structure is defined by the probabilistic events which are related to the boundary and the interaction. The state of the probability relation is dependent on the nature of the phenomenon and on the nature of the material in which the phenomenon is taking place.

*Consequences* are characterized as being undesired and irreversible which means that they cause damage more or less impossible to repair. The damage may be caused only to the process itself or even to the whole universum. The damage may be quantified by the loss of economic, esthetic and cultural value, by the loss of health and life, by the amount of human suffering etc.

Damage occurring in the exterior is caused by the phenomena in the exterior material. This material may include some material which originally belonged to the interior or to the boundary and was moved over or from the boundary due to an release, explosion, fire, etc. The phenomena in the exterior are not under control usually. However, some control is possible if suitable protection and emergency procedures are available. The quantity of the damage in the exterior depends on the rate and on the extent of the phenomena occurring in it and there is no basis to define certain general areal or temporal limits for the exterior, but they must be considered case by case.

When having defined process and safety in the object hierarchy, we can define process design by the same concepts. *Process design* is decisions on the control - boundary and interaction - of phenomena (Pohjola et al., 1993b). After having defined the boundary, i.e. having designed the process, there is the interaction left which can be changed. *Process operation* is then decisions on process interactions (Pohjola et al., 1993b).

## SAFETY BALANCE

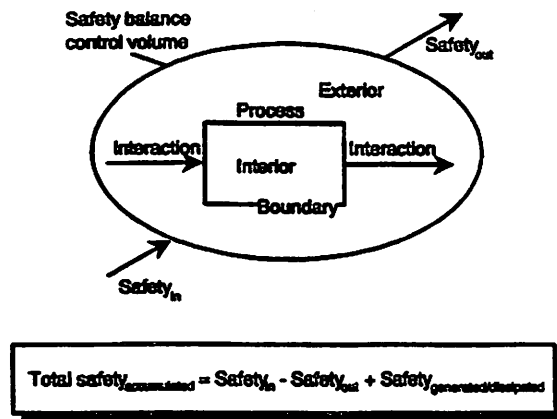


Figure 2. Safety balance (Pohjola et al., 1994).

The notion of safety balance was first presented by Pohjola et al. (1993b) and will be demonstrated shortly in (Pohjola et al., 1994). The safety balance is needed to assess the change of the total process safety due to the changes in safety of the parts of the process. These changes may occur in all of the process elements - in the interior (phenomena), in the boundary, in the interaction and in the exterior - during the process design. In process operation the boundary is fixed and changes are more likely in the control of the process or in the exterior. Nevertheless, unintended changes in boundary, corrosion or rupture a.e., may occur affecting the safety during the operation, too.

## SAFETY IN PROCESS DESIGN

Safety requirements can be taken for a constant for the total process which is to be designed. Generally,  $\text{Safety} = f[\text{Probability}, \text{Consequences}]$  (Requirements, 1991), hence,

$$\text{The total Safety} = f\{\text{Aggr}_{(P)}[\text{Prob.}(i)], \text{Aggr}_{(C)}[\text{Conseq.}(i)]\} = \text{Constant} \quad (1)$$

(Pohjola et al., 1993b) where the constant represents the safety requirements. As stated before, it is not common to have defined safety requirements. And even if they exist, it does not help the designer very much in the detailed design. According to our methodology, safety balance can be written

$$\text{Total safety}_{\text{accumulated}} = \text{Safety}_{\text{in}} - \text{Safety}_{\text{out}} + \text{Safety}_{\text{generated/dissipated}} = \text{Constant}. \quad (2)$$

Hence, by disaggregating the process in relevant subparts and by selecting safety balance control volume accordingly, we can use the safety balance as a technique to translate the safety requirement of the whole process into requirements for the subparts of the process. Process design is decisions on the control - boundary and interaction - of phenomena. In the synthesis-analysis-evaluation task cycle we first have safety as a part of the performance function. If we decide to weight the safety most, we end up to the Safety-Driven Process Design methodology, which means that we let safety guide our decisions. If the safety part of the performance function is dependent on the structure of the process, the synthesis will be considered from the safety point of view in safety-driven process design. When the structure has been synthesised we analyse the state and proceed to the evaluation activity. Evaluation has the systematics to compare different alternatives with each other (including the safety point of view), or the produced design (safety) with the (safety) requirements. Along the synthesis-analysis-evaluation loop we get more information on the safety of the designed object and we can compare the achieved safety with the requirements more and more reliably.

A simple example, where the total safety has been defined by aggregating the probabilities and consequences of the subparts of the process and the safety balance has been used, will be presented in (Pohjola et al., 1994).

## DISCUSSION

The mostly used and only methodology in process design has been the one by Douglas (1988). Ponton (1993) has built 'an environment for creative process design' which, however, is based on the Douglas methodology as well. The deficiency in these developments is that the decision criteria can not be weighted as desired which means that the economy is the leading factor in the design.

Our methodology starts from the very basic definitions, and models both declarative

and procedural knowledge by using object and task hierarchies. So far everything seems to work well, but we are aware that there still is a lot to do before this methodology is in every day use. One of the biggest problems will be the lack and the poor quality of the knowledge which especially is a problem when speaking about the safety. The other problem will be the acceptable safety and the representation of the safety requirements. One attempt to take the safety requirements into the design process was made by Karns et al. (1992) as they presented the Achievability analysis concept.

## CONCLUSIONS

Safety considerations in process design have been moved from the use of the experiences - the adherence to good practice - to the use of the safety analysis for two decades ago. We suggest that the third generation in this development would be the safety-driven process design which has been briefly presented in this paper.

## ACKNOWLEDGEMENTS

This work is a part of the PROTUS and CARD-2 projects both financed by the Technology Development Centre of Finland (TEKES).

## REFERENCES

- Douglas, J.M., 1988, "Conceptual Design of Chemical Processes." McGraw-Hill Book Company, New York.
- Pohjola, V.J., Alha, M.K. and Ainassaari, J., 1993a, Methodology of process design, Paper presented in ESCAPE-3, Graz, 5-7 July, 1993. To be published in: *Computers chem. Engng.* 18(S), 1994, pp. S307-S311.
- Pohjola, V.J., Koivisto, R.A. and Alha, M.K., 1993b, Conceptual association of safety with process design and operation. Foundations of computer aided process operations - FOCAPO, Mount Crested Butte, Colorado, 18.-23. 7.1993. 6 p.
- Ponton, J.W., 1993, Developing an environment for creative process design. The 11th International Congress of Chemical Engineering, Chemical Equipment Design and Automation - CHISA'93, Prague, 29 August - 3 September 1993. 10 p.
- Karns, J.J., Fragola, J.R., Kahan, L. and Pelaccio, D., 1992, Nuclear electric propulsion: operational reliability and crew safety study. SAIC, New York.
- Koivisto, R. and Reunanen, M., 1993, Systematic methods in safety considerations during process design - requirements, limitations and usefulness. The 11th International Congress of Chemical Engineering, Chemical Equipment Design and Automation - CHISA'93, Prague, 29 August - 3 September 1993. 10 p.
- Pohjola, V.J., Koivisto, R.A. and Alha, M.K., 1994, Fundamentals of safety-based computer-aided process design, ESCAPE-4, Dublin, March 23-30, 1994. (submitted).
- Requirements..., 1991, Requirements and guidelines for analysis of technological risks, draft 56(Secretariat)353. Geneva, International Electrotechnical Commission, Technical Committee no 56:353. 30 p.
- Thurston, D.L. and Blair, A., 1993, A method for integrating environmental impacts into product design. Proceedings of the International Conference on Engineering Design - ICED'93, The Hague, August 17-19, 1993. pp. 765-772.
- Van Steen, J.F.J. and Gerlings, P.D.O., 1989, Expert opinion in safety studies, Delft University of Technology.
- Virranto, A.M., 1994, An object-oriented taxonomy of declarative process knowledge, Paper presented in ESCAPE-3, Graz, 5-7 July, 1993. To be published in: *Computers chem. Engng.* 18(S), 1994, pp. S737-S741.



## SHORT-CUT RISK ASSESSMENT

Geoff Wells<sup>1</sup> and Steve Allum<sup>2</sup>

<sup>1</sup>University of Sheffield, Dept. of Mech. and Proc Eng, Sheffield, S1 3JD, UK,

<sup>2</sup>Bowring Marsh & McLennan Ltd, Bowring Building, London EC3P 3BE

### SUMMARY

Performing a short-cut risk evaluation leads to a better understanding of the system - particularly of incident scenarios, hazard identification and human response in an emergency. Generating estimates of risk allows the benefit of risk reduction measures to be gauged. The method adopted here uses estimates of event likelihood per year and consequences as measured by severity. The factors given in the severity categories encourage a complete study of the ways of causing damage and harm to property, business, people and the environment. The assessment values also serve to indicate where further work is required, including performing a detailed Quantified Risk Assessment.

### THE ASSESSMENT OF RISK

In general the standards of safety in the process industries are high due to the implementation of rigorous management systems, the safety awareness of the workforce, and compliance with regulations, codes of practice and standards. To this approach can be added risk management with full or partial Quantified Risk Assessment (QRA) being used particularly for the assessment of major hazards. The process of risk assessment involves an analysis phase incorporating hazard identification, risk evaluation and assessment against set criteria.

Other factors also affect decisions as to the suitability of a project or whether to keep an activity operating. These include:

- Economic criteria for justifiable expenditure and consequential loss.
- Acceptability criteria for effluents, emissions, wastes and noise.
- Access, egress, environs and location of site.
- Acceptability and consultation requirements of outside bodies.
- Impact on site of notifiable status.
- Availability of local expertise, skills and training.

Considerable experienced judgement is needed to interpret all these factors and allow for the uncertainties inherent in the calculation. It is also on occasion necessary to convince others that the risk is tolerable and under control. QRA provides objective data to assist in judging divergent views on the allocation of resources to safety expenditure. It assists in making decisions as to whether to cease production on a large plant whilst repairs to a section are carried out. Of course there will still be disagreement about the potential hazard or the tolerability to risk of the public around the site. However some of the arguments can then be related to quantitative values which are capable of rigorous scrutiny. Hence QRA leads to a better understanding of the system and its potential weaknesses enabling a significant reduction of the risk to be achieved.

## TOLERABLE RISK

The target of any company is to have zero accidents. However it is inevitable that unlikely major events will occur at some location because of the large number of companies worldwide. So arguments have been accepted by Regulators that the staff of an operating company should when carrying out a design use a company standard which sets target values for the maximum risk which might be tolerated from their activities. In the UK these values have been greatly influenced by publications on risk criteria for land use planning by The Health and Safety Executive. An intolerable risk is specified which cannot be justified on any grounds, say an individual risk of  $10^{-4}$  fatalities per year; a broadly acceptable region is stated in which the risk is considered by the Regulators to be negligible, say  $10^{-6}$  per year; and inbetween is the ALARP region where the risk should be as low as reasonably practicable and only undertaken if a benefit is desired.

The current company target values for land-based operation which companies in the UK appear to be using are similar to those given in Table 1.

**Table 1. Target values of risk**

<b>Employee individual risk</b>	
• All process causes	$3 \times 10^{-5}$ per year
• Specific process cause	$10^{-5}$ per year
<b>Public individual risk</b>	
• All process causes	$10^{-5}$ per year
• Specific process cause	$10^{-6}$ per year
<b>Risk of major incidents (i.e. societal risk)</b>	
• Near miss from all process causes	$10^{-4}$ per year
• Accident from all process causes	$10^{-5}$ per year
• Catastrophic accident from all process causes	$10^{-6}$ per year
• Accident from specific process causes	$10^{-6}$ per year
• Catastrophic accident, specific process causes	$10^{-7}$ per year

These are compromise best estimates obtained from canvassing opinions in industry and the above values quoted by HSE. The highest targets might be exceeded by an order of magnitude ( $\times 10$ ) in circumstances deemed important by the company. If any vulnerable groups were in the vicinity then the more restrictive values would apply. Such target values of tolerable risk would probably be considered acceptable by many social categories of people and someone working at the location. But they certainly would not be accepted by groups including a majority of egalitarians or sectarianists. Any member of the public would be aggrieved to find a chemical development in 'their backyard'. So the debate will continue and increasingly people have the right to know. This has increased the extent of disputes over risk values and marked the end of pronouncements from on high of acceptable risk...and quite right too given the uncertainties in the data, see Table 2.

**Table 2. Sources of Uncertainty in QRA****System description**

Process description, drawings, or procedures do not represent actuality.  
 Site area maps and population data may be incorrect or out of date.  
 Available weather data may be inappropriate.

**Hazard identification**

Failure to identify all the significant failure events  
 Poor modelling of the incident scenario  
 Failure to include all significant events which have been identified  
 Identification of major hazards and their causes may be incomplete.  
 Hazard screening techniques may omit important cases.  
 Failure to incorporate all control measures in incident scenarios.

**Frequency techniques**

Extrapolation of historical data may overlook hazards from scale-up.  
 Limitation of fault tree theory requires system simplification.  
 Incompleteness in fault and event tree analysis.  
 Data may be inaccurate, incomplete, or inappropriate.  
 Inherent problems in ascertaining human factors.  
 Frequencies modified by different management and maintenance factors.

**Consequence techniques**

Inappropriate model selection and validation.  
 Incorrect physical basis for model and uncertainties in physical data.  
 Source terms selected incorrectly.  
 Uncertainties in damage effects.  
 Mitigating effects incorrectly applied.

**Risk estimation**

Assumptions to reduce the depth of treatment.  
 Restricted conditions of wind speed and stability.

An absolute estimate of risk is compared with specific target values of estimated risk. This is therefore highly sensitive to uncertainty resulting from errors in the evaluation due to incompleteness or inaccurate manipulation of data. Typically the likelihood of a given top event in QRA estimates has an absolute uncertainty of one or more orders of magnitude, that is a difference such as exists between  $10^{-4}$  and  $10^{-3}$ . Such an order of magnitude uncertainty in individual risk often corresponds to a much smaller uncertainty in physical location of the isorisk contour from a flammable event as many physical effects diminish rapidly with distance. This is not necessarily the case for toxic events which can reach surprising distances in both gaseous and liquid phases. Therefore in this case the values of absolute risk must be treated with great caution and at best merely indicate that high standards have been adopted to reduce the risk to the general levels usually found acceptable within the process industries. Certainly it would be very hard in such a case to justify the accuracy of the absolute risk value.

The relative use of risk estimates is less sensitive to error as the resulting risk estimates are subject to similar uncertainties, many of which will cancel out when evaluating the change in risk. It is therefore possible to estimate the reduction in risk achieved through the modification of a system with considerable accuracy, and only cases falling near or into an intolerable risk zone need to be prioritised for detailed study. The regular use of such estimates for all manner of situations enhances the judgement as to whether the risk involved in the task appears acceptable and encourages more accurate evaluation when this is necessary.

## SHORT CUT RISK ASSESSMENT METHOD (SCRAM)

The assessment of risk using short-cut methods enables the analyst to be able to claim that the plant or the task has been assessed and adjusted such that the plant is designed to the same standards of safety and procedures as those considered to represent good practice in the process industries. The production standards necessary to maintain these norms will or have been identified and appropriate measures taken to ensure they are implemented and that continued vigilance is affected. Although further improvements might be made these would probably involve such costs as to make the plant uneconomic. Also lower standards would expose the company and its total environment to undesirable financial risk. However the company will continue to review its safety standards and maintain them at an acceptable level as risk criteria continue to tighten.

The technique accepts that the absolute value of risk will not be assessed with confidence due to uncertainties in the data. However the company's shareholders, employees, Regulators, public etc. can be assured that the risk to the environs will be similar to that in comparable processes and that appropriate measures will be taken to reduce any impact of emergencies no matter how rare these might be.

Several methods exist for short-cut risk assessment. In the Short Cut Risk Assessment Method, SCRAM, the risk is defined in terms of the Likelihood, L, of a specific undesired event occurring within a given period or in particular circumstances and the Severity, S, which is a measure of the expected consequence of an incident outcome.

The target risk is defined by the equation:

$$\text{Target Risk} = \log_{10}10^L + \log_{10}10^S = L + S$$

where:

- L is the exponent of likelihood as measured by frequency (a negative value),
- S is the severity category as given in Table 4.

The target risk is only acceptable to the assessor when its value is equal to, or less than, zero. Other methods are available which in effect sum the absolute values of these terms and the choice of which to use can be left to the familiarity with each method of the analyst.

To reduce the risk either reduce the likelihood of occurrence, which is a measure of the expected probability or frequency of occurrence of an event, and/or ameliorate the severity of the consequences or its occurrence by appropriate measures.

The severity categories which are assigned to any incident scenario should be based on the highest level indicated by the category: The 'major' consequences correspond to the ranking of 'high' used as the highest level by many companies. The levels 'severe' and 'catastrophic' relate to very rare events occurring at most one in 100,000 years and are included to reflect that such incidents may occur on a worldwide basis each year at each facility.

In no way should the list be used to imply that loss corresponding to a 'major effect on business with loss of occupancy up to three months' is more serious than 'injuries to less than five plant personnel with 1 in 10 chance of fatality'. Most companies and individuals within the company would regard the latter as more important. The list presents practical targets for design purposes only. The severity categories given in Table 4 have no status. They represent an amalgamation of various viewpoints collected over the years and are updated as authoritative views are heard at conferences and meetings. It has been noted that there is an increased trend during the last decade to recommend higher task constraints and the recommended values for likelihood and severity ranking may well soon require an increase by an order of magnitude i.e. from  $10^{-5}$  to  $10^{-6}$  etc., particularly for categories above major.

The severity categories allow for the effects on the business of an incident. Further attention has to feature, such as whether a new acquisition has the same high standards of safety or a location may not have the same expertise available as at other sites of the parent company. Even risk estimates can have an effect on the business. A communication to reassure the public about risk can have the opposite effect if it is not seen to be credible given the local reputation of the company. Similarly a warning as to the action to take in an emergency can cause public concern, even though it is argued that this action will be necessary on average only once every 100,000 years.

**Table 4. Severity Categories**

***CATASTROPHIC CONSEQUENCES: Severity 5***

Catastrophic damage and severe clean-up costs  
 On-site: Loss of normal occupancy 3 months  
 Off-site: Loss of normal occupancy 1 month  
 Severe national pressure to shutdown this or similar plants  
 Three or more fatalities of plant personnel  
 Fatality of member of public or at least five injuries  
 Catastrophic damage and severe clean-up costs  
 Damage to sites of special scientific interest or historic building  
 Severe permanent or long-term environmental damage to a significant area of land  
*Acceptable frequency 0.00001 per year*

***SEVERE CONSEQUENCES: Severity 4***

Severe damage and major clean-up  
 Major effect on business with loss of occupancy up to 3 months  
 Possible damage to public property  
 Single fatality or injuries to more than five plant personnel  
 A 1 in 10 chance of a public fatality  
 Short-term environmental damage over a significant area of land  
 Severe media reaction  
*Acceptable frequency 0.0001 per year*

***MAJOR CONSEQUENCES: Severity 3***

Major damage and minor clean-up  
 Minor effect on business but no loss of building occupancy  
 Injuries to less than five plant personnel with 1 in 10 chance of fatality  
 Some hospitalisation of public  
 Short-term environmental damage to water, land, flora or fauna  
 Considerable media reaction  
*Acceptable frequency 0.001 times per year*

***APPRECIABLE CONSEQUENCES: Severity 2***

Appreciable damage to plant  
 No effect on business other than loss of production  
 Reportable near miss incident under CIMAH  
 Injury to plant personnel  
 Minor annoyance to public  
*Acceptable frequency 0.01 times per year*

***MINOR CONSEQUENCES / NEAR MISS: Severity 1***

Near-miss incident with significant quality released  
 Minor damage to plant  
 No effect on business  
 Possible injury to plant personnel  
 No effect on public, possible smell  
*Acceptable frequency 0.1 times per year*

## FURTHER STUDIES

Should the results from short cut risk assessment appear sensible when tested against experience and should the accuracy required be appropriate, then a prioritisation can be carried out for further study. A sensitivity analysis can demonstrate the significance of effects although the absolute degree of uncertainty of ultimate effects cannot be demonstrated by short-cut methods. A full Quantified Risk Assessment can then be carried out when appropriate making a 'precise' prediction of the realisation of the hazards, an improved and realistic estimate of the level of damage from the hazards, a comparison with company guidelines for risk and acceptability criteria, modification of the system to reduce the risk, and resolution of the problem with provision made for feedback, feed-forward and monitoring of the system.

A failure rate is not an intrinsic and immutable property of a piece of equipment. Values vary due to factors such as the severity of the processing medium and the operating environment, the suitability for service, the maintenance strategies adopted and factors related to the data itself and the defined equipment boundary. The quality of data for use in risk assessment is generally poor with much published data stemming from sources going back past the 80's. This has achieved a certain status quo as it is perceived as giving historically correct answers. However, much of the data does not distinguish for example between low recovery, fast and dangerous failures and high recovery, slow and safe failures in control systems or data. It does not allow for changes in the historical record, such as have affected the likelihood of BLEVE's and the time available for evacuation, due to the change in relevant technology, fire-fighting and plant layout over the last 20 years.

Also data must be adjusted by a range of organisational, management and human factors. For many processes the factors-affecting consequences are not critical as the extent of possible damage is restricted and well defined. Also it is not difficult to distinguish between a soundly run works operating technology which is well understood by the work force and one badly maintained, having new or novel technology outside the skills of the work force. A process unit having novel technology at a site close to a populated area, but remote from technological support is obviously going to be more at risk. The approach recommended is to look for major variances in one or more factors and change values by up to an order of magnitude. If such adjustments affect key variables, such as the likelihood of immediate cause and the probability of inadequate emergency control then the risk is almost certainly going to appear unacceptable. This will then direct appropriate remedial action to either eliminate the deficiency or reduce its effects.

The study of serious accidents often shows that there is a fairly immediate reduction of safety by the removal or degradation of some clearly identified defence against incidents and this normally causes at least an order of magnitude increase in the probability of the protection failing. It also shows that a procedure was not available in the event of an emergency. Similarly changes occur external to the plant such as in external threats or in plant environs. For example dwellings may be built close to the plant. Performance indicators and standards should be set to control inputs, outputs and work activities. The study of risk should identify specific indicators representing latent and active errors affecting a given scenario. These are in addition to general indicators set by the safety management system or audits. For example the number of times a specific alarm sounds can be treated as a performance indicator to discourage this being misused by operators.

Full motivational safety awareness must be maintained. People choose to behave safely if they realise the consequences. Economic strictures might suggest continuing operation when precautions are faulty but all concerned should be aware of the possible consequences of this decision and its effect on residual risk.

**105 Environmental Risk Management--Restoration**

*Chair: T.E. McKone, LLNL*

**Scope Definition for the Hanford Tank Farms PRA**

*J.P. Kindinger (PLG), D.W. Stack (LANL)*

**Risk Management Applications at the INEL for Advanced Test Reactor Operations and  
Safety and Environmental Restoration and Waste Management**

*S.A. Atkinson, R.L. Nitschke (INEL)*

**Decision Analysis in Environmental Risk Management: Evaluating Multiple  
Stakeholder/Multiple Objective Decisions**

*D.C. Bell, G. Apostolakis, W.E. Kastenberg (UCLA)*

## SCOPE DEFINITION FOR THE HANFORD TANK FARMS PRA

John P. Kindinger<sup>1</sup> and Desmond W. Stack<sup>2</sup>

<sup>1</sup>PLG, Inc.

4590 MacArthur Boulevard, Suite 400  
Newport Beach, CA 92660-2027

<sup>2</sup>Los Alamos National Laboratory

Engineering and Safety Analysis Group, N6  
P.O. Box 990, MS K557  
Los Alamos, NM 87545

## INTRODUCTION

Careful scope definition is important for the success of every probabilistic risk assessment (PRA). Agreement on the scope of the PRA between the PRA analysts and the decision makers who will use the PRA results is necessary to define the appropriate resources needed to do the analysis and to ensure that the PRA will be able to provide insights into the questions of most interest to the decision makers. This paper describes the systematic definition of the scope of the PRA being performed by LANL and PLG for the 177 high-level waste storage tanks located at the U.S. Department of Energy (DOE) Hanford facility.

PRA typically use estimates of the frequency of severe accidents and/or health effects resulting from accidents to measure risk. These parameters were also included in the Hanford Tank Farms (HTF) PRA but were not found to be sufficient to describe the total scope of the analysis. At Hanford, the PRA scope definition question was complicated by the following factors:

- Because of the projected high costs and technological uncertainty of proposed storage and remediation schemes, measures of economic and environmental risk as well as health risk were needed to support the overall risk management of the site.
- Because the PRA spans different eras in the life of the tank farms, different health, economic, and environmental risks are possible at different times.
- At Hanford, radionuclides and hazardous chemicals released into the soil may remain there for hundreds or thousands of years before reemerging to produce unwanted consequences. Thus, for these accident sequences, there is a difference between the time of the event and the time of the consequences.



- For sequences where there is a time span between the event and its potential consequences, changes in site use restrictions during the period in question could impact the predicted magnitude of the consequences in the future.

To comprehensively address these issues, three dimensions were used in defining the scope of the HTF PRA. They are as follows:

1. The time span of the events included in the PRA.
2. The time span of the consequences included in the PRA.
3. The consequence measures used as risk indices

The next three sections discuss each scope dimension in detail and support the integrated scope description presented in the final section.

## **TIME SPAN OF THE EVENTS INCLUDED IN THE PRA**

The life cycle of the Hanford Tank Farms can be described in terms of the four eras or phases that are discussed below. Each era presents different potential health and economic risks. It is recognized that the boundaries between these eras cannot be neatly delineated at any one point in time. They will necessarily overlap and be of different durations for different tanks. None-the-less, these eras provide a useful basis for describing the scope of this and future risk assessment activities.

### **Production Era**

This is the period of plutonium production that began in 1943 and continued for approximately 50 years, until present time. This era includes the direct loading of wastes from separation and purification processing to the tank farms as well as the in-farm processing and evaporation of wastes.

Releases of radionuclides and hazardous chemicals did occur in this era to both the atmosphere and the soil. Acute health effects from these releases, if known, are already realized and are not considered further in this analysis. Delayed consequences from hazardous materials still in the soil beneath the site are possible.

### **Interim Storage Era**

This is the period of time between the interim stabilization of nonwatchlist tank wastes and the final stabilization for long-term storage in place or removal of the wastes for processing. Risks from activities to stabilize watchlist tanks and maintain and characterize all tanks are included in this era. Additions of new waste from site-wide clean-up activities will continue through this era, which is expected to last 10 to 20 years.

### **Remediation Era**

This is the period when tank wastes are prepared for final long-term storage. Activities in this era are expected to take 20 to 30 years, and may range from minimal action to removal of all tank wastes for processing and disposal.

### **Long-Term Storage Era**

Even the most ambitious proposals for remediation of the HTF include long-term storage of at least low-level wastes onsite. Long-term storage should begin within 30 to 50 years from now and extend indefinitely.

## **THE TIME SPAN OF THE CONSEQUENCES INCLUDED IN THE PRA**

Radionuclides and hazardous chemicals released into the soil at Hanford may remain there for hundreds or thousands of years before possibly reemerging to produce unwanted consequences. Factors influencing the timing of the consequence realization include the time, magnitude, and location of the initial release as well as future restrictions on public access to the Hanford site.

Two areas containing tank farms are located in the approximate center of the Hanford reservation. Radionuclide or hazardous chemical releases from the tank farm area must travel at least 2 miles to reach the nearest point of public access, highway 240, and at least 8 miles to cross the nearest point of the site boundary. With these boundaries, hazardous compounds released into the soil may bind with minerals and become immobile or decay and dilute sufficiently before reaching the site boundary so that their potential health risks are negligible. If the boundaries of the site should be moved in the future and the general public allowed closer access to the tank farms, potential health effects from future, or past, releases could be increased. This is especially true if water wells are dug onsite, allowing a new more direct exposure path to be formed. Thus, changes in site use restrictions could impact the magnitude of future consequences predicted from past or future groundwater contamination.

## **CONSEQUENCE MEASURES INCLUDED IN THE PRA**

### **Health Effects Risk**

Potential health effects from exposure to radionuclides and hazardous chemicals are included in the HTF PRA. As described in report Section 6, radionuclide exposure is measured in person-rem and converted to health effects through the use of generally accepted models. Hazardous chemical exposure is measured by the estimated peak concentration of the chemical in the environment and is generally not converted into potential health effects.

Potential health risks from atmospheric releases are calculated for the onsite worker and the offsite populations. The sources of risk included in the HTF PRA include exposure from accidental releases and their cleanup. Normal occupational exposure is limited by regulations and is assumed to present negligible health risk. Delayed doses from subterranean liquid releases are also calculated but are reported separately due to the difference in time and the fact that any consequences will be realized by different individuals.

### **Economic Risk**

Decisions on alternative strategies for storage and remediation of the HTF will consider costs as well as possible health effects. The measure of economic risk is, of course, dollars, and procedures for incorporating time-value effects in decision making are well known. The systematic inclusion of uncertainty in economic analysis is much less prevalent.

When viewed from the decision-making perspective, the sources of economic risk include uncertainty about the cost of planned activities as well as accidents. For the HTF PRA, the following categories of economic risk have been identified for evaluation:

**Expected Costs for Storage and Remediation Activities.** This category includes the estimated costs of normal storage and planned remediation activities. Decision alternatives

may include trade-offs between one-time remediation costs and long-term maintenance costs.

**Added Costs from Technological Failure of Planned Remediation Activities.** New technologies inherently present the risk of technological failure. Major technological uncertainty exists about the characteristics of the HTF wastes, the ability to stabilize them in-situ, remove them from the tanks, concentrate radionuclides, and vitrify waste to repository specifications. Setbacks and failures in these and other tasks represent significant economic risks.

**Onsite Cleanup Costs for Accidents.** This includes the collection and disposal of contaminated soil, the repair of damaged tanks, or the interdiction and treatment of contaminated groundwater.

**Offsite Collateral Damage from Accidents.** Included in this category is the economic cost of offsite damage to the local environment, such as lost farm production, contaminated fisheries, or the forced outage of WPPS #2.

**DOE Programmatic Damage from Accidents.** This includes any added costs to DOE for remediation and restoration activities at Hanford and other facilities that result from an accident at Hanford. This is analogous to the Three Mile Island action plan requirements that were imposed on all commercial reactors after the Three Mile Island Unit 2 accident. An example might be that an accident at 101-SY would cause DOE to retrieve all single-shell tank wastes rather than leave them in place.

## INTEGRATED PRA SCOPE DESCRIPTION

The timing of potential HTF events and the consequence discussed above can be joined to define the time span of coverage of the PRA. Because of the potential delay between the time when hazardous materials are released into the soil and the time when they may produce health consequences, a two-dimensional concept of time is needed to describe the scope of coverage of the PRA. Figure 1 provides a graphical representation of this concept. The times of risk-producing events represented by the life cycle eras of the HTF are presented along the top axis from left to right. The vertical axis depicts the time when consequences from a release are realized. For acute health effects from atmospheric releases, there is no delay between the time of release and the time of consequence. For releases into the soil, however, there is a potential delay from the time of release until the material migrates offsite or the site boundaries are changed allowing public access to already contaminated areas. Using these two axes, nine hypothetical regions are defined for potential risk evaluation.

Region 1 represents the completed production era for which acute consequences have already been realized. Regions 2 and 3 represent the potential future consequences from releases that occurred during the production era. These potential future consequences are arbitrarily divided into time spans with and without continued restriction of public site access. Regions 4, 6, and 8 represent the potential future consequences from events occurring during the interim storage, remediation, and long-term storage eras while site use restriction is continued. Regions 5, 7, and 9 represent the potential consequences from events occurring in these eras after the expiration of site use restrictions.

The HTF PRA effort is divided into three phases. The first phase addresses health and economic risks for time scope region 4 (interim storage) from Tank 101-SY. This report

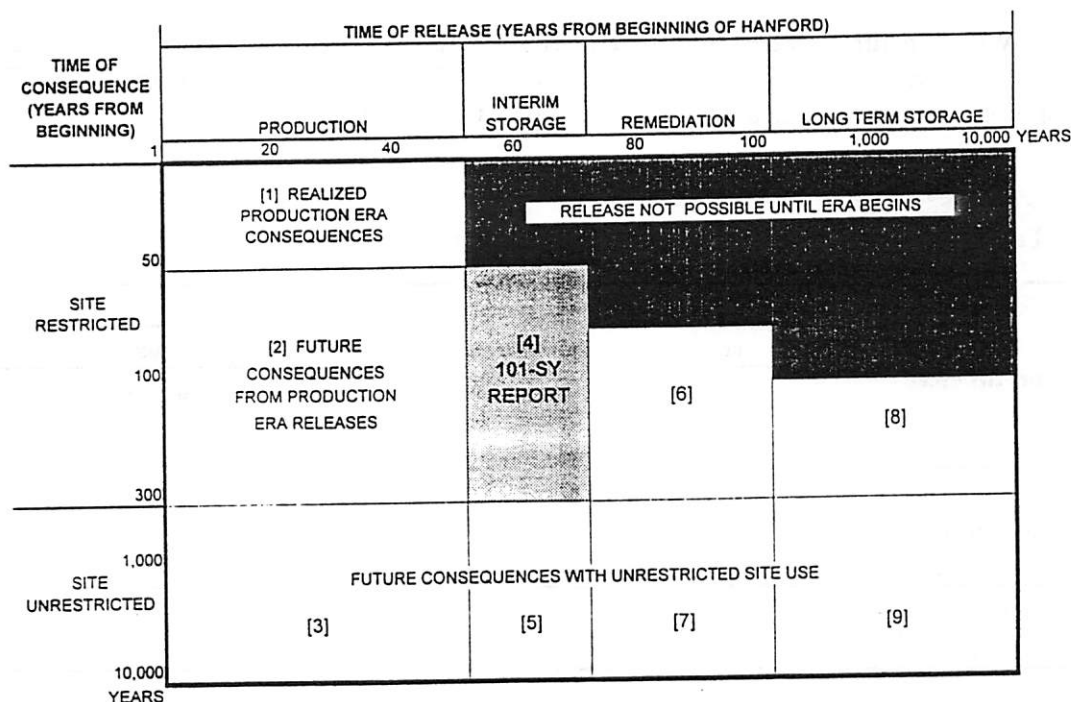


Figure 1. Hanford Tank Farm life cycle and scope of the PRA.

documents the results of Phase 1. Phase 2 will expand the evaluation for region 4 to all 177 storage tanks, and Phase 3 will address regions 6 (remediation) and 8 (long-term storage).

Time scope regions 3, 5, 7, and 9 are not included in this analysis because potential risks in the very long term are believed to be dominated by releases that have already occurred in the production era. These releases include approximately 200 million gallons of supernatant liquids skimmed from the tanks and deposited in cribs<sup>1</sup>, plus between 600,000 and 900,000 gallons from tank leaks.<sup>2</sup> Any additional leaks occurring during the interim storage or remediation eras will add only incrementally to the radionuclide inventory already in the subterranean environment at Hanford. Preliminary analyses of the potential risk from subterranean contamination indicate the following points:

- The leaked fluids are primarily composed of cesium 137 and strontium 90 plus much smaller quantities of longer-lived isotopes. Cs and Sr both exhibit half-lives of about 30 years and therefore will be substantially decayed away within about 300 years.
- Estimates of the time that it would take for these radionuclides to migrate beyond the current site boundaries range from 300 to 1,800 years. Thus, Cs and Sr may never migrate beyond the current site boundaries in significant quantities.
- Risks over the very long term will then be dominated by questions about the possible propagation of long-lived isotopes (released during the production era) through the subterranean environment and the very long-term access of the public

to the site. No decisions currently available to DOE management will influence the outcome of these questions.

With the time scope regions of interest identified above, the important consequence measures can be specified for each region to define the total scope of the PRA. Table 1 presents a matrix describing the total scope of the PRA.

Table 1. Integrated PRA scope definition matrix.

HTF LIFE CYCLE ERA	CONSEQUENCE MEASURES								
	HEALTH RISKS				ECONOMIC RISKS				
	Worker Accident Exposure	Worker Cleanup Exposure	Offsite Population Exposure	Delayed Exposure to Leaks	Expected Operating Costs	Technological Failure	Accident Onsite Cleanup Costs	Accident Offsite Collateral Damage	Accident DOE Programmatic Damage
Interim Storage [4]	1,2	1,2	1,2	1,2			1,2	1,2	1,2
Remediation [6]	3	3	3	3	3	3	3	3	3
Long-Term Storage[8]	N/A	N/A	N/A	3	3	3	N/A	N/A	N/A

1 PRA Phase 1, Tank 101-SY Only  
2 PRA Phase 2, All Tanks  
3 PRA Phase 3, All Tanks

## REFERENCES

1. J. D. Anderson, *A History of the 200 Area Tank Farms*, WHC-MR-0132, Table 6 (1990).
2. *Tank Farm Surveillance and Waste Status Summary Report for July 1992*, WHC-EP-0182-52, Appendix H (1992).

## **RISK MANAGEMENT APPLICATIONS AT THE INEL FOR ADVANCED TEST REACTOR OPERATIONS AND SAFETY AND ENVIRONMENTAL RESTORATION AND WASTE MANAGEMENT**

Steven A. Atkinson and Robert L. Nitschke

Idaho National Engineering Laboratory  
EG&G Idaho, Inc.  
P. O. Box 1625, Idaho Falls ID 83415

### **INTRODUCTION**

Risk management employing risk assessment methodologies is being actively applied for many different activities at the Idaho National Engineering Laboratory (INEL). The major applications under the jurisdiction of EG&G Idaho, the principal operating contractor at the INEL, are in the areas of operations and safety upgrades at major operating facilities such as the Advanced Test Reactor (ATR), for facilities hazards assessments, and for environmental restoration and waste management safety and risk assessment, operations, and program decisions.

The ATR has recently completed a major safety envelope analysis and upgrade program initiated in 1987 that included a full probabilistic safety assessment (PSA) and a strong risk management emphasis. With the completion of the base ATR PSA, the major focus of ATR PSA activity is now on risk management. The principal objective of the ATR PSA program has been to apply the results and insights from the PSA to guide safety improvements and to evaluate and prioritize potential facility or operational changes, questions or concerns. Risk management applications gain importance as ATR begins operating on a more restrictive budget which requires that only the "real" problems be addressed.

Risk analysis and risk management has become a major component of INEL environmental restoration and waste management programs in order to define responsible and cost-effective approaches to control and minimize the risks from residual waste and current and future waste management activities while also meeting federal and state requirements. Risk analysis techniques and risk communication play a key role in the decisions made, with public input, by the three responsible regulatory agencies (Department of Energy, State of Idaho, and Environmental Protection Agency) concerning sites with potential harmful health or environmental effects.

---

\*Work supported by the U.S. Department of Energy, Assistant Secretary for Nuclear Energy, under Idaho Operations Office Contract DE-AC07-76ID01570.

## **THE ATR RISK MANAGEMENT PROGRAM**

The ATR management organization directs the ATR PSA and provides risk management support. Most of the associated risk assessments are performed by the EG&G Idaho Risk Assessment Unit, a professional support group that provides risk assessment services for the Idaho National Engineering Laboratory and other Department Of Energy (DOE) facilities and for the U. S. Nuclear Regulatory Commission. The full ATR PSA model is on personal computer software for performing risk management evaluations. The development of simple software and training ATR support groups on its use is also being done for routine use that would not involve PSA model revisions.

ATR risk management activities, including a review of operational incidents and facility operating data, are compiled and reported to management yearly in an ATR Risk Management Report.

## **ATR PSA APPLICATIONS AND RISK MANAGEMENT ACTIVITIES**

The results, insights, and risk models of the ATR PSA are being used to address the following reactor operations issues:

- Defining risk-significant, cost-effective upgrades,
- Operational safety improvements such as operator training for transient management, procedures improvements, and for instrumentation and controls,
- Reviews of proposed facility or operational changes,
- Evaluation of operational occurrences and other safety or risk concerns,
- Providing guidance for aging and maintenance improvement programs,
- Provide input and guidance to other safety upgrade programs

### **Operational Safety**

A principal application of the ATR PSA has been to provide input to the development of upgraded emergency operating procedures now in use at the ATR. The ATR PSA defined important accident sequences, the important contributing component and human errors and their associated failure modes, and important system interactions or dependencies all of which are important for the development of emergency procedures. The ATR PSA included detailed human reliability analyses for the significant human errors which defined significant improvements in the emergency procedures. Additional improvements to emergency and abnormal operating procedures are being defined from the recently completed shutdown operations PSA.

### **Operational Occurrence Reviews**

Operational occurrences and other reportable ATR events are reviewed for their risk significance. All event and operations data are collected, tracked, and periodically updated to define current event and component failure frequencies for the ATR and to detect any significant trends. Effects of prior facility improvements show a trend of decreasing occurrences for several important initiators. However, as the facility ages, other component failure events are beginning to increase such as diesel generator failures and certain check valve failures which has identified a need to overhaul or replace these components in order to preserve the current low fuel damage frequency estimate.

## **ATR Safety Envelope Upgrade Program**

The ATR PSA is utilized to provide guidance, input, and reviews for the following ATR safety and operational upgrade projects:

- New process and experiment control systems and simulator upgrades
- Accident monitoring instrumentation and safety parameter display system
- Emergency planning upgrades
- ATR aging and life extension
- Safety equipment qualification
- ATR maintenance and surveillance improvements
- Updated ATR Safety Analysis Report and Technical Safety Requirements

### **Significant Applications**

Some of the significant risk management applications of the ATR PSA, besides the development of upgraded emergency procedures, have been:

- Identification of the most risk-significant and cost effective facility upgrades to significantly reduce the fuel damage risk exposure for external events (relocation of a battery-backed power system, diesel-generator pit flooding mitigation upgrades, and seismic upgrades),
- Identification of risk-significant and cost effective facility and operational upgrades to significantly reduce the risk for shutdown and cask handling operations (some of these were to simply recommend that certain operations be restricted to the period of shutdown when the reactor is defueled).
- Elimination of a \$2.5 million diesel generator electrical system upgrade shown to not be risk-significant and halving the cost of a battery-backed power system relocation project based on what was risk-important,
- Evaluating the fuel damage risk implications of component failures and outages as ATR equipment reaches end-of-life. Risk-based guidance is being provided on temporary, alternate operational configurations, acceptable outage times, surveillance, and possible Technical Specifications changes.
- Evaluating proposed operational upgrades and operational incidents for their risk-significance to provide management guidance,
- Defining the most risk-significant components and subsystems, based on both their importance to the PSA results and their significance if failed, for use in the aging, maintenance improvement, and environmental qualification programs. The confinement analyses for severe accidents performed for the Level 2 PSA also provided input to the environmental qualification study.

The ATR operates with buses that are continuously powered by an operating diesel generator and backed up by a fast auto-start diesel generator located separately from the running diesel generator. In addition, significant loads are on a swing bus that will automatically switch to off-site power upon a loss of the diesel generators. The external events analysis for the PSA defined potential flooding of the diesel generator pit (where the two machines used to normally provide diesel generator



power are located) as a dominating fuel damage risk contributor which resulted in the estimated fuel damage frequency being an outlier for nuclear reactors. The diesel pit flooding sequences were significant because of its location over the common electrical systems switchgear room, potential paths for the flooding to propagate directly to the critical switchgear, and the high frequency for the initiating event (diesel pit flooding had previously occurred several times). The battery-backed power system relocation and upgrades of diesel pit seals and drains essentially eliminated these sequences and reduced the estimated mean fuel damage frequency by 70%. Several seismic upgrades defined from the PSA decreased the fuel damage risk by another 5%.

## **ENVIRONMENTAL RESTORATION AND WASTE MANAGEMENT RISK MANAGEMENT ACTIVITIES**

Three types of risk assessment and management activities are performed for INEL environmental restoration and waste management programs. The first is a performance assessment for the disposal and control of radioactive waste. This involves a computational determination that waste disposal will meet performance objectives for chronic and acute exposures from released radioactivity now and into the future.

The second type of risk management activity supports safety analyses for waste management facilities operations and environmental restoration activities for former facilities and completed activities including decontamination and decommissioning (D&D). Risk assessment methods are used to define the dominant risk contributors so as to better identify and control the vulnerabilities. Final Safety Analysis Reports (SARs) have been completed for the three major waste management facilities operated by EG&G Idaho for the INEL; the Waste Experimental Reduction Facility (WERF), the Mixed Waste Storage Facility (MWSF) and the Radioactive Waste Management Complex (RWMC). WERF processes low-level radioactive waste (LLW) by compaction, incineration, and metal sizing operations. MWSF provides temporary storage for mixed LLW. RWMC is an 165 acre controlled access area with facilities and equipment to dispose of INEL generated LLW and to temporarily store and manage transuranic waste (TRU) received from the INEL and other DOE sites. Preliminary SARs have been prepared for the Dry Cask Storage Program and the Waste Characterization Facility (WCF).

Safety analyses including risk assessment have also been performed for environmental characterization or restoration activities in support of D&D of the INEL Hot Laundry and the former Boiling Water Reactor Experiment-V (BORAX-V), and to define an interim cleanup action for unexploded ordnance locations from when the INEL had been a U. S. Navy gunnery test range.

The third risk management activity pertains to remedial investigation and feasibility studies performed to define preferred alternatives for appropriate action to prevent, mitigate, or abate a potential release of hazardous substances from inactive waste sites. This activity is the one which makes the most use of risk assessments and risk-based decision making. A baseline risk assessment is performed to provide guidance for the evaluation of alternative actions including the possibility of no action.

Four hundred potential remediation sites have been identified at the INEL. About 90 of these have been subsequently identified as needing no remedial action. About 200 sites need only a screening evaluation in order to determine that no action is required (60 of these screening evaluations have been completed). About 150 sites need sampling data to confirm or refute their risk potential (15 of these have been completed). Twenty of these sites have been further classified as needing a baseline risk assessment to define or to evaluate remedial action alternatives. Three of these

assessments will be discussed as examples for the application of risk management methodologies for waste site environmental remediation decisions.

## **EXAMPLES OF RISK MANAGEMENT FOR WASTE SITE REMEDIATION**

Three examples of the application of risk assessment to define alternatives for waste site remediation consisting of very different contaminant situations are discussed. Note that risk management decisions for this process (under the CERCLA act) are the jurisdiction of the DOE Idaho Office, the State of Idaho, and the Environmental Protection Agency (EPA), Region X. These examples consist of:

- A site containing containerized disposed plutonium contaminated evaporation salts on a pad covered by soil. A baseline risk assessment was conducted to determine the incremental risk to the public and the environment if no action was performed to determine what if any action would be needed.
- A unlined pond formerly used for the disposal of low-level radioactive waste water. An interim action risk assessment was performed for potential on-site worker exposures to determine the risk to the workers and to assess potential alternative actions.
- A site with leaking volatile organic contaminants from shallow buried drums. A baseline risk assessment was conducted to determine the incremental risk to the public and environment if no action was performed based on an assumed future hypothetical residential exposure. This risk assessment was then used to determine whether remedial action was prudent.

### **Risk Assessment for Buried Containerized Radioactive Waste**

The site for the first example was a disposal site constructed in 1972 to handle and store containerized radioactive waste contaminated with less than 10 nCi/g of TRU. This waste was predominately evaporator salts from waste water treatment at another DOE facility site. The containers consisted of 55 gallon drums and plywood boxes. The containers were stacked horizontally in staggered layers on an asphalt pad. In 1978 the site was closed by placing plywood or polyethylene over the containers followed by about 1.4 m of soil. At the time of closure, there were over 18,000 55-gal drums and 2000 plywood boxes for a total volume of over 10,000 cubic meters of waste.

The baseline risk assessment for this first example was conducted to determine the risk to the public and to the environment if no remedial action were taken. The evaluation assumed 100 years of institutional control over the site followed by 1000 years with no control. Both an occupational and a hypothetical future residential exposure scenario were considered with up to five exposure paths (soil ingestion, soil inhalation, direct exposure from radionuclides, ingestion of ground water and of home-grown produce).

The risk characterization indicated that the carcinogenic risk for current and future scenarios was below or within the National Contingency Plan acceptable risk range (Code of Federal Regulations, Title 40, Part 300) of  $10^{-4}$  to  $10^{-6}$ . The only potentially unacceptable result was for an infant about 200 years into the future from nitrate contamination of the groundwater. Based on this assessment, it was decided to take only limited action to contour the soil cover and to monitor water infiltration and the erosion rate over two years to confirm the sufficiency of the assessment.

## **A Nuclear Facility Decommissioned Low Level Waste Pond**

The subject of the second example is an unlined pond which had been receiving LLW water from operating nuclear reactors since the early 1950's and other waste water from cooling tower blowdowns, ion-exchange wastes, and supporting laboratories. The pond and its three waste water infiltration/evaporation cells covers approximately four acres.

Water evaporation and infiltration over the years has resulted in the pond sediments becoming highly contaminated with Co-60 and Cs-137 radionuclides and hazardous chromium. After construction of a new lined pond, an evaluation was needed to help determine the best interim action to take with regard to the now abandoned pond. A risk assessment was conducted to determine the risk to a worker at the reactor site located at the downwind edge of the abandoned pond. The assessment examined three exposure pathways: inhalation of soil contaminated air, ingestion of contaminated soil, and direct exposure to gamma radiation.

The results of the risk assessment were that the cancer risk from the direct exposure path could be well above the acceptable range. The other exposure paths resulted in acceptable consequences. Therefore, action to protect the workers at the site was decided upon. An initial decision to remove cesium by chemical extraction was abandoned after failure of pilot scale tests. Since the predominate risk is exposure to the Cs-137 daughter gamma rays, the current action is to consolidate the pond sediments into a smaller area and to back fill the area of the sediments with clean soil.

### **Subsurface Organic Contamination**

The third example is for organic contamination, mainly from solvents such as carbon tetrachloride, of the subsurface or the vadose zone from wastes disposed over a 20 year period. Over 88,000 gallons of organic wastes from several DOE sites had been disposed of in this area until 1970. The contaminants were usually mixed with calcium silicate to form a viscous sludge which was double-bagged and placed in 55 gallon drums. The drums were placed in shallow pits and covered with a soil layer.

A baseline risk assessment was conducted for the leaking drums at this site to determine the incremental risk to the public and the environment if no action were taken. The evaluation assumed 100 years of institutional control and then proceeded about 150 years into the future at which time the contaminant concentrations had peaked. Both an occupational and a hypothetical residential exposure scenario were considered with five exposure routes. The five exposure routes in this case were inhalation of vapors, ingestion of contaminated soil, ingestion of contaminated water, inhalation of vapors from contaminated water while showering, and ingestion of contaminated home-grown produce.

The evaluation determined that the potential carcinogenic risks were slightly above the acceptable risk range for hypothetical receptors. The risks were dominated by inhalation of vapors and ingestion of groundwater. Although the risks were small and just marginally unacceptable, a decision was made to remediate the vadose zone since a suitable technology was available for vapor vacuum extraction.

## **DECISION ANALYSIS IN ENVIRONMENTAL RISK MANAGEMENT: EVALUATING MULTIPLE STAKEHOLDER/MULTIPLE OBJECTIVE DECISIONS**

David C. Bell, George Apostolakis, and William E. Kastenberg

Mechanical, Aerospace & Nuclear Engineering  
University of California, Los Angeles  
Los Angeles, CA 90024-1597

### **INTRODUCTION**

The need for achieving maximum risk reduction with minimum cost expenditures in the course of environmental remediation is becoming increasingly more important. When groundwater is contaminated, the many complex and interrelated issues involved make remediation a difficult task, subject to intense regulatory and public scrutiny. The engineering processes and technologies chosen for a remediation effort must be evaluated in terms of their ability to satisfy regulations and their cost. However, spatial variability of hydrogeological features and data limitations invoke very large uncertainties that system optimization cannot address. Environmental remediation decisions can no longer be based solely on a single objective such as cost. Environmental remediation managers must make decisions that not only satisfy their own objectives, but also those of other stakeholders, namely their regulators and the public. These stakeholders also play a role in the remediation process. Regulators are required by law to make decisions that affect the remediation effort, while an environmentally-conscious society desires involvement in the decision-making process. Environmental remediation is then further confounded by the fact that each stakeholder is impacted by decisions of the other stakeholders.

This paper describes work in progress to develop a risk management/decision analysis methodology used to model decision consequences for multiple stakeholders in environmental remediation. The methodology is based on the use of a conditional influence diagram to model the inter-relationships among various stakeholder groups and objectives in a risk-based decision analytical-framework. An influence diagram can encapsulate the complex relationships that are important when evaluating available remediation options and quantifies the decision options. Game theory is then used to assess resolution when conflict among the multiple stakeholders is possible. The methodology is to be used as a decision making tool in an environmental decision support system.

## THE PROBLEM

The problem to be addressed is a contaminated site where a volatile organic compound (VOC) from a facility has entered the subsurface over a long period of time and has contaminated the groundwater. Site characterization has shown that a contaminant plume, as high as 1,000 ppb, has formed in the saturated zone and is moving with the natural groundwater flow toward a commercial water producing well. Hydrogeologic analysis has determined that the plume is at some depth and is not expected to reach the well for over 200 years. A baseline risk assessment estimates an incremental individual lifetime (70-year) risk of cancer on the order of  $1 \times 10^{-7}$ . The facility owner is still required to remediate to prevent further degradation of groundwater resources. Figure 1 illustrates the relationship between the reduction of average contaminant concentration and the cost of remediation over time. The facility owners are required to reduce the contaminant concentration to a certain level, known as the maximum contamination level (MCL), determined and enforced by the regulator. However, natural retardation processes cause the rate at which the VOC concentration is reduced to decrease as the concentration level approaches the MCL. This significantly lengthens the time required to achieve cleanup, or even prevents total cleanup.

In this situation, the facility owner sees (Figure 1) that approximately 50% of the total costs are spent to remove the last few percent of the contamination. The facility owner feels that money spent in the last phases of pump-and-treat remediation are disproportionate to the relative risk reduction obtained. Significant cost savings can be realized by stopping the remediation process when it is no longer cost effective and letting natural degradation processes take over. The facility owner wishes to petition the regulatory agency for an alternate contaminant level (ACL) that will significantly shorten the time required for operating the remediation process, and hence reduce cumulative cost as shown in Figure 2. The facility owner must provide compelling reasons as to why an ACL should be granted, and the RA must decide upon the acceptability of an ACL.

The argument for, and the acceptability of an ACL is complicated by several things. First, there is the issue of uncertainty. There are many inherent uncertainties involved in subsurface remediation that both create and complicate decision-making for the facility owner. For example, while the contaminant plume may be identified, its boundaries and the mass of the contaminant in the plume are still uncertain due to varying natural properties and data limitations. The facility owner is also faced with limited resources in which to conduct remediation. This leads to an underlying conflict with the regulatory agency, which is obliged to enforce regulations regardless of other constraints. Finally there is the local community; which demands unconditional safety, and wants to be included in the decision making process. Decision analysis is the ideal method to rationally confront these issues since it is intended to deal with complex issues involving uncertainty.

## METHODOLOGY

The risk management/decision analysis methodology developed here is based on the risk management framework for two stakeholders of Hong and Apostolakis (1993). The methodology utilizes the essence of decision analysis where information is collected and evaluated before another decision is made. One advantage of decision analysis is in the treatment of uncertainty by encoding informed judgment in the form of probability assignments to events and variables. The methodology also uses risk-based objectives in the decision analysis since one of the major objectives is the reduction of risk (Kastenberg and Cave, 1990). The work described in this paper will apply these concepts and tools to the groundwater remediation problem described above.

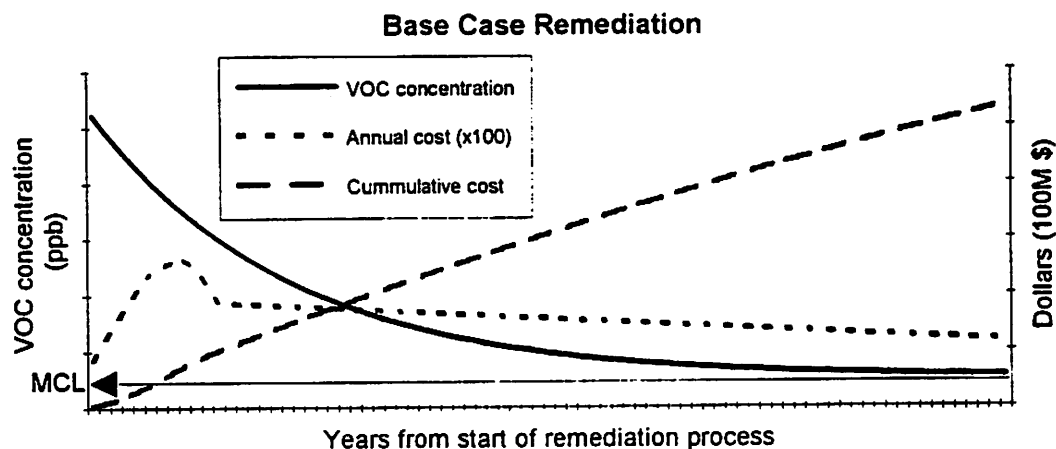


Figure 1. Base Case Remediation Chronology

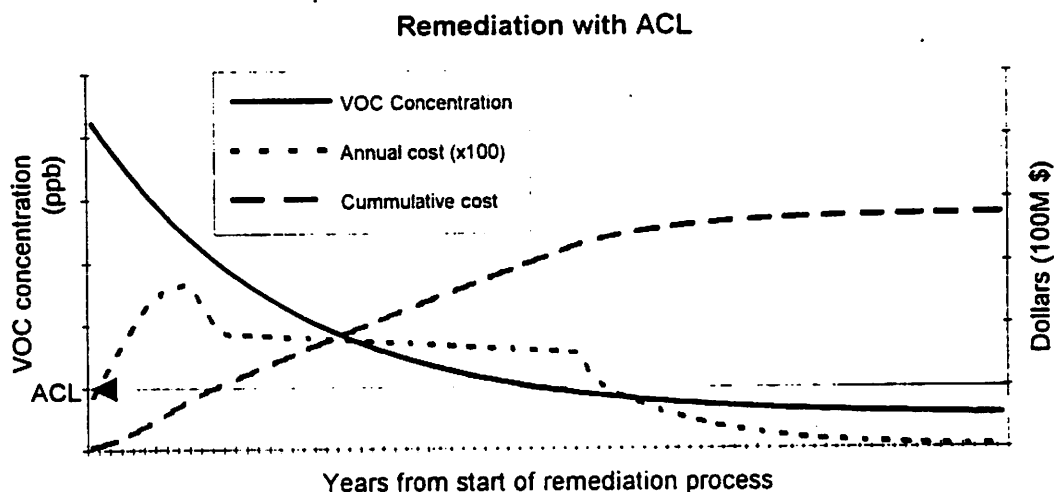


Figure 2. Remediation to ACL Chronology

In order to develop the methodology, the facility owner (FO) is identified as the stakeholder responsible for cleaning the groundwater. The degree of remediation to be done is determined by the regulatory agency (RA), which is the stakeholder charged with establishing and enforcing the relevant requirements. While the FO is primarily concerned with achieving remediation goals in the most cost expedient manner, the RA is primarily concerned with the protection of public health and the environment. A certain amount of conflict exists between the two stakeholders when the policy of meeting all the applicable remedial requirements may be incompatible with the limited resources available to the FO. Both stakeholders must be cognizant of the uncertainties involved and respond to the public's perceptions of risk when making decisions.

Development of the methodology used here begins with a decision structure that aims to capture the issues involved with a specific remediation decision, the attributes that result from the decision, and the degree to which objectives are fulfilled. From this structure an influence diagram is formulated to model the flow of information and the variability of parameters affecting the decision. The influence diagram used here models the conditional effect of one stakeholder's decision on the other, as Hong and Apostolakis (1993) describe.

The influence diagram is used to evaluate each available decision alternative of one stakeholder, conditioned on each available decision of the other stakeholder. In this manner, alternative pairs are formed representing values for the primary and the conditioning stakeholder. If the decision structures for the stakeholders are different, then a separate influence diagram is built for each. Values assigned to the outcomes are put in the form of a bimatrix for use in game theory analysis.

To continue describing the situation used to demonstrate this methodology, the following scenario is hypothesized. It is felt that in order for the FO to get the ACL exemption, the FO must give something in the form of a tradeoff. The FO proposes to double the pumping rate to be used in the remediation process to appease the public by expediting the time to cleanup. The higher pumping rate will cost the FO money now, but may save money later. The RA may be indifferent to the pumping rate, but the public may be more satisfied with faster cleanup.

## INFLUENCE DIAGRAMS

Influence diagram formulation follows the definition of influence diagrams as given by Howard and Matheson (1981) where three levels of specification are distinguished for a decision problem: relation, function and number. The level of relation uses decision, chance, and value nodes to portray the dependence of variables on each other. A complete description of influence diagram terminology is found in Howard and Matheson (1981).

The influence diagrams used to analyze the groundwater remediation situation discussed above are described here. The level of relation for the site owner's influence diagram is shown in Figure 3. It begins with a decision node, **FO choose Q**, representing a binary decision between two alternative pumping rates,  $Q_1$  and  $Q_2$ . Decision nodes are drawn as squares in the figure. **Time to Cleanup** is the attribute dependent upon the chosen pumping rate. **Time to Cleanup** is also dependent upon the source contaminant level, **Co source**, and the MCL established by the RA. Since the contaminant level is uncertain, the **Time to Cleanup** is also uncertain and both are represented as a chance nodes, are drawn as ovals. Since this is the FO's influence diagram, the decision of the RA to **choose the MCL** is the conditional decision node, distinguished by the dashed square node. Another attribute affected by the choice of MCL is the **70-year average concentration** at the exposure point, which is the down-gradient drinking water well. This is because the MCL determines the mass of contamination that is now able to migrate down gradient to the well. The **70-year Average Concentration** is also affected by many hydrogeologic parameters, primarily the hydraulic conductivity, and this influence is represented by the arc from **Hydraulic Conductivity** to the **70-year Average Concentration** chance node. This concentration attribute then directly determines the **Health Risk**, which is one of our objectives, and is a combination chance/value node. Returning to the **Time to Cleanup** attribute, this factor is a direct predecessor to the second objective, **Cleanup Cost**, since it determines how long the extraction pumps shall be run. **Cleanup Cost** is also a chance/value node, but is also dependent on the pumping rate chosen, as shown by the influence arc drawn from the FO decision node to the **Cleanup Cost** node. **Time to Cleanup** also affects the third objective, **Public Satisfaction**. While the public desires an expedient cleanup, they know that a higher MCL will mean a higher resultant health risk, and therefore **Public Satisfaction** is also dependent on the **Health Risk** chance/value node.

The influence diagram for the RA is exactly the same in terms of the level of relation, however the primary and conditional decision nodes are switched. The decision for the RA is to choose between the MCL or ACL. This decision is now conditioned on the decision of the FO to choose a pumping rate and thus the **FO choose Q** node will be distinguished by

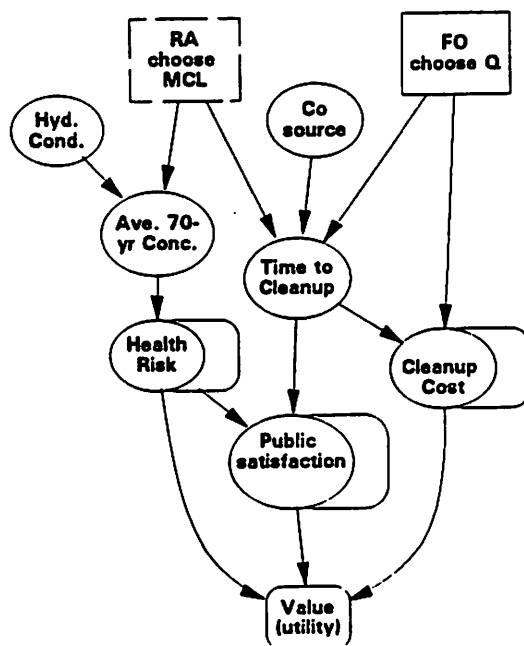


Figure 3. Influence Diagram for Facility Owner (FO), conditioned on Regulatory Agency (RA).

the dashed square node. This modeling represents the potential conflict that exists between a site owner and a regulator.

Influence diagrams are useful in portraying the decision analysis concept of explicitly accounting for parameter uncertainty and propagating them through the decision structure. For example, the source concentration ( $Co$ ) in the plume is assigned a distribution of values to represent its variable nature. This distribution will affect the Time to Cleanup and consequently the Cleanup Cost and Public Satisfaction. Propagation of the uncertainty is done either numerically, such as by a Monte Carlo method, or analytically.

The level of function for the influence diagrams is important to assign values to the decisions. The Time to Cleanup node is developed from a simple mass balance of a well-mixed tank model for contaminant removal. The mass balance is solved as an expression of time to achieve the desired MCL so that

$$time = \frac{-\ln(MCL/Co)}{\left(\frac{Q}{V_w R} + \frac{\lambda}{R}\right)} \quad (1)$$

where  $Co$  is the source concentration present,  $V_w$  is the volume of groundwater containing the VOC,  $Q$  is the pumping rate selected,  $R$  is the retardation factor for the VOC, and  $\lambda$  is the natural decay rate coefficient. The function level for Health Risk is simply the product of the 70-year average concentration, the exposure, and the cancer potency factor for the VOC. Cleanup Cost is determined from a linear relationship based on the time to cleanup and the chosen pumping rate. The function level for the 70-year Average Concentration node can be any solution to the advection-dispersion transport equation for a one dimensional flow, two-dimensional dispersion, homogeneous medium. Public satisfaction is measured with a constructed scale.



## EVALUATION

The influence diagram includes three objectives upon which the stakeholder will evaluate its decision. If a decision is made based on these absolute values, then the attitude of the stakeholder and actual worth of an objective to the stakeholder is neglected. Utility theory is used to include the stakeholders attitude, such as being risk averse, in the decision making process and to give proper weighting to the objective. Utility is also able to combine the three objectives with different units into one value. First, each objective is converted into a utility that reflects the stakeholder's decision making attitude. Then the utilities are combined in a multiattribute utility analysis using an equation like

$$u(x) = \sum_{i=1}^n k_i u_i(x_i) + k \sum_{i=1}^n \sum_{j=1}^n k_{ikj} u_i(x_i) u_j(x_j) + k^2 \sum_{i=1}^n \sum_{j=1}^n \sum_{l=1}^n k_{ikjkl} u_i(x_i) u_j(x_j) u_l(x_l) \quad (2)$$

where  $k_i$  and  $u_i$  refer to the scaling constants and utility for each objective (i) respectively; and  $k$  is the multiattribute scaling constant. For a situation where there are two stakeholders with two alternatives on which to decide, there will be 8 solutions forming four alternative pairs of results. These results usually show a conditional decision-making process. For example, the FO will choose a pumping rate of  $Q_1$  if the RA sticks with the MCL, but will choose to pump at  $Q_2$  if the RA allows for the ACL. Game theory is then used to portray that the first apparent solution, called the equilibrium solution, is often not the optimal solution where both stakeholders will be better off if they cooperate.

Once the decision structure and influence diagram model have been established, other evaluations can be conducted. Tradeoffs between the stakeholder groups can be evaluated. Uncertainty analysis will provide insight as to the effect of uncertainty on the decision making process. Decision making uncertainty may be reduced by obtaining information, but obtaining information may be cost prohibitive with little or no added benefit. A value of information analysis will help a remediation manager determine if collecting more field information is valuable to meeting the objectives. These analyses should help to provide a means of identifying the appropriate level of characterization needed for remedial actions, and an appropriate level of effort to demonstrate compliance.

This methodology can be incorporated into a Decision Support System (DSS) to be used by environmental restoration decision makers to determine optimal solutions. It can also be used as a communication tool to demonstrate to all the stakeholders, the impacts of their decisions. With these tools, the question of "How clean is clean?" can then be addressed.

## REFERENCES

- Hong, Y., and Apostolakis, G., 1993. Conditional Influence Diagram in Risk Management, to appear in *Risk Analysis*.
- Howard, R.A., 1983, The Evolution of Decision Analysis, in "Readings on the Principles and Applications of Decision Analysis," Vol. 1, R.A. Howard and J.E. Matheson (eds.), Strategic Decisions Group, Menlo Park, Calif., 6-16.
- Kastenberg, W., and Cave, L., 1990. Value/Impact Assessment for the Evaluation of Risk Reduction: Development of a Framework, *Reliability Engineering and System Safety*, 28, 205-227.

## **RISK ASSESSMENT DATA BANKS AT THE SAVANNAH RIVER SITE**

**Christina S. Townsend, William S. Durant, Donna F. Baughman**

**Nuclear Processes Safety Research  
Savannah River Technology Center  
Savannah River Site  
Westinghouse Savannah River Company  
Aiken, SC 29802**

### **INTRODUCTION**

In the risk assessment business, it is a well known fact that past mistakes will not be remembered if nothing is done to record them and make them available for future reference and review. The Savannah River Site maintains a computer database system for non-reactor facilities that contains a compilation of the incidents that have occurred since the start up of the Site in 1953. The nationally recognized data banks are highly valued across the U. S. Department of Energy (DOE) complex for their use in risk-related analyses. They provide data for uses such as failure rate analyses, equipment reliability and breakdown studies, project justification, incident investigations, design studies, Safety Analysis Reports, Process Hazards Reviews, consequence analyses, quality assurance studies, trend analyses, management decision, administrative control effectiveness studies, and process problem solving.

Five risk assessment data banks exist in the areas of reprocessing, fuel fabrication, waste management, tritium, and the Savannah River Technology Center. The data banks are comprised of approximately one-third million entries collectively and continue to grow at a rate of about two hundred entries per day.

### **DATA COLLECTION HISTORY**

The incident collection effort was begun in 1973 initially for the nuclear fuel reprocessing and waste management facilities at the Site. Available written information concerning incidents involving equipment failures, process upsets, operating errors, facility and personnel contamination, personnel injuries, environmental insults, etc. was gathered and abstracted into the data bank by a team of five technical analysts. The philosophy of the analysts was that if the event was of sufficient concern to be recorded, then it was important enough to include in the data bank. The analysts used five sources of data: incident reports, daily and monthly status reports, audit records, fire department records, and equipment histories. After a 20 man-month effort, 8000 entries dating back to 1953, when the Savannah River Site was started, were abstracted into the original data bank.

As more value was placed on keeping an incident history for use in risk assessment and as reporting requirements increased, many new sources of information became available to the data bank analysts, and the data collection effort grew. Today a vast collection of internal sources, both published and unpublished, are provided by the facility

managers and reviewed daily by analysts to identify events that should be recorded in the data banks (Table 1).

**Table1. Example source documents.**

Published data sources	Unpublished data sources
<ul style="list-style-type: none"> <li>• Operating incident reports</li> <li>• Special hazards investigations</li> <li>• Plant technical monthly reports</li> <li>• Daily teletypes</li> <li>• Fire department reports</li> <li>• Works engineering monthly reports</li> <li>• Waste management monthly reports</li> <li>• Criticality audits</li> <li>• Power department incident reports</li> </ul>	<ul style="list-style-type: none"> <li>• Senior supervisor log books</li> <li>• Health protection department log books</li> <li>• Burial ground log books</li> <li>• Waste management log books</li> <li>• Salvage yard receipt records</li> <li>• Canyon crane log books</li> <li>• Decontamination log books</li> <li>• Maintenance log books</li> </ul>

As the risk-based safety analysis effort at the Savannah River Site grew, the need for data banks for the other major facilities on the site was identified. New data banks were developed for the fuel fabrication facilities, tritium facilities, and the Savannah River Technology Center. Collectively, the data banks contain a compilation of approximately 370,000 events.

## DATA DESCRIPTION AND USES

Incident information recorded in the data banks includes a description of the incident, where and when the incident occurred, the source documents from which the incident was abstracted, the type of incident, repair times, and consequences. Some typical examples of information contained in the data banks include data on fires, robots, instruments, nuclear criticality potential, computers, pumps, valves, etc (Table 2).

### Table 2. Example events

Acc#	Source	Date	Area	Facility	Operation	Equipment
78571	28	02/04/80	F	I	A6	076
	02				44	066
	49					
MAINT RM - AT APPROX. 10:05 AM, FIRE ALARM BOX NO. 32 SOUNDED. ELECTRIC MOTOR ON ARGON PURIFICATION UNIT UNDER CAB. BURNED INTERNALLY ACTIVATING HALON FIRE SUPPRESSION SYSTEM. 8-4						
44182	27	04/16/80	F	B	44	608
	01					589
	10					412
	07					464
	28					076
	36					030
						216
						153
PIPE WELDING OPERATION INSIDE PLASTIC CONTAINMENT HUT IN JB-LINE CAUSED IGNITION OF PLASTIC TAPE AND CONSUMPTION OF 1.5 SQ. FT. OF HUT PLASTIC. TAPE WAS NOT FIRE RETARDANT IN VIOLATION OF DPSOL. POTENTIAL FOR CONTAMINATION AND BURNS TO WELDER. SI-80-4-46. OI-221-F-JB-80-4. 1046X10-12MICROCI PU/CC.						
102485	28	05/28/80	F	M	86	468
					44	524
						024
						206
						076
SANITARY LANDFILL - BUILDING 740-G - THE FIRE APPARENTLY WAS CAUSED BY FAILURE OF A GASKET AT THE FUEL FILTER WHICH RESULTED IN FUEL SPRAYING ON A HOT EXHAUST MANIFOLD.						

The data banks were originally developed for use in risk-based safety studies at the Savannah River Technology Center, but many other uses for the data have been identified (Table 3).

**Table 3. Data bank uses.**

- Failure rate data
- Equipment breakdown histories
- Generic incident histories
- Dates of specific incidents
- Consequences of incidents
- Repair/response times
- Data for design studies
- Data for quality assurance studies
- Trend analyses
- Data for project justification
- Data for process hazards analyses
- Training
- Process problem solving
- Management decision data
- Administrative controls effectiveness studies
- Incident audits
- Data for reliability studies
- References to source documents

## COMPUTER DESIGN HISTORY

The cost of maintaining the data banks has always been a concern to DOE and to the Site managers. Technological advances in the computer industry have contributed to the growth and data retrieval efficiency of the data banks while reducing the cost of maintaining them.

The original data bank was handwritten by technical analysts. In 1974 the data were transferred to punch cards where they were updated periodically by technical personnel. When magnetic storage media were developed, the data banks were stored on an IBM mainframe and manipulated by a collection of FORTRAN and JCL programs. Processing data was cumbersome, and retrieving data for analysis was not interactive and thus had to be done by the data management group upon request. Technical personnel were still needed for much of the data processing, although clerical personnel were handling some of the tasks.

Today all of the data banks, except the classified tritium data bank, are maintained in a state-of-the-art central interactive database system which is supported by a full-time computer scientist. The system resides on a VAX 6620 computer and was developed using a commercial database software package. The processing of information is handled by clerical instead of technical personnel. The data management effort is now handled by a data specialist, who acquires the source documents, tracks the abstracting and input process using a computerized data logging system, and manages the clerical staff.

Expert systems programs have also been developed to analyze and categorize the incidents, choosing from approximately 1000 categories, for data standardization and retrieval efficiency (Table 4). This effort was previously a tedious manual task done by technical analysts, who are now free to concentrate on researching the source documents for events. Such improvements allow the staff to process approximately 200 new entries per day.

**Table 4. Example incident categories.**

Unit operation identifiers	Equipment and keyword identifiers
<ul style="list-style-type: none"> <li>• first cycle solvent extraction</li> <li>• second uranium cycle</li> <li>• fuel storage</li> <li>• dissolving</li> </ul>	<ul style="list-style-type: none"> <li>• agitator</li> <li>• air reversal</li> <li>• ammonia compounds</li> <li>• band saw</li> </ul>

- ion exchange, canyons
- solvent washing
- cold feed
- solution adjustment
- precipitation
- filtration
- roasting / dehydration
- reduction / calcination
- special recovery
- product storage and accountability
- waste handling
- cask operations
- fuel and target operations
- resin regeneration
- laundry
- GP waste and chem makeup tankage
- transfer tanks
- acid recovery
- crane and hoist operations
- first level
- transport by truck
- sampling
- inspections
- breathing air
- boiler
- chemical addition error
- clothing contamination
- derail
- dropped / fell
- emergency power
- explosion
- fatality
- generator
- hepa filter
- improper storage
- injury
- leaks
- mislabeled
- nitric acid
- release, environmental
- spill
- tank 48
- transfer error
- uncontrolled reaction
- valving error
- warm crane

## DATA RETRIEVAL AND MANIPULATION

Retrieval of information can be accomplished by searching the databases using any combination of information that describes common incidents (e.g. all incidents that occurred in the F-Canyon fuel reprocessing facility in June of 1991 involving false alarms but not false nuclear incident monitor alarms). Information can be viewed on-line or by generating hard copy reports. Statistical analyses, such as trending, generating repair times, response times, incident duration, and initiator frequencies can be performed within the system. Such analyses are routinely provided to customers across the Site and the DOE complex (Figures 1 and 2). More extensive analyses, such as calculating failure rates and determining root causes, are also a customer service available using the information stored in the data banks.

Anyone on the site network who has a database account can view the data on-line, produce hard copy reports, and execute statistical programs to perform calculations. A training program is in place to train engineers across the site to use the system. Many customers now retrieve information on their own, which further reduces the cost of providing information from the data banks to customers. At present, the number of users performing their own searches is about half of those performed by the data managing group for customers per month.

Off-site customers can also obtain data bank information. Department of Energy and contractors can contact the data managing group to receive information. All other customers, such as sub-contractors, can request information from the Department of Energy Operations Office at the Savannah River Site.

## CONCLUSION

The data banks at the Savannah River Site continue to be recognized by their customers across the DOE complex as invaluable resources to the safety analysis and risk management effort at nuclear facilities. On a scale of 0 to 5, with 4 being excellent and 5 being outstanding, data bank customer service has consistently been rated a 4.5.

The banks will continue to grow, and enhancements are continually made to the system based on overall value to the risk assessment effort, on customer feedback, on cost, and on a continuing goal to increase the utilization of the data banks.

**REFERENCES**

Durant, W.S., Galloway, W.D., and Lux, C.R., 1988, Data bank for probabilistic risk assessment of nuclear-fuel reprocessing plants, *IEEE Transactions on Reliability* . 37:2.

Figure 1. Trend plot.

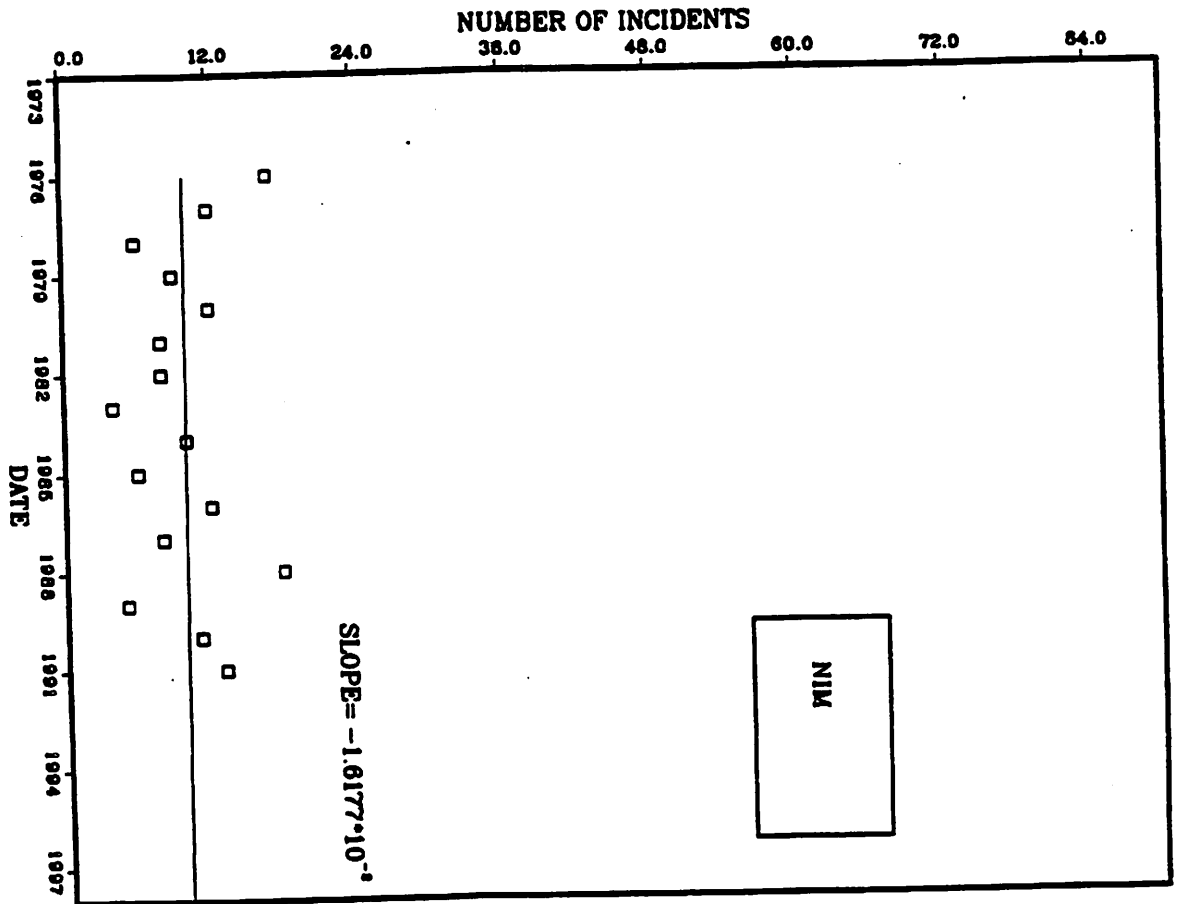
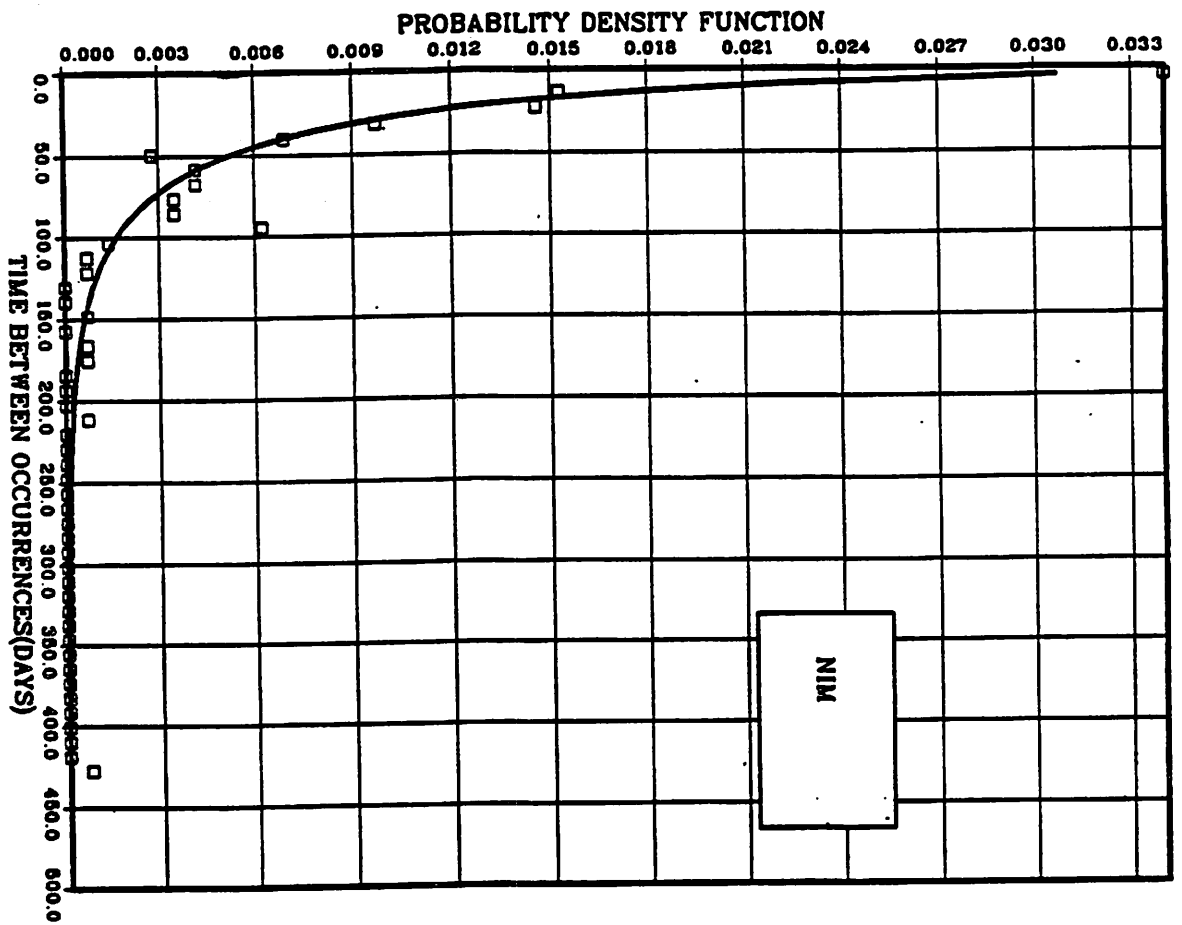


Figure 2. Distribution curve.



## **DATA WORTH ANALYSIS FOR PERFORMANCE ASSESSMENT USING INFLUENCE DIAGRAMS**

Janis E. White<sup>1</sup> and A. Sharif Heger<sup>2</sup>

<sup>1</sup>INTERA, Inc. 1650 University Blvd., Albuquerque, New Mexico

<sup>2</sup>University of New Mexico, FEC 247, Albuquerque, New Mexico

### **INTRODUCTION**

Data worth analysis using influence diagrams is a new methodology that can be used in decision making problems. This methodology provides a coherent structure for determining an optimum decision with respect to the need for additional data and is a natural interpretation of the utility function associated with the influence diagram for the specified decision problem. Advantages of using this methodology include the ability to design data collection experiments with a specific worth, clear enunciation of interdependencies among components of the decision problem, direct incorporation of expert knowledge, a simple visual representation of these relationships and the flow of information required to reach a solution, and a straightforward transcription of the methodology to an automated computer algorithm.

The use of influence diagrams in data worth analysis is shown in detail by applying it to a hydrological decision problem. The first section of this paper describes the state of the art in performance assessment decision analysis and establishes the importance of data worth analysis in the presence of limited resources. This section is followed by the definition of the influence diagram and a discussion of its properties. Next, influence diagrams are constructed for the data worth problems given in Freeze, et al. (1992). These constructions illustrate how these diagrams use their graphical structure to model uncertainties as well as the sometimes obscure flow of information in the decision making process. Constructing an influence diagram is itself a useful analytic tool in the sense that the underlying decision problem can become more clearly understood in terms of information flow. The influence diagram results are compared to the decision trees and accompanying tables that appear in Freeze et al. (1992) to demonstrate the simplicity of data worth analysis based on the influence diagram. The paper concludes with a description and demonstration of a new computer code (Bridge) as used for data worth analysis.

### **DATA WORTH ANALYSIS IN PERFORMANCE ASSESSMENT**

Stringent budgetary constraints coupled with increasing regulatory burdens demand the decisions to gather data be based on cost-conscious considerations as well as uncertainty reduction. Except for pathologically ill-conceived tests, additional data will always reduce some uncertainties in a model. So reducing uncertainty can no longer be the sole justification for consuming limited resources. Decision makers must now be able to assess the cost-effectiveness, or worth, of additional data. Data worth analysis addresses this need as well as the similar need identified by the Department of Energy (DOE) in its Applied Development,



Demonstration, Testing, Evaluation Plan (1989), Section 2.2.2.3. The DOE called for a methodology to reduce uncertainty and data collection that would result in a prioritization of data requirement along with recognizing critical assumptions in the problem.

Data worth, the value of data that could be collected as part of the decision-making process, is represented as the change in the utility function of the decision problem. This method is naturally amenable to formal mathematical optimization techniques and so gives decision analysts all the necessary tools to assess the worth of various data with respect to reducing uncertainty, for example, or minimizing risk.

Decision analysis in complex systems and situations such as performance assessments requires methods for efficient and complete modeling of factors influencing the decision. Applying influence diagrams in combination with data worth analysis produces a method which not only satisfies these requirements but also gives rise to an intuitive representation of complex structures not possible in the more traditional decision tree representation. In addition to appealing to intuition, data worth analysis using influence diagrams is a rigorous description of the general decision problem and may be automated by transcribing the diagram into a straightforward code.

## INFLUENCE DIAGRAMS

Influence diagrams are typically used to model situations with uncertainty and interdependencies. These diagrams visually depict sources of uncertainty, dependence, and flow of information into decision nodes. Incorporating Bayesian analysis with mathematical random graph theory, these diagrams carry with them the methodology for analyzing their structure.

An influence diagram is a directed graph with no cycles that visually displays relationships between uncertain quantities and the flow of information about such quantities in the decision making process. As originally conceived by Miller et al. (1976), the influence diagram is a high-level graphically-based tool for decision makers. The result is intuitive representation of the underlying decision problem that can be readily grasped by decision makers while at the same time is rigorous enough to determine numerically the value of various decisions as defined by the utility function of the problem.

For decision making problems the influence diagram has three kinds of nodes, as shown in Figure 1. Chance or random nodes are drawn as circles and represent uncertain quantities. Decision nodes are drawn as rectangles and represent decision functions whose values correspond to the decision alternatives. Finally, every influence diagram in decision making has a value node. The value node is drawn as a diamond and is the terminal node of the diagram. It represents the utility or value function associated with the decision problem. Some authors such as Jae and Apostolakis (1992) use a "deterministic" node drawn as a double circle to show fixed parameters, but such nodes are merely a special case of chance nodes and so will not be distinguished here.

In addition to having three kinds of nodes, the influence diagram has two kinds of arcs. Arcs incident to, or going into, a chance node show conditional dependencies and are known as conditional arcs. Arcs incident to a decision node depict the information that must be available at the time the decision represented by that node is made. These arcs are known as informational arcs. Arcs into the value node are informational as well. The distinction between the two kinds of arcs is important because conditional arcs can be reversed under certain conditions but informational arcs cannot be reversed under any conditions.

## APPLICATION

Consider the following example of a hydrological decision problem. Freeze et al. (1992) posed the problem as:

A landfill is to be sited in the location shown in Figure 1, and two design alternatives are under consideration: (1) a single-liner design, and (2) a no-liner design. There are other facets to a landfill design, including capping specifications, leachate collection systems, and cell configurations, but for illustrative purposes the example will be limited to the two liner options. The hydrological environment illustrated in the figure features an upper unconfined

aquifer, an aquitard, and lower confined aquifer. The aquitard is of uncertain continuity. There could be a window of higher permeability material through it, and if so, such a window would provide an advective transport route for potential landfill leachate to reach downstream water-supply well in the lower aquifer. Such an occurrence would constitute a failure of the landfill design.

The initial decision problem is to choose one of the design alternatives, i.e., install the liner or do not install the liner, for the landfill. Even without collecting any data about the existence of a window of more permeable material in the aquitard, it is possible to determine an optimum decision if the utility or objective function is specified. In the present example Freeze et al. (1992) use a standard risk-cost-benefit form of the utility function that depends on the probability of failure (risk) and the monetary consequences of such a failure. Dollar amounts used in the utility function are shown in a payoff table similar to Table 1.

Table 1. Payoff table for the example problem.

Alternatives	Benefits	Costs	Cost of Failure
No liner	\$1,000K	\$300K	\$1,000K
Liner	\$1,000K	\$500K	\$1,000K

The influence diagram for the initial decision problem is given in Figure 1. Let  $L$  represent the decision regarding the liner so that  $L = 0$  means do not install liner while  $L = 1$  means install liner. Also let  $\theta$  represent the existence of a window through the aquitard. In this case,  $\theta = 0$  means no window exists, and  $\theta = 1$  means a window exists.

The value of the utility function  $V(\theta, L)$  is determined by the existence of a window,  $\theta$  and by the decision to install the liner,  $L$ . Since it is unknown if a window exists, the value of  $\theta$  is uncertain and so  $\theta$  is shown as a chance node with the probability density function  $p(\theta)$ . Without any information about how likely the existence of a window is, a neutral or noninformative probability density function is assumed. That is,  $p(\theta)$  is taken to be 0.5 for each value of  $\theta$ .

Freeze et al. (1992) use the values in Table 1 to specify portions of their objective function so that

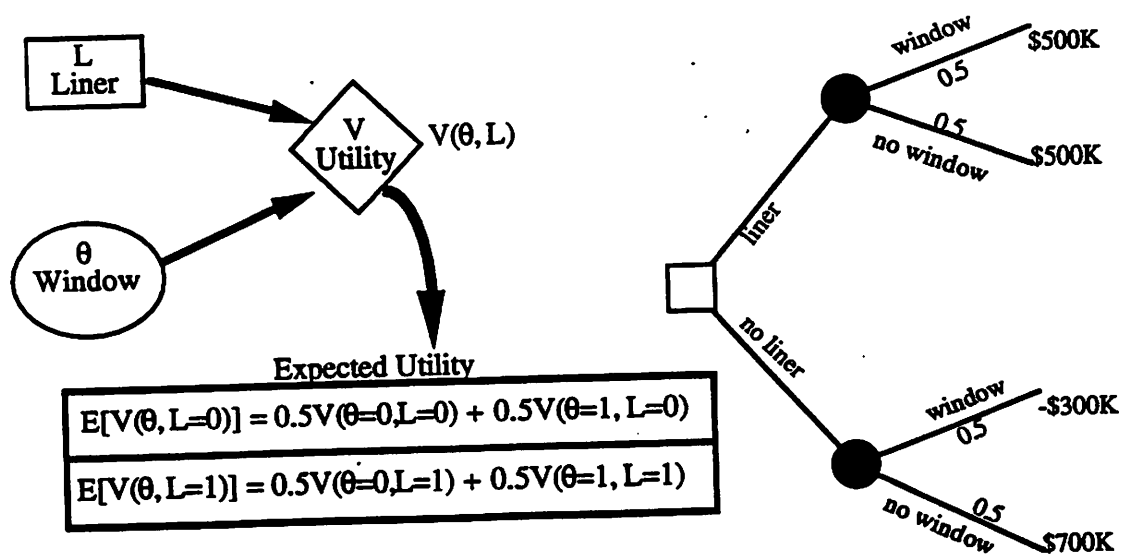


Figure 1. Influence diagram for the initial decision problem.

$$V(\theta, L) = 1,000 - C(L) - 1,000 P_f(\theta), \quad (1)$$

where  $C(L)$  is the cost associated with each design alternative and  $P_f(\theta)$  is the probability of failure of the design.  $C(L)$  is defined as

$$C(L) = 300 + 200 L, \quad (2)$$

and in the absence of any further data about the site, the probability that the system fails can be written

$$P_f(\theta) = \theta (1 - L). \quad (3)$$

The expected utility for the design alternatives can now be computed to determine the optimum decision. In general, the expected utility is given by the formula

$$E[V(\theta, L = l)] = \int_0^1 p(\theta) V(\theta, L = l) d\theta. \quad (4)$$

In the present case,

$$\begin{aligned} E[V(\theta, L = 0)] &= 0.5 V(\theta = 0, L = 0) + 0.5 V(\theta = 1, L = 0) \\ &= 0.5 (700 - 300) \\ &= 200 \\ &= \text{expected utility for no liner design.} \\ E[V(\theta, L = 1)] &= 0.5 V(\theta = 0, L = 1) + 0.5 V(\theta = 1, L = 1) \\ &= 0.5 (500 + 500) \\ &= 500 \\ &= \text{expected utility for liner design.} \end{aligned} \quad (5)$$

So the optimum design decision given no additional data about the site and neutral belief about the existence of a window through the aquitard is to install the liner. Figure 1 also shows both the influence diagram and decision tree for the initial decision problem. The results computed in Equation (5) are also shown in table form.

## THE DATA WORTH PROBLEM

Now consider the data worth problem for the influence diagram of Figure 2. Another chance node representing the data from a potential site investigation has been added before the liner/no liner decision node along with another decision node. Now the first decision to be made in the problem is to select an experimental or test design,  $T_i$ ,  $i = 0, 1, \dots$ , for the investigation. In particular let  $T_0$  be the test design where no data are collected. Then the simple optimization discussed above becomes the baseline case for the data worth analysis of the hydrological problem. The value of the utility function is constant for the decision to install the liner.

One way to interpret this result is that once the decision to install the liner is made, the existence of the window is moot and no longer of interest. However, before the decision is made to install the liner, the value of the utility function decreases as  $P_f(\theta)$  increases, and  $P_f(\theta)$  depends on the site investigation plan selected,  $T_i$ , and thus on the data,  $y$ , collected by such a plan. Properly, then,  $P_f(\theta)$  is written

$$P_f(\theta) = p(\theta = 1 | y). \quad (6)$$

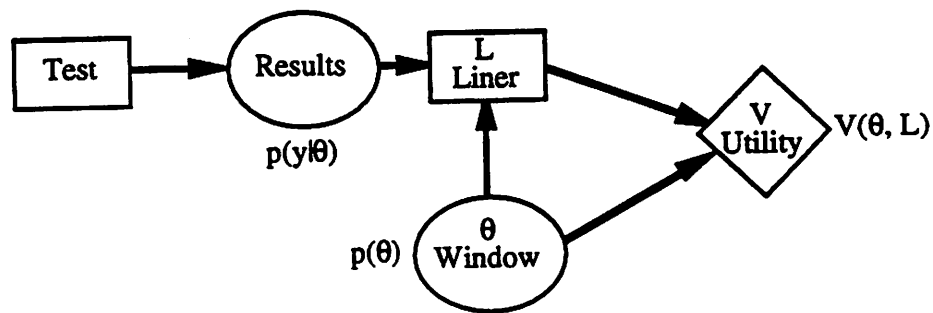


Figure 2. influence diagram for the data worth example.

The data worth analysis begins by considering the  $T_i$  where the value of the utility function is greater than that of the baseline case's optimum decision. The optimization strategy is to collect enough data through site investigation to reduce the probability of system failure. When  $P_f(\theta) = 0.2$  the value of the utility function is the same for either alternative. For smaller failure probabilities, the value of the utility function for the decision not to install the liner is greater than that of the baseline. For larger failure probabilities, not installing the liner is riskier than installing the liner. Collecting data to reduce the failure probability in this problem is, in effect, reducing uncertainty about the existence of the window.

## COMPUTER IMPLEMENTATION

Data worth analysis offers a principled way of organizing information and it can serve as an effective mechanism for allocating resources effectively. To this end, a computer system, called The Bridge<sup>®</sup>, is under development jointly by the University of New Mexico, Sandia National Laboratories, and Los Alamos National Laboratory to provide a platform for education, for debate, for negotiation, and for analysis of risk-related issues.

The Bridge represents an integrated approach to thinking about risk analysis. The methodology behind The Bridge should prove to be a powerful tool because it generates a tractable mechanism for all camps to reach an acceptable forum. The system provides a common ground for negotiation and reasoning to deal constructively with complex technical and scientific endeavors while enabling the public to partner with the researcher in order to directly influence decisions. It is hoped that this partnership will in turn lead to solutions that are both publicly acceptable and technically sound.

One important feature of this system is data worth analysis. This feature has its foundation in influence diagram methodology and conforms to the tenets of Bayesian probability theory. The current version of the Bridge is an application that runs on a UNIX workstation with the X windowing system.

## CONCLUSIONS

Even for this simple example, several differences between the decision tree analysis and the influence diagram approach are apparent. First, the influence diagram is more compact than the decision tree, and the difference in compactness can grow exponentially as nodes are added. Second, the decision tree representation clashes with the natural way of modeling causal relationships in the environment (Pearl, 1988, p 304). In fact, the decision tree here cannot directly show the natural flow of information into the utility function. Perceptions about interdependencies among variables cannot be readily inferred from the tree's structure, and therefore, decision analysts are often forced to a two-stage strategy where they construct probability trees to assess conditional probabilities in the first stage and convert these trees to comparable decision tree representations in the second stage using Bayes' Rule (Pearl, 1988). Influence diagrams give decision analysts a comprehensive, single-stage tool that not only accommodates interdependencies in an analysis but visually depicts them as well. Therefore the use of influence diagrams is more efficient for representing and analyzing

decision options. This method integrates beliefs (chance nodes) with actions (decision nodes) (Howard and Matheson, 1981).

## ACKNOWLEDGMENTS

The authors wish to express their gratitude to Mr. Paul Davis of Sandia National Laboratories for his support of this project.

## REFERENCES

- Freeze, R.A., James, B., Massmann J., Sperling, T., and Smith, L., 1992, Hydrological decision analysis: 4. The concept of data worth and its use in the development of site investigation strategies, *Ground Water*, 30-4, 574-588.
- United States Department of Energy, 1989, "Applied Research, Development, Demonstration, Testing and Evaluation Plan (Draft)," Section 2.2.2.3.
- Miller, A.C., Merkhofer, M.M., Howard, R.A., Matheson, J.E., and Rice, T.R., 1976, "Development of Automated Aids for Decision Analysis," Final Technical Report, DARPA No. 2742, SRI International, Menlo Park, California.
- Jae, M. and Apostolakis, G.E., 1992, The use of influence diagrams for evaluating severe accident management strategies, *Nuclear Technology*, 99-2, 142-157.
- Pearl, J., 1988, "Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference," Morgan Kaufmann, San Mateo, California.
- Howard, R.A., and Matheson, J.E., 1981, Influence diagrams, in: "Principles and Applications of Decision Analysis, 2," Strategic Decisions Group, Menlo Park, California.

## **INTEGRATED ISSUE MANAGEMENT DATABASE SYSTEMS**

Herb Wilhite and J. Randy Pearson

CYCLA Corporation  
206 High Avenue  
Strawberry Plains, TN 37871

### **INTRODUCTION**

Many organizations today face an increasingly complex burden of issues that can fundamentally and profoundly affect the way they perform, and, in some cases, even whether they continue to exist. Such issues are identified as a result of both internal and external oversight evaluations and self-assessments, and are likely to represent risks both to the organization and to other stakeholders.

In most cases, issues must be resolved within an atmosphere of budgetary constraint. As such, the organization has limited resources with which to effectively manage the risks represented by the issues and attempt to achieve issue resolution within any given budgetary period. Thus, the organization needs a method of prioritizing and managing risks in a cost effective manner, using traceable management-decision processes that are demonstrable and defensible to all stakeholders. To meet this need the organization must:

- be continually aware of the needs and issues confronting the organization;
- understand the underlying root causes of the issues and the full spectrum of cost-effective strategies and activities to address the issues;
- accurately determine the type and level of resources required to perform those activities;
- assign available resources to the most important activities in a manner that maximizes overall benefits within a constrained budget;
- establish and document commitments to implement those activities in a controlled manner to provide all stakeholders a common and rational basis for performance expectation and accountability;
- track and report the status of all identified issues, commitments, and budgeted actions; and,

- perform all of these tasks in a structured, traceable, and defensible manner that can be easily communicated and demonstrated to all internal and external stakeholders.

Thus, the fundamental steps in an effective risk-based Issue management process should include issue identification, prioritization, and analysis; corrective action/project development and prioritization; decision-making, resource allocation, and commitment-making; and tracking and reporting.

CYCLA Corporation has developed an easy-to-use but very powerful database system to support and link all steps in the issue management process. The CYCLA Integrated Issue Management Database System (IIMS) is being successfully applied by several organizations to support most or all of the steps necessary to implement an integrated, risk-based issue management process. These include:

- United States Enrichment Corporation (formerly Martin Marietta Energy Systems (MMES) Uranium Enrichment Business Systems)
- U. S. Department of Energy (DOE) facilities managed by MMES in Oak Ridge, Tennessee
- All DOE facility operating contractors and DOE Field Offices and Program Secretarial Offices in development of the DOE Safety and Health Five-Year Plan.
- U. S. Department of Transportation

This paper briefly describes the CYCLA IIMS, including a discussion of its purpose, design, and application.

## **IIMS PURPOSE**

The IIMS has been developed and continues to be refined to support prudent, systematic, and effective risk-management and decision making. It has been designed to assist facility and organization managers in the collection, identification, analysis, and prioritization of issues and the activities (corrective actions and projects) designed to resolve those issues. The IIMS can support a formally controlled issue-tracking, status-reporting, and close-out process, and can provide the bases from which management can effectively make, report, and defend prudent management decisions affecting the allocation of constrained resources. In support of this purpose, the IIMS can assist an organization's managers to answer the following logical questions concerning the resolution of issues and the management of constrained resources.

- What is the organization trying to accomplish with its constrained resources?
- Where is the organization with respect to achieving its objectives?
- What is the set of potential activities that are being suggested by all legitimate parties and from which the optimum set of activities must be chosen?
- What are the relative benefits of each activity with respect to helping the organization achieve its objectives?
- What is the amount of each type of constrained resources required to implement each activity?
- What subset of activities that can be implemented within available resource levels would produce the most overall benefits?

Given answers to the previous questions, the IIMS can also assist the organization to assure itself and its customers that it is completing activities, resolving and closing issues, achieving its objectives, and fulfilling its commitments. The IIMS can also help the organization close the planning cycle by utilizing insights gained from planning and implementing activities to establish new strategic objectives and identify new issues.

## **IIMS DESIGN**

The IIMS has been developed using Microsoft FoxPro/DOS, Version 2.5, database management system software. It features a modern, easy-to-use, windows-type user interface and operates on either individual standalone PCs or local area network (LAN) systems.

The IIMS is developed and distributed as a run-time application, thus requiring no additional software purchases by the using organization. On standalone PCs, installation and use of the IIMS requires a 386SX or higher processor with at least 2 megabytes (MB) of installed and *available* random access memory (RAM). Organizations planning new hardware purchases to support implementation of a CYCLA IIMS are recommended to procure computers having at least 33MHz 486 processors with at least 4MB RAM (8MB is preferred). Other computer requirements for operation of the IIMS may vary, depending on the particular application and operating environment, and are discussed at the time the specifics of the organization's IIMS application are discussed.

### **Common Library**

The IIMS architecture is based on a large common library of integrated and related modules. This common library is proprietary and comprises approximately 60% of the size of any IIMS application. From this common platform, each IIMS application can be quickly customized to fit an organization's specific needs consistent with their management methods and processes. The IIMS architecture benefits all users by ensuring that updates, improvements, and enhancements can be quickly migrated to the IIMS applications in use among various organizations. This design also provides an effective basis for quality control. Any common problems identified can be quickly and consistently resolved for each IIMS application sharing the common platform. This design has proven very beneficial in the development, maintenance and update modifications of IIMS applications currently in use. Each common platform level is archived for future reference as subsequent revisions are incorporated.

### **User Interface**

Installation of each IIMS application is designed to be quick and easy for the user. The application guides the user through a series of message screens and prompts to ensure that the IIMS is correctly installed. The IIMS can detect the presence of previous installations of the application and will indicate to the user whether they are installing for the first time or updating to a new revision. The IIMS will also, at the user's discretion, automatically identify and make changes to the computer's configuration files to ensure certain minimum settings.



The IIMS features a User Module which provides login and password protection, user access controls and user preferences. From this module, an organization's system administrator can add or delete users and edit user access privileges to ensure access control to the system and data integrity. User's can be granted incremental privileges within seven access levels, from "Read Only" to "System Administrator". The IIMS is also designed to provide for easy data validation where possible and appropriate. Validated data specific to an organization's needs and processes is retrieved from reference tables and made available to the user through a variety of intuitive and convenient screen controls.

The IIMS is designed to provide maximum flexibility in viewing and reporting data. The interface screens are designed to allow data to be entered or edited without the user having to move through multiple layers of menus. It also features a "management user" option which can eliminate any burden for managers to navigate data entry screens and enable them to quickly and easily select or define combinations of data filters, list orders, and standard output reports for their own use.

Perhaps most importantly, the IIMS features very powerful decision support tools. These are the indexing, filtering, and reporting capabilities. Described below, the indexing filtering, and reporting capabilities of the IIMS work in combination to provide the user and organization managers with the ability to produce many valuable and informative reports. Among others, output reports can include:

- Prioritized lists of open issues and related activities
- Reports of milestones due in an upcoming period
- Reports of activities completed in a previous period
- Activity cost summaries
- Summary reports of relative risk-reduction versus cost

Indexing allows the user to control the order in which data records appear within the system, both in printed output and when scrolling through and editing records. Each IIMS application is normally designed with several standard indexing options. Additionally, the user can create and save special user-defined indexes to order data in other ways as the need arises.

Filtering allows the user to define specific subsets of the data to be viewed, edited, or reported. The filtering capabilities of the IIMS allow virtually any subset of data to be specified, including the ability to search on specific text strings in specified data fields. Most IIMS applications include key data elements in on-screen controls that the user can specify; this obviates the need for the user to become familiar with software-specific language and syntax to establish filter criteria. As with the indexing features, the user can create and save special user-defined filters to use as the need arises.

Reporting allows the user to select from a number of standard output reports applicable to the specific IIMS application, or to create new user-defined reports to respond to the needs of an organization's managers.

### **Data Entities**

As noted above, the fundamental steps in an effective risk-based issue management process should include issue identification, prioritization, and analysis; corrective

action/project development and prioritization; decision-making, resource allocation, and commitment-making; and tracking and reporting. An organization may include some or all of these elements in its issue management process and, subsequently, in its IIMS application.

Each IIMS application consists of several distinct data entities. These generally include Source, Issue, Activity, and Milestone entities. The format, content, and nomenclature of the Source, Issue, Activity, and Milestone data records can be customized to an organization's specific needs. While each IIMS application is created to be specific to the needs of the using organization, the data captured in the IIMS is generally intended to provide information about each of the entities noted. This information can be grouped in various ways and serves to identify, categorize, analyze, and track each data record. The following table depicts the some of the typical data elements within each IIMS entity. Each entity is described below.

Table 1: Typical Data Elements in IIMS Data Entities

Purpose	Typical Data Elements
Identification	<ul style="list-style-type: none"> <li>• System assigned ID</li> <li>• External document IDs</li> <li>• Source organization</li> <li>• Responsible organization</li> <li>• Title of record</li> <li>• Description (full text)</li> <li>• Reference documents</li> <li>• Source evaluation dates (scheduled, started, and completed)</li> <li>• Date identified (Issues)</li> <li>• Originator's name</li> <li>• Action plan ID</li> </ul>
Categorization	<ul style="list-style-type: none"> <li>• Source type (internal or external evaluation)</li> <li>• Nature of Source evaluation</li> <li>• Responsible division</li> <li>• Responsible manager</li> <li>• Issue type (finding, deviation, etc.)</li> <li>• Functional area</li> <li>• Compliance driver (OSHA, law, standard, etc.)</li> <li>• Hazard level</li> <li>• Activity type</li> <li>• Commitment flag</li> <li>• Category (Environmental, Safety &amp; Health, Management, etc.)</li> <li>• User-definable codes</li> </ul>
Analysis	<ul style="list-style-type: none"> <li>• Source evaluation manpower impact</li> <li>• Issue evaluation</li> <li>• Final response to Issue (full text)</li> <li>• Risk prioritization</li> <li>• Issue root cause codes</li> <li>• Analysis comments</li> <li>• Cost data</li> <li>• Account codes</li> <li>• WBS codes</li> <li>• Reference data sheet numbers</li> <li>• Commitments met, missed, or rescheduled</li> </ul>
Tracking	<ul style="list-style-type: none"> <li>• Status code</li> <li>• Last status change date</li> <li>• Closure verification level required</li> <li>• Response document and date issued</li> <li>• Closure dates</li> <li>• Status remarks</li> <li>• Status history data</li> <li>• Closure document and evidence</li> <li>• Closed by (individual)</li> <li>• Commitment tracking fields (by whom, to whom, etc.)</li> </ul>
System Fields	<ul style="list-style-type: none"> <li>• Record origination date</li> <li>• Record revision date, time, user</li> <li>• Number of entity records</li> <li>• Others as needed</li> </ul>

**Source Entity.** The Source entity provides information concerning the sources of the Issues. Each Source (evaluation, assessment, audit, etc.) may result in numerous findings, problems, etc. which are designated as "Issues" in the IIMS. Thus, Source records have a one-to-many relationship with Issues.

**Issue Entity.** The Issue entity provides information concerning the nature of the Issues and their relationships to Sources, other Issues, and Activities. Issues have a many-to-one relationship with Sources and a many-to-many relationship with Activities.

**Activity Entity.** Activities are those steps identified by an organization that are taken to resolve specific Issues. Activities, some of which may be by necessity short term, are allotted a many-to-many relationship with Issues. That is, one Activity may be identified to help resolve one or more than one Issue; conversely, one Issue may be resolved by one or multiple Activities. The Activity entity provides information concerning Activities and their links to Issues and Milestones.

**Milestone Entity.** The Milestone entity provides information about the Milestones associated with an Activity. Milestones are used to provide information about the performance status of an Activity.

## **APPLICATION**

The IIMS is designed to provide data management and control, and management information and support relevant to the implementation and use of an integrated risk-based issue management process. The IIMS can gather, relate, and report data and information from multiple sources. Thus, use of the IIMS has been instrumental at both MMES and DOE facilities in integrating data from multiple, less flexible databases, that could not readily support integration of data and information.

The IIMS gathers and reports data pertaining to Activity costs and Milestones and data relevant to Issue and Activity status and closure. It also supports the performance of root cause analyses of Issues, with built in reference tables for selecting cause codes.

The IIMS supports the risk-based prioritization of both Issues and Activities. The risk model used to determine relative Issue and Activity priorities is designed into and called from within the IIMS software. As such, the user can select the risk model attributes applicable to a particular Issue or Activity and the IIMS will calculate and display the total relative risk score. The IIMS can be modified to support other priority models that are applied in a risk-based management process.

Finally, the IIMS can support management to efficiently and effectively analyze and report large amounts of data, and can focus management attention on critical decision areas. These and other IIMS attributes continue to support the Management of DOE, MMES, and other organizations in identifying cost-effective Activities based on risk-reduction, defining relative Issue and Activity priorities, allocating constrained resources in an optimal manner, and establishing a traceable and defensible Activity selection and budgeting process.

**107 Organizational Factors and Nuclear Power Plant Safety**

*Chair: K. Dahlgren, Swedish Nucl. Pwr. Insp.*

**Organizational Factors and Nuclear Power Plant Safety: A Process Oriented Approach**

*K. Dahlgren (SNPI, Sweden); J. Olson (Battelle)*

**Organizational Assessment of a Maintenance Department at a Nuclear Power Plant**

*L. Reiman (STUK, Finland), L. Norros (VTT, Finland)*

**Evaluation of Quality Systems**

*I. Blom (SNPI, Sweden), B. Melber, N. Durbin (Battelle)*

**Two Solutions to the Same Problem - Assessing Processes and Their Outcomes**

*G. Svensson (SNPI, Sweden)*

## **ORGANIZATIONAL FACTORS AND NUCLEAR POWER PLANT SAFETY: A PROCESS ORIENTED APPROACH**

Kerstin Dahlgren<sup>1</sup>, and Jon Olson<sup>2</sup>

<sup>1</sup>Swedish Nuclear Power Inspectorate  
Department of Man Technology Organization  
Box 27106  
S102 52 Stockholm, Sweden

<sup>2</sup>Battelle Human Affairs Research Center  
PO Box C5395, 4000 N.E. 41st Street  
Seattle, Washington, 98105-5428, USA

### **INTRODUCTION**

The relationship between organizational factors and nuclear power plant safety has most clearly been identified through the causal analysis of incidents and accidents. The development of more sophisticated and systematic methods for incident analysis (such as HPES, ASSET, AEB, etc.) has also facilitated the detection of these often less manifest contributions to incidents and has allowed for systematic improvements to be made. However, the enhancement of nuclear plant safety cannot rely only on actions taken in response to failures (reactive prevention). It is also dependent upon the ability of organizations to identify the nature and causes of developing problems and to develop effective interventions to meet them (proactive prevention). There is thus a need for organizations to develop a more proactive approach to safety management through processes that will promote improved performance over time. Organizations of this kind have been characterized as "learning organizations" (Senge, 1990; Olson and Thurber, 1991). The ability to learn is central to the plant's ability to improve. Organizations can learn when they can adapt to changes in external or internal operating contingencies, and thus be more efficient or effective.

The Swedish Nuclear Power Inspectorate, SKI, has in its regulatory approach to the area of management and organization focussed on the process of continuous improvement and have in collaboration with Battelle Human Affairs Research Center, Seattle, developed a conceptual model of the important characteristics of a continuous improvement organization and how to assess it. In this work SKI has also recognized the importance of the regulatory goals and strategies adopted by SKI for promoting an improvement process on the part of the utilities, which will be further discussed below.

### **WHAT IS A CONTINUOUS IMPROVEMENT APPROACH?**

With the ascension of Japan as a world economic power, much has been written about continuous improvement as an important element in Japan's success. Students of Japan's transformation of the safety performance of its nuclear power industry recognize the same

element at work. Commentors on continuous improvement have described it variously as an approach to life, an integrated theory of management, and a discrete strategy for exploiting certain types of markets. Its application to nuclear power plant safety, however, causes us to emphasize the following:

- Continuous improvement implies goals, since improvement must be in reference to something desired. Thus, activities in a CI organization are essentially intentional and are oriented toward the goals of the organization. Very little in a CI organization is done simply due to convention or habit.
- As a derivative of this emphasis on goal oriented activities, CI organizations are dominated by strategies and plans and all that these imply, including priorities, schedules and performance objectives and measures. Thus, members of a CI organization not only know where they are headed, but they also have a pretty good idea of how they are going to get there.
- CI organizations take responsibility for their own success. While the market or regulatory agency may present significant challenges to the utility, CI organizations are active in meeting these challenges; they do not take on the passive role of the victim.
- CI organizations recognize analysis as a primary means for meeting market and regulatory requirements. CI organizations value useful information, whether from their own operating experience or from the experience of others. CI organizations value expertise and organize in ways to get the maximum value out of available data and experience.
- As a derivative of the emphasis on analysis, CI organizations are inherently participatory (this does not necessarily mean that they are democratic). CI organizations favor the free flow information and the ability of each staff member to contribute appropriately to the solution of operational and organizational problems. Techniques of authority and control that inhibit the sharing of information are inappropriate in a CI organization. Techniques that encourage team work and cooperation and the flow of information both upward and downward in the organization lead to decisions based on more accurate and complete data, a consideration of a wider range of contingencies, and solutions that are better adapted for implementation within the organization.

While the value of such principles may appear to be self-evident, in reality, most organizations fall short on one or more of these key factors. In the nuclear industry, for example, there are many organizations that identify safety as their primary goal, but have no recognizable strategy for promoting safety beyond the requirements of the regulatory agency. Other utilities maintain a passive attitude toward safety regulation—they only deal with safety issues when the regulator tells them exactly what to do. Many organizations treat analysis as a side activity rather than as an activity that needs to be present in the discharge of every function in the plant.

## **WHY IS A CONTINUOUS IMPROVEMENT APPROACH IMPORTANT FOR SAFETY?**

Why should a regulator put so much emphasis on the continuous improvement approach? The answer is that experience tells us that it is important for safety. Three general reasons can be given.

- Managing and operating a nuclear power plant includes dealing with a number of uncertainties. Some of these uncertainties have to do with the unplanned interactions of system parts, others with the causes and consequences of human error, and other with the effects of aging and other sources of plant degradation. Thus, the knowledge base that appears adequate today may be proven by events and experience to be inadequate for managing safety. A CI organization anticipates the dynamic requirements of managing for safety, and looks constantly for indications of and ways to protect against developing safety problems.

- A CI organization also looks for ways to do what it is currently doing in better and more efficient ways. A CI organization looks for ways to improve the efficiency and effectiveness of each task, so that the available resources can have the greatest impact on safety and other plant goals. For example, rather than continuing to perform corrective maintenance on a frequently failing component, a CI organization will investigate whether the component or the system can be changed to improve the overall reliability of the system. CI organizations can accomplish more with the same resources than can non-CI organizations.
- Finally, we believe that the important elements of what is frequently called the safety culture are imbedded within the more general concept of continuous improvement. Specifically, a CI organization requires of its members that they take personal responsibility for advancing the organization's goals (including safety), that actions be intentional rather than haphazard, and that people look for ways of doing their tasks better or resolving organizational problems. Further, the CI organization looks to develop or facilitate organizational structures and processes for supporting these fundamental aspects of the safety culture.

While there are many clear safety advantages to a CI approach, fostering a CI approach within a regulatory framework has its own challenges. Many of the common regulatory strategies and practices are inconsistent with promoting a CI approach within the utility. In the following section, we discuss how the activities of the regulator may need to be adjusted in order to promote continuous improvement on the part of the regulated organization. We use the Swedish situation as our primary example.

## **THE SWEDISH REGULATORY APPROACH**

The overall Swedish regulatory policy is based on the two roles given to SKI and specified in the SKI charter. The first role is the formal regulatory and supervisory role. It includes issuing formal rules and guidelines, licensing of installations and procedures, inspection and enforcement and analyzing incidents and other operational experiences. The second role given to SKI is the active promotion of safety improvements. The regulatory strategy of SKI is expressed as: "The licensee has the full and undivided responsibility for safety. SKI shall monitor how the licensees shoulder that responsibility by forming a well-founded opinion on the safety status of the installations and on the quality of licensee safety work." SKI's role and strategy thus implies the necessity to both assess management and organizational factors and to promote a continuous improvement approach.

### **Selecting and Applying Criteria for Judging Effectiveness of Quality System Methods**

In terms of assessment, SKI has various means of gaining information on organizational factors. These include operating experience through reportable events (LERs) including trends, incident investigation, periodic safety reviews including PSA studies, inspections, plant modifications, etc. When these sources of information are used for assessing improvement, the main strategy for evaluations has been to focus on the learning process, including the organization's ability to recognize and diagnose problems, to formulate and implement solutions, and to monitor the effects of the solutions and make adjustments as required by experience.

Operating experience covers both the follow up of reportable events (LERs), trends based on these events, incident analysis, and the periodic safety reviews (called ASAR, As operated Safety Analysis Report) covering experiences in a 10 year perspective. With regard to LERs and incident investigations SKI, in addition to the weekly follow up of these events, makes a more extensive yearly review of how incidents are reported and analyzed, solutions formulated, implemented and evaluated, particularly with regard to events that are classified as related to the interplay between man, technology and organization (MTO). The review is conducted as a team inspection with the team

consisting of MTO specialists and SKI inspectors. The SKI assessment and feedback on the approach taken is then seen as one opportunity for promoting improvements. Another effort to support this process has been the arrangement of a seminar together with all utilities to encourage the sharing of experiences between utilities with regard to methods and strategies used to deal with the analysis of events.

The periodic safety reviews have recently changed focus so as to include more clearly requirements on an analysis of operating experiences from an organizational perspective. The SKI evaluations of the ASAR reports concern the ability of the utility to analyze experiences, evaluate them and draw conclusions regarding necessary safety improvements.

**Inspections.** The shift in regulatory strategy adopted by SKI, with a gradual shift in emphasis from assessing technical performance of systems and components to assessing the quality of management, operation and maintenance, has in turn required the development of new methods for inspections. Examples are the new approaches developed to perform inspections in the areas of organization and management, quality systems and maintenance programs. In addition to the need to develop models, assessment methods and evaluation criteria within these areas, the new approach to inspection has involved a change in the role of the inspectors with new requirements on knowledges and skills. Great efforts have therefore been devoted, first of all, to the continuous involvement of inspectors in the development of the conceptual as well as methodological work within these areas, carried out mainly through research efforts. Also in the field-testing of new "tools" for inspection and in parallel to this special training in the techniques of interviewing.

This developmental work recently resulted in a first team inspection, again with inspectors together with MTO specialists, within the areas of management and organization, quality systems and maintenance programs. An important lesson from these inspections has been the need to be very familiar with various aspects of organizational context (such as history, organizational changes, relations to corporate offices, etc.) as well as the formal systems for safety management in order to be able to understand and interpret how these are carried out in practice. Another challenge for SKI is how to present and follow-up on observations made in these inspections so as to really promote improvements on the part of the utility. SKI also realizes the need for monitoring and assessing the impact of these new approaches to inspection as a basis for further improvements of its regulatory strategies.

**Plant modifications** are in many cases handled through the interaction of several functional units within the plant organization and can therefore serve as an important information source on organizational factors. In fact, one of the major plant modifications recently made in five of the Swedish reactors served as the case study in the team inspections mentioned above. It gave a good opportunity to evaluate the organization's ability to handle the various steps in the learning process and of how the formal systems of safety management functioned in practice. The importance of proper analyses and resources for these analyses in the initial phases of this modification work as well as the risk of taking shortcuts in the formal systems for quality and safety management due to time pressure were some of the findings.

In the evaluation of how the plants handled this major modification, the role played by SKI was also assessed. In this specific case, the plant modifications were made in response to a requirement by SKI. The five reactors were ordered to shut down their operation when a basic design deficiency was discovered in connection with an incident at one of the reactors. An independent investigation evaluated how SKI handled the regulatory work from the time of the incident up to the decision to shut down the five reactors, whereas the team inspections assessed the influence of SKI's regulatory approach on the utilities' ways of dealing with the necessary modifications. An important observation was the need to formulate requirements so as to maintain the proper roles and responsibilities in terms of safety according to the regulatory model adopted i.e., for the "ownership" of safety to belong completely to the utility organizations.



The analysis of the problems connected with this need for plant modifications was at SKI performed largely through a teamwork effort, with the integration and coordination of the views from different specialist groups. While this supported the development of a well-founded opinion on necessary improvements to be made, it put extra demands on SKI not to fall into the trap of also suggesting possible solutions to the problems, which is the responsibility of the utility according to the model adopted for the interaction between the regulatory body and the licensees in Sweden.

### **The Relevance of Rules and Regulations in Promoting Continuous Improvement**

In general, the regulatory approach of SKI implies keeping regulations at a minimum. Two reasons being to support the licensees' full responsibility for safety and also to allow for the development of the best solutions to safety problems. Too detailed regulations risk limiting consideration to be taken to new technological innovations in the choice of solutions. The development of rules or regulations in the area of management and organization is connected with special problems. Detailed regulations in this area of management and organization is connected with special problems. Detailed regulations in this area are neither conceivable nor desirable. SKI has only one regulation that influences the conduct of work within the utilities and that is in the area of quality systems. However, this regulation is formulated in a broad sense requiring utilities to implement a quality system "for all activities that affect the quality level," while allowing for flexibility in organizational structure and approach and encouraging a focus on improvement over time.

SKI is at the moment in the process of revising all its regulations. Special consideration is being given to the impact these will have on how plant organizations manage their safety work. There is general agreement that, apart from keeping regulations at a minimum, the development should go in a direction that promotes continuous safety improvements to be made. Or as one manager formulated it: "when the licensee faces a problem we want them to look for the best solution instead of the right paragraph to follow."

### **REFERENCES**

- Olson, J., and Thurber, J., 1991, *Learning in nuclear power plants*. Paper presented at a consultants meeting: "The Influence of Organization and Management on the Safety of NPPs and Other Complex Industrial Systems," IAEA & IIASA, WP-91-28.
- Senge, P., 1990, "The Fifth Discipline: The Art of the Learning Organization," Doubleday, New York.

## **ORGANIZATIONAL ASSESSMENT OF A MAINTENANCE DEPARTMENT AT A NUCLEAR POWER PLANT**

**Lasse Reiman**  
Finnish Centre for Radiation and Nuclear Safety (STUK)

**Leena Norros**  
Technical Research Centre of Finland (VTT)

### **INTRODUCTION**

Maintenance has a substantial influence on the safety and availability of a nuclear power plant, but the management of maintenance and the work of maintenance technicians has not been studied extensively. The functions of a maintenance organization change gradually with the aging of a plant and with developments in technology. Preventive maintenance is getting increased attention. The importance of plant modifications and their management is increasing. Especially the high quality of work in maintenance affects the safety of a nuclear power plant. Therefore, an essential issue in an assessment of a maintenance organization is how this high quality can be achieved.

The purpose of the study has been to develop a method for organizational assessment from the point of view of work culture, and to apply the method in a case study. The case study was carried out at the TVO NPP in Olkiluoto. The co-operation of TVO and the contributions of the personnel of the maintenance department are gratefully acknowledged.

### **METHODOLOGICAL CONSIDERATIONS**

#### **Safety culture**

In a report by the International Nuclear Safety Advisory Group (INSAG) on safety culture (IAEA, 1991) the attainment of a good safety culture is implicitly conceived as a process of internalizing given safety goals that are defined by the managers of the organization. In our study not only top-down but also bottom-up mechanisms that promote the development of safety culture are identified.

Commitment is an essential element of the concept of safety culture introduced by INSAG. Organizational commitment may be defined as the relative strength of an individual's identification with and involvement in a particular organization (Porter et. al., 1974). When defined in this way, commitment involves an active relationship with the

organization and hence, commitment could be inferred not only from the expressions of an individual's beliefs and opinions but also from his actions.

Great similarities can be seen between the objectives of safety culture and those of a quality programme (Williams, 1991). Quality is thus likely to improve substantially from the introduction of a safety culture. Especially as regards maintenance work, excellence in quality can be regarded to promote excellence in safety. Due to this we prefer to use the term work culture to refer to the norms and values that control the attempts of the personnel to achieve the goals of their work.

### **Development of safety culture**

Our attempt, and the problem of the study, was to understand the mechanisms of development of work culture and to find means to promote such development.

A schema to conceptualize our assumptions about the development of work culture in a mature organization is presented in Fig. 1. Orientation is the central concept of the model. This concept, introduced originally by Galperin (1979), is used to indicate a person's typical way to frame a problem in a situation that requires actions. The starting point in our attempt to describe different types of orientation was an idea of the double character of a problem. While a problem is a threat to the functionality of the system in which it appears, it is simultaneously a possibility to develop it. It was assumed that this dual character of the problem itself could be useful to differentiate a person's optional reactions towards the problems he faces in his work (Norros, 1989). The more the person is oriented towards the development possibilities inherent in the problem the higher development potential he expresses in his way of work. It is further assumed, that the extent of utilization of the development potentials can also be interpreted as an indication of a person's expertise in a particular work.

The original disturbance orientation model has been tested in different industrial contexts. For this study a problem orientation model was developed. The model includes four orientation types which are (1) Withdrawal orientation, (2) Routine orientation, (3) Individual initiative orientation, (4) Systematic development orientation. The characteristics of different orientation types are discussed in Wahlström et. al. (1992).

As depicted in the figure, management, through expressing their solutions to managerial problems, and their subordinates, through expressing their solutions to problems of their work, contribute to the development potential of the organization. In addition, organizational mechanisms, which the management is responsible for, and emergent processes are needed for the development of culture. Both are regarded as signs of active commitment to organizational development.

In highly complex and risk-intensive production, (NPP production is commonly considered such), there is great pressure for both expertise and rule regulated activity. Other conflicting goals have also been identified in this kind of production (Cameron, 1986; Perrow, 1984). Therefore it was assumed that expertise that exceeds routine orientation would be called for. Individual initiative orientation would be insufficient in the long term for two reasons: The complexity of and the interdependencies in the system require co-operation and communication to carry out tasks. The second reason is that conscious control of initiative is essential for safety. Thus, systematic development orientation would be required.

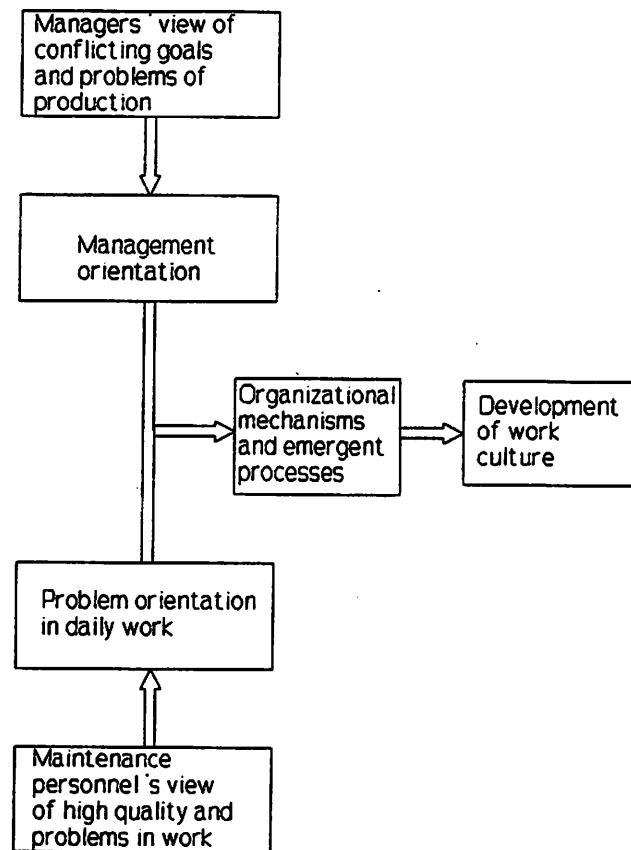


Figure 1. A scheme of the development of work culture.

## ASSESSMENT OF THE MAINTENANCE DEPARTMENT OF THE TVO NPP

### Methods

The study was carried out at the TVO NPP in Olkiluoto; 22 people from the maintenance organization were interviewed. The organization was divided into three levels: management (5), foremen (5) and technicians (10). In addition, one person from the work planning section and QC were interviewed. The electrical maintenance section was selected to represent the maintenance organization. A major part of the personnel of the electrical maintenance section were interviewed in the study. Different sets of questions were prepared for each level of the organization. Word for word protocols of the interviews were prepared and analyzed by both researchers independently.

The questions to the management were grouped based on the main functions of the management. The three main areas selected were (1) personnel management, (2) setting and implementing goals and (3) development activities. These were further divided into more detailed dimensions.

The questions presented to foremen and technicians dealt especially with the question how to achieve high quality in maintenance work. The questions were aimed at bringing forward practical cases where problems in the execution of work or in the attainment of high quality had existed. The purpose was to get them to speak in concrete terms of the contents and of the problems of their work and their relation to these problems. Also questions related to motivation, responsibility and co-operation were presented.

After a preliminary analysis the results were discussed with the personnel of each of the three organizational levels of the study separately and a final analysis of the data was made.

## Results

The analysis of the interview data was divided into three steps. First, it was investigated, both among the managers and the maintenance personnel, what problems challenge the attainment of the goals of the organization and what conflicts exist in the functions of different organizational units. Secondly, the interview data was used to assess the characteristic features of the managers' and personnel's orientation to these problems. The last part of the analysis dealt with the commitment of the personnel. An attempt was made to find concrete organizational means which could promote the commitment of the personnel to the development of the culture in the maintenance organization. Also emergent processes that, as such, would be signs of commitment to organizational development, were looked for. Also defensive mechanisms were noted.

**Problems.** Problems were interpreted as expressions of internal tensions within the organization. Internal tensions of work were first analyzed for each personnel group separately. They were then related to each other in order to identify some general features that could be considered internal conflicts within the maintenance activity as a whole. As a result of this analysis three internal conflicts in maintenance activity were identified.

First, as a result of the complexity of the production process, maintenance tasks cannot be preplanned in full. This causes demands for situational flexibility which is difficult to achieve in a functionally organized and compartmentalized maintenance organization. Second, even though predicting maintenance demands may be difficult, anticipation and early detection of problems should be aimed at. Adequate information technological and conceptual tools should be utilized for this purpose within the whole maintenance. Third, mastery of the continuously changing technology and organization is the far-reaching goal of maintenance. To achieve this goal, greater integration and co-operation between the different engineering disciplines and between design, maintenance and operations within the organization is needed.

Also three general conflicts in the prevailing way of work in maintenance and in the management of maintenance were noted. The first conflict deals with the difficulty of finding an optimal principle to control activities carried out in the organization. Rule regulation should not hinder the utilization of expertise in problem situations. The second issue is related to open and restricted communication. The third contradiction in the way of work is the difficulty to create learning in highly regulated activities with a growing proportion of preventive actions.

**Development potential of the personnel.** A problem orientation model was used to evaluate the development potential of personnel. The model that expresses the basic approaches to a problem situation was operationalized by using particular dimensions based on different aspects of each personnel group's work. The orientations of managers, foremen and technicians were studied. The orientation profiles for managers were elicited in regard with the main areas of managerial activities. The dimensions in orientation for foremen and technicians were adopted from earlier studies in conventional industry and they included the object of work, motivation, communication and work culture dimensions. As an example of the results, Fig. 2 summarises the average problem orientations of managers.

The managers were well aware of different optional leadership styles and they were also willing to evaluate their own leadership against these. Conceptual prerequisites for

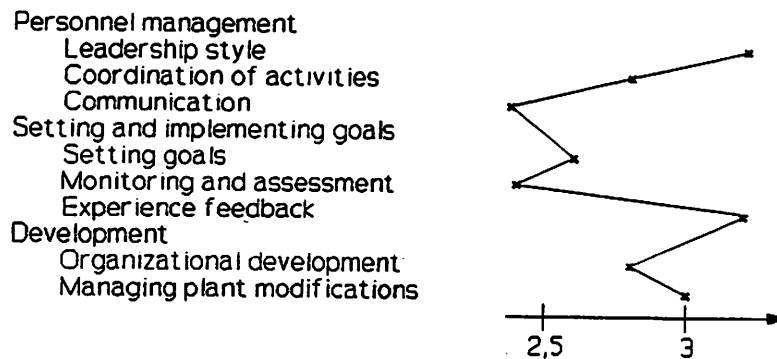


Figure 2. The average orientation of managers.

modern developmental management style can be seen to exist within the management. Other interview data reveal, however, that the preferred leadership style is only partially realized in management practices. This discrepancy between theory and practice was in principle identified also by the managers themselves. One of the affected areas was setting and implementing goals. In particular the sub-dimensions setting goals and monitoring and assessment were not as advanced as the other subdimensions.

While the orientation of the managers was mainly evaluated from the point of view of how the object of work is defined, the orientation of foremen and technicians was evaluated also from the motivation, co-operation, and work culture points of view. The general impression of the foremens' development potential is very promising. The highest potentials were registered in the area of work culture and co-operation. Regarding work culture, foremen gave advanced definitions of the requirements of quality in changing maintenance work and they were aware of the means to make the demand for quality effective in maintenance. Co-operation was well conceptualized, valued and practised in daily work.

The dimensions used in the evaluation of technicians' average orientations equal those used for the foremen. A lesser motivational potential resembles the orientation of the foremen. Some further aspects are particular to the orientations of the technicians. They manifest clear weaknesses in regard with the subdimension control of work within the work culture dimension. This subdimension was designed to represent the personnel approach to the rule regulation vs. expertise based regulation dilemma. Typical of the technicians was to interpret the rules as given. In the dimension quality of work which is also a subdimension of work culture the technicians are at a satisfactory level. High quality standards were interpreted as essential and the technicians were able to define features of quality. In the dimension object of work the technicians associated their responsibilities strictly with the execution of given tasks. Thus, quality is valued but its content is becoming outdated. The fact that technicians did not seem to identify the role of conceptual tools in the development of expertise gives further evidence that the technicians' conceptions of their work need enhancement.

**Development mechanisms.** The formation of work culture within an organization requires organizational mediators. Four central mechanisms (feedback, communication, co-operation, learning and development) were identified and their existence in the organization was studied. In a strict sense, as a set of conscious instruments for organizational development, such mechanisms could not be observed in the interviews, whereas elements of such were found.

## Conclusions

Based on the results of the analysis a general judgment of the development potential in the maintenance organization was made. A diagnosis of the situation is that the starting point for the organizational development is rather good. The potential required to implement such a development program was found to exist. This potential is especially strong among the maintenance foremen and exists also in the management. It seems that there is a common awareness of the internal conflicts and development necessities of the maintenance activity. However, some important prerequisites for carrying out the necessary development actions are lacking. For the first, the prevailing way of work, that was identified through evaluation of the personnel's work orientation, has some deficiencies which hinder the personnel from optimally meeting the demands of the tasks. Second, important organizational mechanisms that would promote the utilization of the potentials could not be found. Without explicit impulses from their superiors, e.g. conceptual and co-operative development measures, the potential of technicians cannot be developed and realized further. This puts pressure for the management to implement their advanced management philosophy into practical measures. This could be carried out in integration with technical modifications which seem to be well mastered. It should be noted also, that the utility has nowadays started an extensive organizational development program within the production department, which includes also the maintenance functions.

## REFERENCES

- Cameron, K.S., 1986, Effectiveness as paradox: consensus and conflicts in conceptions of organizational effectiveness. *Management Science*, Vol. 32, No. 5.
- Galperin, P.J., 1979, Introduction to psychology. Helsinki. (Original Vvedenije v psihologiju, Moskva, 1976.)
- IAEA Safety Series No. 75-INSAG-4, 1991, Safety Culture. IAEA, Vienna.
- Norros, L., 1989, Responsibility for system development as an element of process operators' professional expertise. Proceedings of the 2nd European Meeting on Cognitive Science Approaches to Process Control. Siena, Italy.
- Perrow, C., 1984, Normal accidents: Living with high-risk technologies. Basic Books, New York.
- Porter, L.W., Steers, R.M., Mowday, R.T., and Boulian, P.V., 1974, Organizational commitment, job satisfaction, and turnover among psychiatric technicians. *Journal of Applied Psychology*, 59, pp. 603-609.
- Schein, E.H., 1985, Organizational culture and leadership. Jossey-Bass Publishers.
- Wahlström, B., Norros, L., and Reiman, L., 1992, Human factors research in the nuclear power field in Finland. Proceedings of the IEEE Fifth Conference on Human Factors in Power Plants.
- Williams, J.C., 1991, Safety Cultures - Their impact on quality, reliability, competitiveness and profitability. *European Reliability '91*.

## EVALUATION OF QUALITY SYSTEMS

Irène Blom<sup>1</sup>, Barbara Melber<sup>2</sup>, and Nancy Durbin<sup>2</sup>

<sup>1</sup>Swedish Nuclear Power Inspectorate  
Box 27106  
S102 52 Stockholm, Sweden

<sup>2</sup>Battelle Human Affairs Research Center  
PO Box C5395, 4000 N.E. 41st Street  
Seattle, Washington, 98105-5428, USA

## INTRODUCTION

The importance of quality systems on nuclear facility performance has not been considered in a systematic way even though a facility's quality processes are expected to have important effects on safety. For example, the effects of quality systems are not included in Swedish PSA studies.

In 1990, The Swedish Nuclear Power Inspectorate initiated a major revision of quality assurance regulations. The revised regulations took effect in January, 1991. They are broad in nature and emphasize establishment of and reliance on quality systems for "all activities that effect the quality level." The more general composition of the regulation allows nuclear facilities flexibility in organizational structure and approach and encourages a focus on improvement over time. The intent of these new regulations is to move away from a traditional focus primarily on performance of hardware to a focus on a quality system that encompasses organizational and human performance.

The Swedish Nuclear Power Inspectorate (SKI), assisted by Battelle Human Affairs Research Center, Seattle, is developing a methodology for evaluating the effectiveness of such systems. The approach used is to identify factors critical to the effectiveness of quality systems in the nuclear context and to develop criteria to assess the functioning of these critical factors. These factors and criteria were developed based on expert knowledge and extensive interviews with SKI staff and Swedish nuclear facility personnel. This paper summarizes the evaluation method developed and presented in a draft handbook. The evaluation method is currently being tested by SKI inspectors.

## THE EVALUATION METHOD

Quality systems are both difficult and important to evaluate because they cover all activities that affect the performance of nuclear facilities. These systems may appear to be boundless and undefinable and people often state that "everything we do, all the time, affects quality." That statement is true. However, the quality system is not the activities done within an organization, or "everything we do, all the time." A quality system is a specific set of methods designed to assure desired levels of performance of activities. Although the set of methods that comprise a quality system is limited, the methods are



applied to carrying out all activities. Thus, the nature of quality systems makes it important to establish clear goals for an evaluation method.

In order to evaluate the quality system, the evaluation method establishes four major goals: Be selective; Cover the full cycle of quality system methods; Capture the dynamic nature of the system; Provide support for improving quality systems. Selectivity is important because SKI collects information on the quality system across the whole range of activities in the facility. Since it is not possible (nor desirable) to observe or document all aspects of a quality system (or any other system being evaluated) there must be an intentional selection of information.

It is important that the selection of areas for evaluation covers the full range of quality system methods since an imbalance of emphasis can result in an incorrect view of the functioning of a quality system. Such imbalances in emphasis are common problems of evaluation methods. They often result from an over-emphasis on inspecting what is easy to obtain information on (for example, elements that can be counted, that are straightforward rather than complex and subtle) rather than on inspecting what is important, in terms of understanding how a quality system functions.

Because an effective quality system relies on an iterative cycle of a number of steps (identifying problems, analyzing their causes, making decisions regarding how to solve problems, implementing these decisions, evaluating how well the solutions work, and incorporating successful solutions into the organizations' policies and procedures for carrying out the work), information needs to be gathered and carefully documented for evaluation over a series of inspection activities in order to assure the coverage of the full cycle. Using outage activities at a nuclear power plant as an example, in order to attain comprehensive information about the quality system for modifications the inspector will need to collect information over the course of the entire year to cover the complete cycle of planning, executing, and evaluating the annual planned outage.

Questions regarding the status of activities related to quality systems are best asked on a "real time" basis to the extent that is feasible. That is, in order to capture the dynamics of the quality system, it is preferable to obtain information on how problems that may need to be resolved are identified while such information is actually being collected and analyzed by facility staff rather than after decisions have been made. Obtaining information regularly during routine inspections, that is in a "prospective" way--following the activities as they occur over time--provides a dynamic view rather than relying on individuals' memories of how decisions were made in the past. However, this is a time-consuming way to gather information and is not always practical. Prospective information-gathering is efficient when it is organized as a part of routine inspection activities which cover a range of areas on a regular basis. Thus, the evaluation of the quality system is an ongoing activity and draws from the full range of inspection activities carried out by SKI. While each inspection results in part of the picture, the combined inspection efforts over time provide a clearer, more complete picture.

The final objective of the evaluation method is that the method itself will contribute to the effectiveness of the quality system. One way that the evaluation method can contribute is to provide an independent view of the functioning of the quality system. Furthermore, the inspection activities should avoid making unnecessarily intrusive demands on the facility. For example, the evaluation method should use information that is collected and tracked on a regular basis as much as possible--for example, for a nuclear power plant these would include internal audit reports, activity plans, and outage reports.

### Selecting and Applying Criteria for Judging Effectiveness of Quality System Methods

Key criteria are used to judge the effectiveness of a facility's quality system methods. These are:

- That the quality system contains methods for the basic components of a quality system: problem identification, problem-solving, and standardizing solutions

- That these methods are prevention-based.
- That the methods are integrated.
- That the methods are focused on process and not only outcomes.

These criteria are used to evaluate the effectiveness of both the formal system (the design of the methods--how the system is supposed to work) and the actual practices (how the methods are actually used) at the facility. A more detailed discussion of each of these criteria is provided below.

### Basic Quality System Components

The quality system is comprised of three components: a set of methods to identify problems, a set of methods to solve problems, and a set of methods to standardize solutions. The quality system provides a way to achieve systematic change and improvement. The methods for problem identification, problem-solving, and standardizing solutions are discussed in more detail below.

**Methods for Identifying Problems.** Methods for identifying problems vary with regard to how problems are identified, who identifies problems, and when problems are identified.

Problems may be identified when a problem is discovered in an unanticipated manner or when a problem is discovered through an intentional process, such as an audit, an operational experience review, or a shift turnover meeting to discuss problem areas. The quality system should have methods to benefit from accidental problem identification as well as having planned methods of problem identification.

Problems may be identified before an actual event, during the initial stages of an event, or after the event has created significant problems. For problems identified at the earliest stage, process improvement identifies and eliminates potential problems and problems are prevented from having safety consequences. Early identification of problems has the advantage of allowing time to consider alternative solutions, creating a more stable and safer environment. It is also important to recognize and respond appropriately to events when they are occurring or after they occur. Control functions, such as inspection and verification of work already carried out, identify problems after the fact. While such functions are a necessary part of a quality system, reliance on control as the primary mechanism for assuring quality leads to a reactive, rather than a preventive, system.

Methods for identifying problems may be inclusive, where all workers are encouraged to report problems, or methods may be exclusive, where specific positions have the responsibility for finding and reporting problems. In most cases, a combination of inclusive and exclusive methods is desirable.

The problem identification methods of a nuclear facility will consist of interactions of when problems are identified, who identifies problems, and how problems are identified. The methods of problem identification should cover these three continuums: accidental to planned; before to after; and inclusive to exclusive.

**Methods for Solving Problems.** There are five steps in a complete method of solving problems:

- Analyzing problems (e.g., identifying causes).
- Developing alternative solutions to problems.
- Selecting solutions to problems.
- Implementing solutions to problems.
- Evaluating impacts of those solutions.

The problem-solving method should assure that changes are made based on the results of systematic analysis of problems and proposed solutions. All steps of the problem-solving process--analyze, develop alternatives, select, implement, and evaluate--need to be included. An organization may focus on problem analysis but spend little effort on developing solutions or may develop excellent plans for action but not execute them. due

to lack of resources or lack of clear assignment of responsibilities for implementation. The final aspect of problem-solving, evaluation of the impact of a solution, is one of the most neglected--and one of the most important--steps in problem-solving. Tracking actual impacts of a solution identifies unanticipated consequences so that adjustments can be made based on actual experience, or if necessary, a back-up solution can be implemented.

**Methods for Standardizing Solutions.** When the organization standardizes solutions it incorporates tested solutions into daily work policies and practices so that improvements become part of the standard operations of the organization. For example, many times an organization will develop a solution for a problem but fail to establish training or procedures to routinely implement that solution. Or, the solution will become part of the formal system but resources may not be allocated. For example, an improved system for reviewing changes may be adopted but additional time for staff to perform the reviews may not be allocated. Thus, the improvement is not fully standardized.

It is important to evaluate and refine solutions before adopting them throughout the organization in order to avoid costly and time-consuming implementation of proposed solutions that may turn out to be inadequate.

### Criteria for Judging Effectiveness

Three criteria for effectiveness were established; (1) the system should be prevention based, (2) the system should be integrated, and (3) the system should be process oriented. These criteria are discussed in detail below.

**Prevention-Based Quality Systems.** A prevention-based approach is at the heart of a quality system geared toward safe operations--SKI's area of concern and oversight--as well as basic to quality improvement in all areas. Prevention-based quality systems rely primarily on methods to anticipate potential problems and develop and implement solutions before these problems occur. While these systems also have methods for addressing existing problems and mediating the consequences of unexpected problems when they occur, they do not rely on event response and after-the-fact analysis as the major methods for safety improvement. One example of a prevention-based method is a predictive maintenance program. Another example is the method for establishing qualifications, such as educational levels and training programs, which assure that nuclear facility staff have the necessary knowledge and skills to perform their jobs prior to taking on job responsibilities.

In order to achieve a prevention-based system, facilities must first address existing problems quickly and effectively before they can expend resources on anticipated problems. Although anticipating problems and preventing them results in long-term savings overall, it is often difficult to obtain resources for prevention-based activities, because there are not immediate visible costs due to a problem anticipated in the future. For example, replacing a part after it wears out delays the cost of replacement. However, the overall costs are greater than replacing it on a standard schedule before an equipment breakdown, due to interruption of normal operations and the need to schedule emergency maintenance work.

**Integration.** Quality systems cover all activities and the linkages among those activities. An effective quality system will:

- Provide coordination across functional units and across management levels of an organization.
- Assess decisions and actions in terms of their effects on the entire organization, as opposed to only in terms of the individual unit most directly affected.

Evaluation of integration judges the extent and nature of mechanisms for coordination that are built into a quality system. This is a central issue for an effective, organization-wide system. If each functional unit attempts to independently create its own quality

system, problem identification and problem-solving are likely to be limited by a narrow view of the issues being addressed and by insufficient authority to fully implement decisions for change, in order to standardize improved methods in the organization.

**Focus on Process.** Effective quality systems focus on processes (how the work is done) rather than only on outcomes or results. They rely on methods of problem identification and problem-solving that attempt to discover the link between actions and outcomes.

Many performance indicators used by facilities focus on results achieved, such as the number of events in a given time period or a power plant's annual capacity factor. While these outcomes are very important indicators of a plant's performance, knowing this information by itself does not provide a basis for improving facility safety or production performance. These indicators measure the results of processes; they do not provide information on the processes that led to these results.

Focusing on process refers to the specific methods for assuring quality. These include, for example, how the planning method for scheduled outages is designed and actually carried out, and whether these methods lead to a well-executed outage. Evaluation of a process focus is based on evidence of a facility's ability to both determine how processes lead to specific outcomes and to use this knowledge for solving problems to improve safety performance.

### **Evaluation of the Formal Quality System and Actual Practices**

In order to determine the effectiveness of a nuclear facility's quality system both the formal system and actual practices need to be evaluated. The formal system refers to the design of methods for problem identification, problem-solving and standardizing solutions. It is the description of how the quality system is supposed to function at a facility. Actual practices refers to what methods are used at a facility to ensure that desired levels of performance are achieved.

A facility may have a well-designed set of methods covering all quality system components, however, if these methods are not followed, the quality system as a whole, is not effective. On the other hand, it is possible (although in practice not typical) to use effective quality system methods even though the design of the quality system is poor.

This situation occurs when facility staff use effective quality system methods although these methods are not part of the formal policies and procedures of the facility. There is still a significant weakness in the overall quality system (although particular activities are carried out appropriately) because the system is relying solely on individual actions without established methods for assurance of the continuance of these actions when a particular individual changes positions and is replaced by someone else.

### **SUMMARY**

Applying the evaluation method requires collecting information and analyzing that information to make judgements about the effectiveness of the quality system.

Information must be:

- selective;
- cover all the components in the improvement cycle; and
- capture the dynamic nature of the quality system.

The analysis must then use the information to determine:

- if the quality system covers the components of the improvement cycle (identify problems, solve problems, standardize solutions);
- if it is prevention based;
- if it is integrated; and
- if it is focused on process as well as outcomes.

## **TWO SOLUTIONS TO THE SAME PROBLEM - ASSESSING PROCESSES AND THEIR OUTCOMES**

Gerd Svensson  
Swedish Nuclear Power Inspectorate  
P.B. 27 106  
S-102 52 Stockholm, Sweden

### **INTRODUCTION**

Complex systems such as nuclear power plants are continuously in development. Observations in daily work by operational and maintenance staff, experiences from minor incidents and planned systematic analyses using PSA are a few but important sources for development.

From a regulatory point of view different positions can be taken when assessing the solutions presented by the plants to the problems identified. The purpose of the paper is to delineate questions asked within a more process-oriented regulatory approach taking examples from a recent case-study.

### **THE FRAME-WORK**

As has been shown by Olson & Thurber (1991) plants differ widely in how they go about solving problems. They differ in their readiness to recognize the need for change, in understanding the true nature of the problem, in creating viable solutions, following them through and in continuing the improvement cycle. The availability and quality of technical resources has an impact on the process as has the competency and credibility of the investigators. The resources and mechanisms provided to support integration and communication between groups and departments is an important factor in all phases. Such differences can be expressed in terms of the engineering, structural, managerial and cultural capacities of the organization to handle the improvement potential.

Thus, there are differences in what is done and how it is done that can be used in plant assessments. These are differences in processes. Such a process-orientation can also be used as a complementary tool in assessments of solutions to an identified problem. It happens that plants which are similar from a technical point of view come up with different solutions. This is often the case when PSA has identified a critical manual operation. One plant might

decide to support the manual operation with changes in instrumentation, procedures, and training whereas another similar plant fully automates the operation.

## THE CASE

Loss of the main and auxiliary feedwater systems followed by failure to manually initiate depressurization is a critical sequence identified in the safety analysis of the newest Swedish BWRs. Automatic depressurization can only take place when low water level in the reactor occurs in combination with high pressure in the containment. Later a modification was made to the effect that the depressurization function could be activated manually from the control room on low water level. In the safety analysis the sequence was calculated to occur with a frequency of  $4.3 \times 10^{-6}$  per year or less depending upon differences in the design. The sequence dominated the total core damage frequency.

In the opinion of the Inspectorate the problem had not been handled satisfactorily neither by plant modifications nor by a satisfactory analysis showing that no further actions were needed. The Inspectorate therefore asked the utilities to present a solution to the problem in conjunction with licensing for routine operations. In the following some questions are discussed which were part of the human factors review.

### What value is put on problem recognition?

Organizations differ in their orientation towards problem recognition. The problems may go unrecognized until the Inspectorate or another external agent bring them to the plant's attention. In this case the initiative for reconsideration came from the Inspectorate, and the work done by the plants was an answer to that. It is then interesting to observe how much effort the plant is willing to spend in order to take ownership of the problem.

Some organizations may be more compliance oriented, trying to just comply with the implicit demands of the external agent. Some organizations will argue for their solution in place, not showing efforts to consider alternative solutions or to more fully understand the problem. Other organizations may use the possibility to, maybe once more, challenge their own previous understanding of the problem.

### How are different groups and experiences included?

PSA- studies are often performed by a few specialists, sometimes not working in the actual plant. The request stimulated in one plant the development of an approach where separate deterministic, probabilistic, human factors, and operational experience studies were made in the problem analytic phase. The four perspectives were later integrated towards the decision phase.

In the human factors analysis, control room staff and instructors analysed four scenarios. They were asked to assess the difficulty in the detection, decision and action phases. Factors considered by the operators were mainly the training, procedures, process information and the number of choices available.

In the PSA-analysis of the sequence, as reported by Hirschberg (1990), conflicting goals and time pressure were seen as the main factors behind nonactivation of manual

depressurization. Operators might feel reluctant to perform the action in view of the consequences associated with unjustified initiation of depressurization. A depressurization event is expected to lead to a relatively long shut-down period due to the substantial loads to which the plant structures are exposed and subsequent need to check the affected equipment. If depressurization is needed, but not carried out, the consequences can be disastrous.

The difference in perspectives of the operators in the plant study and the PSA- analysts is interesting. The operators stress difficulties in diagnosing and handling the situation due to unreliable indications of water level in the reactor vessel. Their procedures also cover measures when level indications are unreliable. As observed by Norros & Reiman (1991) operator conception of risk is to a great extent acquired through earlier operational experience and is different from the analytical engineering view of risk.

The differences in the actual case also indicates that the analytical and the operational approaches are not well integrated in the organization, and that there might be a big learning potential for both in consciously trying to increase their integration.

A more analytical behavioural approach was lacking. The application of deep behavioural knowledge could mean an even better understanding of the problem.

### What levels in the organization are considered in the analysis?

Usually only the operator level is considered in this kind of analysis, whereas managerial and organizational factors are not taken into account. This is also the case in both the PSA-analysis and the operator study described above.

Operational observations would however suggest that this is a decision situation where managerial behaviour could have an impact on operator behaviour e.g. the priorities given to safety and economics in decision making. In reality, the decision to initiate depressurization might be a decision taken by operational management. One approach could for example be to analyse the decision situation (Table 1) both from the operators' and the management's point of view in terms of

- probabilities for different outcomes
- costs for different outcomes
- costs to increase the probability of correct action
- safety enhancements to increase the probability of correct action.

Table 1. Decision situation in depressurization.

		<i>Action called for</i>	
		<i>No DP</i>	<i>DP</i>
<i>Action performed</i>	<i>No DP</i>	Correct	Failure
	<i>DP</i>	Unjustified	Correct

### **Is operating experience reviewed?**

In cases like this, there often is a review of operational experience, own and others. In good projects the review includes besides hardware aspects a review of human aspects. In this case an analysis was made of experiences from failures of the feed water systems in the plant and worldwide. Experiences from events and situations were not systematically analysed where operators and managers had to make a decision facing conflicting goals.

### **Are alternative solutions analysed?**

Developing alternative solutions is thought to encourage consideration of disadvantages as well as advantages of possible solutions. It is also hoped to be a means for avoiding getting locked into a favoured first idea. As in this case, often only one alternative is thoroughly analysed.

Decisions on a suitable automation level is one of the most critical during design and design modifications. In the guidance document developed by Bastl et al (1991) general principles are stated for assigning a specific function to human or to machine. It is e.g. stated that automation should be used to protect society from the fallibility and variability of humans. It should therefore be used when human capacity could easily be overloaded such as situations with severe consequences in case of error, and tasks requiring rapid performance, processing of large quantities of data, high accuracy or repeatability. Human cognitive strengths should be used. Functions which require heuristic or inferential knowledge, and particular flexibility should be assigned to humans. Automated tasks should not be designed to depend upon the human when automation fails.

Initiation of depressurization was in one of the organizations fully automated due to the serious consequences in case of error and the short time available for action in some scenarios. The initiation was made dependent on low water level, but depressurization could be delayed by the operator. Although automated, the function thus could become dependent upon the human actions taken, which indicates that there are problems with the solution.

The other plant decided first to solve the problem with the unreliable level indications. A successful solution of that problem should improve the decision situation of the operators as well as the conditions for a more automatic initiation of depressurization. Improved level measurements should also facilitate operator decision making in other sequences.

## **CONCLUSIONS**

The plants differ somewhat in design, which might have influenced the decisions taken. There were however also differences in how they approached solving the problem. These seemed mainly to be differences in how well different groups and experiences were integrated in the analysis of the problem. It is expected that further improvements can be made through consciously including deep behavioural knowledge into the analysis, particularly in the analysis of operational decision situations on management and operator level involving conflicting goals.



## REFERENCES

- Bastl, W., Jenkinson, J., Kossilov, A., Olmstead, R.A., Oudiz, A., and Sun, B., 1991, Balance between automation and human actions in NPP operation. In "Proceedings of an International Symposium on Balancing Automation and Human Action in Nuclear Power Plants jointly organized by IAEA and NEA", IAEA, Wien.
- Hirschberg, S., (ed.), 1990, "Dependencies, human interaction and uncertainties in probabilistic safety assessment." Final report of the NKA RAS 470, ABB Atom, Västerås.
- Norros, L., and Reiman, L., 1991, Uncertainties in the system as a challenge for NPP operators' expertise. Paper presented at "Probabilistic Safety Assessment and Management", Beverly Hills, California, 1991.
- Olson, J., and Thurber, J., 1991, Learning in nuclear power plants. Paper presented at a consultants meeting "The influence of organization and management on the safety of NPPs and other complex industrial systems", IAEA & IIASA, WP-91-28, July, 1991.

## **108 Interactive Fault Detection and Diagnosis--Approaches**

*Chair: A. Poucet, ITER EDA*

**Development of Diagnosis Systems of Autonomous Operation System for Nuclear Power Plants**

*A. Saiki, K. Okusa, A. Endou (PR& NFD Corp., Japan)*

**A Unified Paradigm for Verifying Reliability Requirements in Dynamic Systems**

*J. Ruiz, M. Roush (U. Maryland)*

**Towards a Taxonomy of System Failures**

*J. Ruiz, M. Modarres (U. Maryland)*

## DEVELOPMENT OF DIAGNOSIS SYSTEMS OF AUTONOMOUS OPERATION SYSTEM FOR NUCLEAR POWER PLANTS

A.Saiki, K.Okusa, and A.Endou

Oarai Engineering Center,  
Power Reactor and Nuclear Fuel Development Corp.,  
Oarai, Ibaraki, Japan 310

### INTRODUCTION

The authors have been developing an autonomous operation system for nuclear power plants. Prime objective of the system is to grade up operation reliability by eliminating human factors and enhancing control capabilities. For this objective, both operator's role and traditional controllers are replaced with artificial intelligence (AI) systems. Construction of a prototype system for a loop type Fast Breeder Reactor(FBR) plant was planned as a means of evaluating applicability of AI systems to the autonomous operation. Main targets of the prototype system are to enhance control capabilities at a normal operation mode and to allow the AI systems to operate the plant in case of anomalies.

In the present paper, norms of autonomy and conceptual design for the prototype system(Endou et al.,1993) are described briefly and two types of methods for diagnosis in the prototype system are proposed on the basis of the conceptual design. One of the method is to determine whether a current operational mode can be maintained in case of anomalies. The other is to identify root causes of anomalies. Both methods are intended to take in changes or effects due to reorganization of functional structure of the plant which is one of essential features of autonomous operation systems.

### AUTONOMOUS OPERATION SYSTEM

Norms of autonomy are defined(Miki et al.,1989) as follows based on an analysis of functions of nuclear power plants; (a) to maintain its own basic functions, (b) to protect oneself from catastrophic events, (c) to reorganize oneself in case of its partial failure, (d) to harmonize with the environment, and (e) to improve its performance by itself.

It can be said that the norm (b) and (d) are almost realized by the plant system itself in the current nuclear plants. On the other hand, the current plants require proper human assist to achieve the norm (a),(c) and (e). Consequently, the most significant subject to be solved immediately in the development of the autonomous operation system is to substitute AI systems for human roles relevant to the norm (a),(c) and (e) in existing plants. In the prototype system, a great emphasis is put on realizing the norm (a) and (c).

For the norm (a), AI systems have to realize knowledge based actions such as human operators would do in case of settling of unanticipated occurrences and unusual application or rearrangement of plant equipment. Therefore, the authors take a model-based approach to which basic features of human cognitive process are reflected. The models should be constructed from multiple viewpoints so as to make them applicable to as many kinds of problems as possible. Consequently, changing a point of view in human problem solving process can be realized by means of selecting a suitable model according to circumstances.

For the norm (c), the autonomous operation system itself must have capability of reorganization of its functions as same as plant system does. A hierarchical distributed cooperative system as shown in Fig.1 is adopted for the autonomous operation system, because distributed cooperative system is superior to centralized system in many respects such as the reorganization, localization of failure effect and because hierarchical system is appropriate for controlling simultaneously subordinate systems. A multi-agent architecture suitable for constructing distributed cooperative systems is applied. Each function such as diagnosis shown in Fig.1 is realized as an agent which consists of a knowledgebase and an inference engine. Methodology diversification is adopted so as to facilitate the reorganization of the functions in the operation system. The methodology diversification is a concept that several methods based on different principles are applied to one specific task in diagnosis or control. An agent which executes a task based on one method is named method agent. The methodology diversification has effects to prevent loss of system functions due to common cause failure by mutual backup and to isolate a failed agent from the system. In order to realize diversity in methodology, an upper level agent is adopted to coordinate method agents. The upper level agent tries to avoid inconsistency among conclusions derived from method agents and to reach a consensus. It also makes the configuration of multi-agent system simpler and reduces the amount of intercommunication among agents.

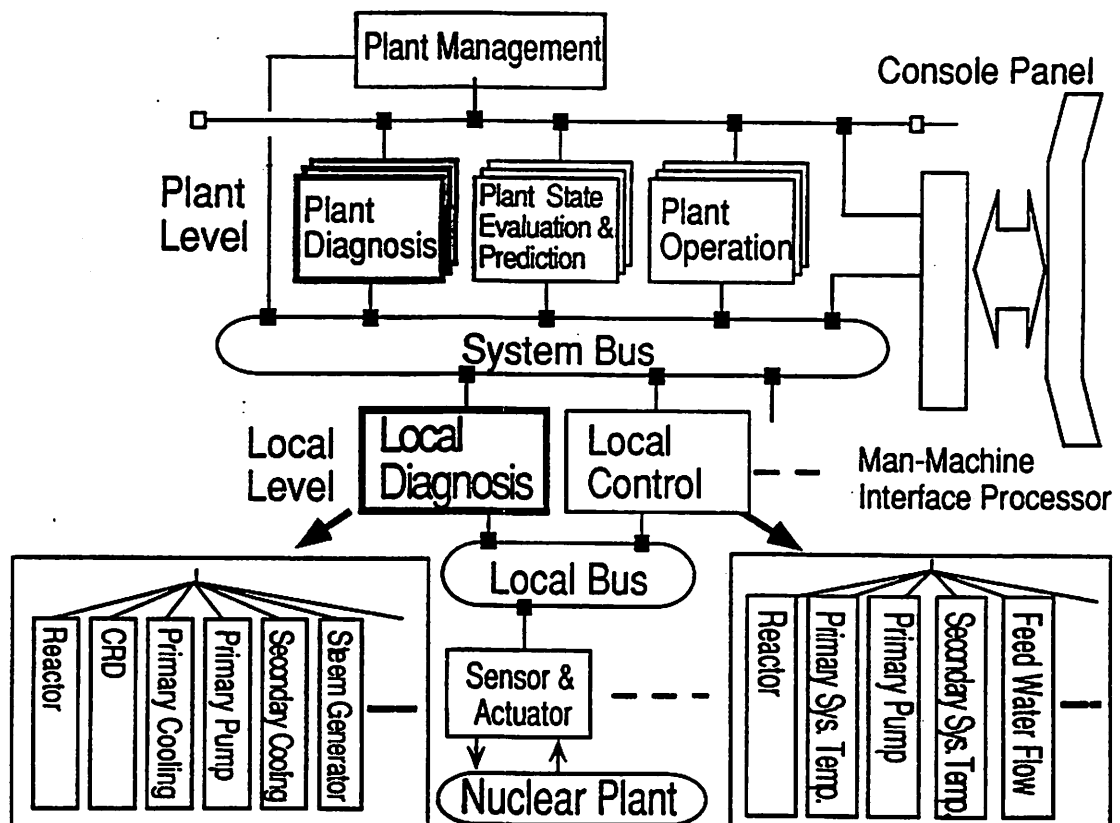


Fig.1 Configuration of prototype autonomous operation system.

One of the aims in distribution of control or diagnosis task is to execute processing efficiently, because distributed agents for decomposed tasks can execute their tasks concurrently. Control and diagnosis agents at local level in the prototype system are prepared for every control system as shown in Fig.1. On the other hand, agents at plant level are prepared for every plant operational mode for the sake of reduction of their task's complexity.

## DIAGNOSIS FUNCTIONS

A main role of diagnosis agents in the autonomous operation system is to obtain information so that control agents can take proper actions. Main actions of the control agents in case of anomalies would be as follows; (a) to choose an appropriate operational mode or efficient control strategies, (b) to reorganize plant functional structure appropriate for the situations if needed, (c) to remove or to fix root causes. Therefore, diagnosis agents in the autonomous operation system should acquire information necessary for both action (a) and (c). In addition, the changes of functional structure of the plant due to the action (b) should be reflected in agents' knowledgebases.

In the prototype system, agents for the plant diagnosis obtain information necessary for the action (a) and agents for the local diagnosis work for the action (c).

### Plant Diagnosis Function

The authors adopt a method using a hierarchical plant functional model as the plant diagnosis which determines whether the control agents will be able to maintain their control goals in case of anomalies.

In the model, an operation goal is positioned at the top and functions necessary to attain the goal are located as subgoals at immediately subordinate positions. In the same manner, a function is decomposed into lower functions. The decomposition of the functions ends at component function level. Fig.2 shows a part of the model for a full power operation mode of an FBR plant. Dashed arrows indicate side effects from a function to others but superior ones. As shown in Fig.2, controlling feed water(FW) flow rate which is a subgoal of controlling heat sink would effect pressure at turbine inlet stream, but the effect would not be used for controlling the pressure.

Knowledge about functional relationship to upper and to lower functions, side effects, methods of examining whether normal conditions can be maintained should be defined for every function. Multiple methods of examination should be defined according to the concept of methodology diversification. The methods that can be defined are as follows; failure detection by set values of alarm signals, estimation based on conservation law of mass or energy, logical integration of conclusions at lower level functions, use of results derived from the local diagnosis, estimation derived from living PSA system(Dinsmore,1989) and so on.

As mentioned before, the plant functional model should be modified according to the reorganization in case of anomalies. A plant diagnosis agent is prepared for every plant operational mode. When an operational mode must be changed for some reason, a plant diagnosis agent for a new operational mode should begin to work. The reorganization at a lower level function is reflected in its active state and its normal conditions. There are several types of active state, such as working, waiting, starting, being isolated. One of waiting functions works only in case of anomalies or another one could substitute other functions. The function for controlling temperature of turbine inlet steam surrounded by dashed rectangle in Fig.2 is an example of a waiting function, because the aim of the function is to decrease the temperature only when it increases abnormally. Starting function is one under way from waiting to working. In case of anomalies, a working function estimated anomalous would be usually isolated so that the function would not affect superior functions.

When anomalies are detected, the plant diagnosis agent tries to distinguish which functions are failed and to investigate relevancy among them. The investigation should take both results estimated according to the normal conditions and the current active state into consideration. When a working function is evaluated to be anomalous, the effect of the anomalous function would influence its superior functions. In this case, it is necessary to search the highest function that is estimated to be effected from the failed function. On the other hand, when a failed function is isolated due to reorganization, then the diagnosis agent does not conclude that the influence would extend to superior functions of the failed function.

An plant diagnosis agent whose model is shown in Fig.2 has been constructed. As a result of the diagnosis using simulated data, it was confirmed that functions effected by a malfunction could be distinguished whether the malfunction was identified or not. Implementation of a mechanism for rebuilding of the model according to the reorganization will keep in step with development of control agents so as to take intercommunication among these agents into account.

### Local Diagnosis Function

The authors adopt method based on a causal network model for identifying root causes of anomalies. The root causes must be identified concretely. Therefore, the model represents both components and process parameters associated with the components as nodes and causal relations among the nodes as links. Fig.3 shows a part of a causal network for an evaporator of an FBR plant at a power operation mode. Arrows in Fig.3 show directions of the causality between pair of nodes. The diagnosis is proceeded by tracking lines reversely to the arrows from symptoms to candidates of root causes. The local diagnosis has to detect those symptoms

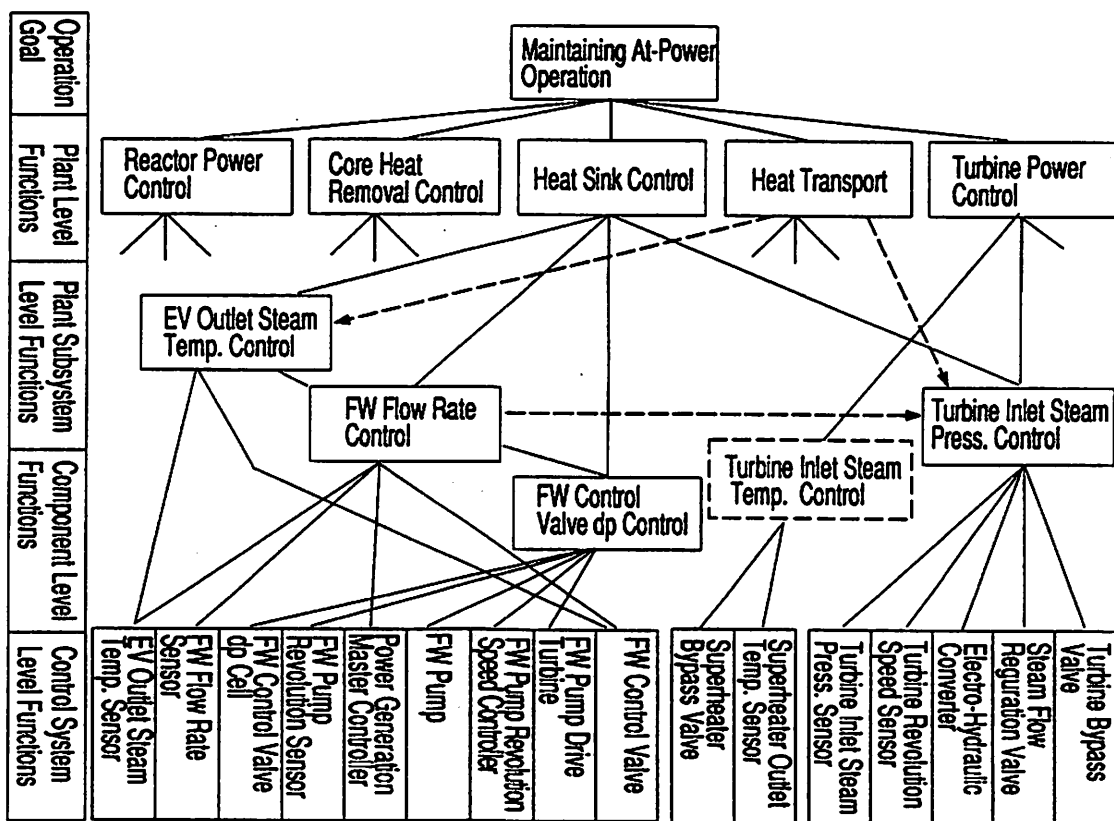


Fig.2 An example of hierarchical plant function model for an FBR plant. Solid lines show the functional relations and dashed lines show side effect relations. Functions surrounded by dashed rectangle are waiting functions.

in order to take countermeasure before significant affection would appear. Numerous methods for detecting anomalies have been proposed, such as harmonic analysis, computational mechanics, optimal estimation, statistical test, fuzzy inference, neural network. According to the concept of methodology diversification, an appropriate set of these methods should be applied to every node for detecting its anomaly.

In general, it is difficult to diagnose a large scale system such as a nuclear plant using its causal network because of its complexity. Decomposition of the total causal network into subnetworks is applied so as to reduce the complexity. The subnetwork is constructed for every plant subsystem as shown in Fig.1. Neighboring networks are connected to each other by same observable node(s) whose state can be monitored. The node for feed water flow in Fig.3 is one of such connecting nodes. Furthermore, active causal links defined next paragraph allow to search effectively which subnetwork includes the root causes of the anomalies.

The active causal links represent relations among process parameters associated with a stream of mass or energy which should exist in a normal situation. If a stream must be cut off for some reason such as change of plant operational mode, then the state of causal links associated with the stream should become nonactive. All of the effects are transmitted along with the streams in a normal situation. Consequently, influence from a root cause occurred in a causal network can be found only in active links in other networks. This is the reason why the effective search for a root cause can be executed using active links.

The reorganization of plant functional structure may lead to change the directions of some streams or to cut off other streams. Therefore, the result of the reorganization can be reflected in directions and active states of causal links.

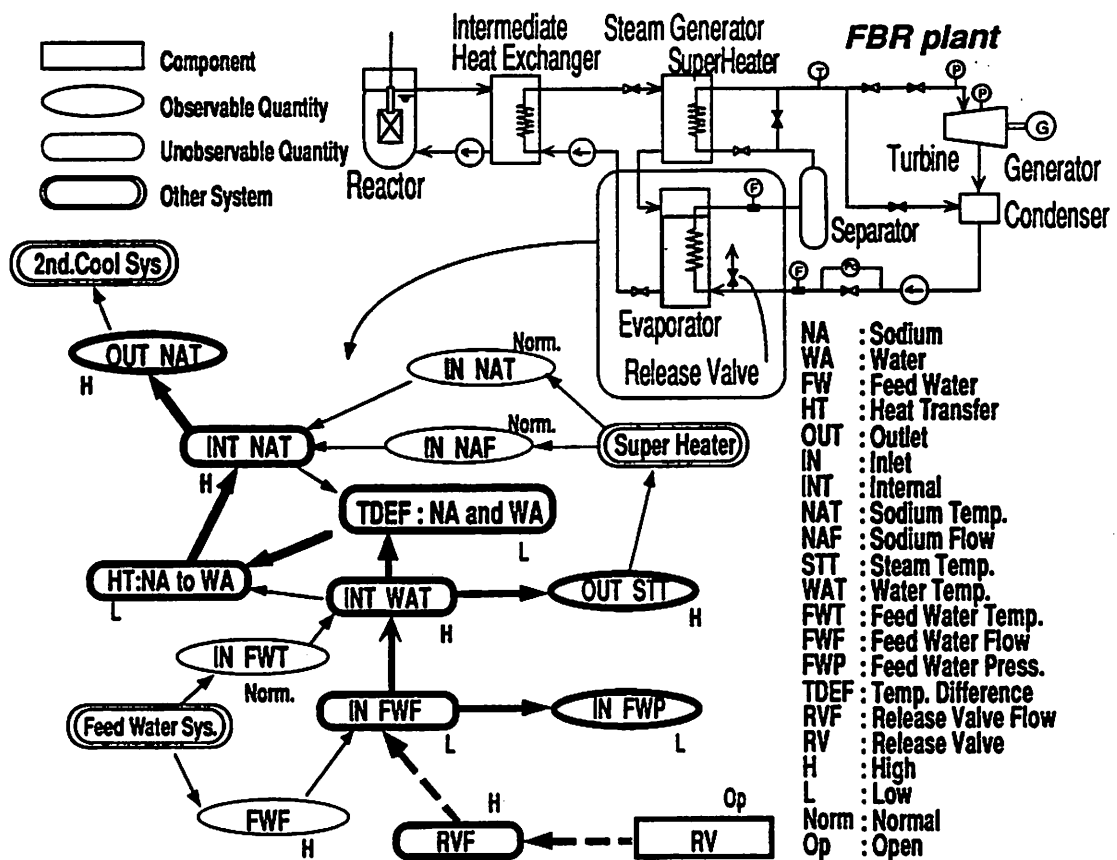


Fig.3 A part of causal network model for an evaporator at a power operation mode. Solid and dashed lines show active and non-active causal links respectively.

At the first step of the diagnosis, every agent of local diagnosis whose network involves anomalous nodes tries to search routes effected by root causes among its active links. If a source node of the routes is connected with other causal network, it is concluded that the influences of anomalies may come from other causal network, because anomalies from other causal networks pass through active causal links as mentioned before. In Fig.3, if temperature at inlet sodium which is connected with the causal network for super heater is inferred to be a source node of anomalies, the influence may come from super heater. If it is inferred that there is no effected route from other networks, then the diagnosis agent tries to search effected routes among non-active causal links and to find candidates of root causes. Fig.3 also illustrates the reasoning process to infer the root cause when temperature at inlet sodium is observed as high to excess. Reasoning is proceeded by tracking bold lines and bold dashed lines reversely to the arrows. In this case, as no influence from other networks is found, the release valve is identified as a root cause.

Implementation of both reasoning mechanism and a network for the evaporator and the super heater shown in Fig.3 has been carried out. As a result of diagnosis, it was concluded that identification of root causes using a causal network could be done. Diagnosis by distributed agents and reflecting of the reorganization in the causal networks as presented in this article are now under development.

## CONCLUSION

A model-based approach is taken to realize humanlike decision-making process by AI systems. A hierarchical distributed cooperative configuration is adopted to the system because of its superiority in reorganization of system functions. The system is realized by a multi-agent system. In the system, methodology diversification is assured by preparing different types of method agent. An upper level agent of method agents is also presented whose roles are coordination of method agents.

Diagnosis methods to determine whether a current operational mode can be maintained based on the hierarchical plant function model and to identify root causes of anomalies based on the distributed causal networks are applied to the prototype autonomous operation system. Both models can take in the effect of the reorganization of plant functional structure. The plant hierarchical model reflects the reorganization in active states of functions. On the other hand, the causal network reflects it in active states of nodes and the directions of the causal links. The active states of the causal links also allow to search root causes efficiently in distributed networks. Application of methodology diversification to both diagnosis methods are also presented.

The validation of the diagnosis methods will be conducted by connecting to a building block type FBR plant simulator(Endou et al.,1992). Development of hierarchical distributed cooperation, rebuilding of the models due to the reorganization, methodology diversification described in the present article are now under development.

## REFERENCE

- Dinsmore,S.C.,Balfanz,H.P.,1989,Living PRA computer systems,Nuclear Safety,Vol.30,No.3.
- Endou,A.,Terashita,N.,Watanabe,K.,1992, Development of building block type simulator for FBR plants, Expert Systems and Computer Simulation in Energy Engineering, Erlangen Germany.
- Endou,A.,Saiki,A.,Miki,T.,Himeno,Y.,1993,Conceptual design of autonomous operation system for nuclear power plants,Joint International Conference on Mathematical Methods and Supercomputing in Nuclear Applications, Karlsruhe, Germany.
- Miki,T.,Tamayama,K.,1989,Conceptual research of autonomous nuclear power plants", Power Plant Dynamics, Control & Testing Symposium, Knoxville, Tennessee, USA.



## A UNIFIED PARADIGM FOR SPECIFYING, MODELING, AND VERIFYING DYNAMIC SYSTEMS

J. Cyrano Ruiz and Marvin L. Roush

Center for Reliability Engineering  
Department of Materials and Nuclear Engineering  
University of Maryland, College Park, Maryland, U.S.A.

### INTRODUCTION

This paper presents an integrated paradigm for Specifying, Modeling, and Verifying (SMV) dynamic systems. The process is performed in three integrated phases.

The first phase of SMV is the *specification* of the system. Relevant characteristics of the system components are specified. These descriptions subsume elements such as: components, events, common-cause failures, and shocks. The specification uses the programming-like syntax (by "programming-like" it is meant a syntax that is similar in style to usual programming languages (e.g., Pascal, Basic, etc . . . ) ) called Reliability Descriptive Language (RDL).

The second phase is the model *generation*. In this phase, the RDL specification of the system is translated into a mathematical model. The translation is performed by a compiler that generates a new extension of Petri nets<sup>1,2,3</sup>, termed Reliability System Assessment Petri nets (RSA Pnets). From this RSA Pnet representation of the system, a reachability state generator automatically synthesizes the event-sequences of the system.

The third phase is the *verification* of the system. Here, the behavior of the system is analyzed using the event-sequences generated in the previous phase. The approach taken in SMV involves automated verification techniques known as model-checking<sup>4</sup>. The specific properties that need to be verified are expressed through formulas written in a new query language called: Reliability Query Language (RQL), which is based on (branching) Temporal Logic.

### THE SPECIFICATION PHASE

As explained in the introduction, the first phase in the SMV paradigm is the specification of the system in question. A more detailed explanation of RDL is given in this section. However, for reasons of space, only a conceptual description of RDL can be presented here. The complete syntax of RDL is defined elsewhere<sup>5</sup>, by means of *Context-Free Grammars* (CFG)<sup>9</sup>. The RDL specification is performed in a "Bottom-Up"

style. The system is defined by listing its components, subsystems, and the way these interact. The "Bottom-Up" approach is sometimes contrasted to the viewpoint known as "Top-Down," or "functional," in which systems are described starting from a high-level formulation of global functions, and proceeding to decompose each function into subfunctions, and so on.

In RDL, the functional information is not provided explicitly. As in other Bottom-Up descriptive approaches, the definitions of functions are implicitly subsumed in the description of components and their interactions. Interactions among components are mainly described through *events*. Thus, from this point of view, the SMV paradigm also belongs to the class of methodologies known as "event-driven." The event-driven approach is very a convenient one for the description of the behavior of dynamic systems.

In general, the structure of an RDL syntactic specification consists of the major following sections:

a) **Component Section** (required): in which system entities such as: pumps, valves, switches, human operators, etc . . . , are described. For each of these, one specifies its name, possible states, initial state, and internal transitions. The term "internal transition" represents possible transitions from one component-state to another. They are "internal" in the sense that they occur without the interaction of other components considered in the analysis.

b) **Special Places** (optional): to offer a means of defining "intermediate states or conditions" in the system. For instance, suppose a phased-mission is being analyzed. In that case, it is desirable to indicate that a certain intermediate phase of the mission has already been achieved. Special places may also play the role of "intermediate events" in Fault Trees<sup>6,7,8</sup>. Another example of special places is given, for instance, in cooling systems. In such systems, the analyst is usually concerned about the temperature and pressure at certain critical points within the piping lines. These critical points are not components *per se*, but can be described through special places.

c) **Defining Failure and Success Sets** (optional): failure or success criteria can be defined. To do this, a collection of state-component sets are specified. During operation, the components may reach simultaneously a global state prescribed by one of the defined failure or success sets. Should this happen, a system mission failure, or a system mission success would have been achieved, respectively.

d) **Simultaneous Internal Transition Sets (SITS)** (optional): in some cases it is necessary to contemplate the possibility of various events happening simultaneously. For instance, suppose a system contains two identical pumps. After describing the two pumps individually, an RDL specification may allow the definition of a SITS called, say, "Two\_Pumps\_Fail." The applications of SITS to the analysis of *Common Cause Failures* should be evident.

e) **Event Section** (required): the event section lays out the relationship among the different components and special places. For each event, one specifies: its name, its preconditions, and its consequences. Preconditions are essentially boolean expressions combining different component states and/or special places. If the boolean expression is true, then the event can take place. Consequences are essentially a list of component states. After an event occurs, certain components

(usually) change from one state to another. These new states are listed as consequences of the event being defined.

f) **Comments** (optional): to enhance the readability and understandability of RDL specifications. These comments are Pascal-like, that is, they consist of arbitrary text enclosed within the symbols: “(“ and “)”.

Figure 1 depicts a small fragment of a specification for RDL. The example shows only the description of an specific system component. For reasons of space, other sections of an RDL specification have not been included. However, the portion displayed in figure 1 should provide the reader with a more concrete idea of the “syntactic-look” of RDL. This fragment is taken, *verbatim*, from a complete RDL description of the Nitric Acid Cooling System<sup>5</sup>. The main elements involved in this system are a temperature sensor, an indicator, controller, two water pumps, a heat exchanger, two valves, and a human operator. A complete description of the system is of little use here.

```

component begin
  name:=INDICATOR;
  states:=
    dim1 := VL, L, N, H, VH; (* temperature *)
    dim2 := NORMAL, STUCK, FAILED; (* status *)
  initially := [ N, NORMAL ];
  internal transitions begin
    GETS_STUCK: from [ * , NORMAL ] to [ * , STUCK ];
    FAILS_HIGH: from [ * , NORMAL ] to [ VH , FAILED];
    FAILS_LOW: from [ * , NORMAL ] to [ VL , FAILED];
  end; (* internal transitions *)
end; (* INDICATOR *)

```

Figure 1. RDL Specification of Temperature Indicator

## THE MODEL-GENERATION PHASE

As mentioned in the introduction, the second phase of the SMV paradigm consists in generating a mathematical model from the previous RDL specification. The mathematical entity used in SMV is an extension of standard Pnets, termed RSA Pnets. The translation is automatically performed by a “compiler,” which takes the RDL specification as an input (a standard ASCII file), and produces a (computer representation) of the RSA Pnet model. From this RSA Pnet, a state-space generator is executed<sup>5</sup>, yielding all the possible event-sequences. It is important to indicate that this phase is transparent for the user (i.e., the analyst) whose role in SMV is restricted to the first and the third phases. The generation of the RSA Pnet as well as the event-sequence computation are performed automatically.

There exist several advantages in adopting a Pnet modeling framework. Pnets provide a precise formalism for state-space analysis<sup>1,2,3</sup>. They also prove to be a convenient visual-communication aid for describing complex systems. In general, Pnets can be applied to model any system that requires some means of representing parallel or concurrent activities. Analysis of their reachability state space can reveal important information about the structure and dynamic behavior of the modeled system<sup>15</sup>. Many properties about the executional behavior of a modeled system can be verified by studying the corresponding coverability graph<sup>3,10</sup>.

Since its original formulation in 1962, Pnet theory has grown considerably and researchers have proposed many practical applications and extensions to the original model. However, one of the main problems with extending the original Pnet model is that the analysis of the proposed extensions can become untractable. In other words, modeling *convenience* is improved at the cost of given up *analytical power*. This is a usual tradeoff in modeling.

Keeping a fair balance in this tradeoff was a central concern in developing the SMV paradigm. RSA Pnets, the extension to Pnets utilized in SMV, provide sufficient modeling convenience, and at the same time are amenable to a full analysis. In essence, the extension was conceived in such a way that every RDL syntactic construct finds a natural interpretation in RSA Pnets.

The usual Pnet notion of "markings," "firing-rules," and "places and transitions" have been generalized to reflect the different syntax-constructs in RDL. A complete description of RSA Pnets exists<sup>5</sup>, but falls out of the scope of this presentation.

## THE VERIFICATION PHASE

As mentioned in the introduction, the query language (RQL) used in SMV is based on Temporal Logic<sup>11,12,14</sup>. The need for a "temporal" dimension in a query language for dynamical systems is clear. Conventional (predicate) logic can be used to express properties such as "component X is failed," or "component Y is working." However, more complex statements involving sequences of events are not easily formulated through conventional logic.

Dynamic systems produce sequences of states as certain events occur. There is thus a need to reason about sequences. These sequences (or "*paths*," as they are also termed), lie at the heart of Temporal Logic and the model-checking techniques. The notion of "time" used here is not an "absolute" one (e.g., expressed in minutes or hours). In SMV, the notion of "time" corresponds to the ordering of the event-sequences generated as the system operates<sup>13</sup>.

Given an initial state, one or more events may happen. When one of these events occurs, the system goes to other states. In those new states, other events may happen, and this process is repeated. In this way, the event-sequences can be visualized as a tree-like structure.

This tree structure has been used in conventional reliability analysis techniques like the Event Tree Methodology in which the analysis starts with an *initiating event*. From this event, the analyst constructs the branches that represent the possible events following the initiating event. This process is repeated and an Event Tree is thus generated. The resulting event-sequences are used to compute probabilities. Also, the Event Tree formulation is usually performed manually by the analysts.

By contrast, in SMV the event-sequences are automatically synthesized from the RDL specification. The event-sequences can be analyzed in more detail to verify more complex properties corresponding to the system behavior. For instance, the relative *order* in which two events occur within a sequence can be important in specific applications. Also, in some systems it may be important to verify that after a certain event has occurred, another specific event occurs (or is avoided). RQL, used along with model-checking techniques, addresses these questions and similar ones.

To do this, RQL introduces *path quantifiers* that allow the reasoning about sequences. Suppose *p* and *g* describe two possible state-configurations. Table 1, shows some of the typical RQL formulations and their corresponding intuitive interpretation (the validity of the formulas depends upon the state that is taken as a reference. Usually, it is assumed that the initial state is taken as a basis). Many of the properties in this table could be

considered "goal-directed" requirements. By verifying properties such as these, one could prove (or disprove) that the system meets specific goals.

Table 1. RQL formulas and their intuitive meaning

COMBINATION	INTUITIVE MEANING
$AF (p)$	$p$ is inevitable
$EF (p)$	$p$ is attainable (feasible)
$AG (p)$	$p$ is invariant
$AG (p \Rightarrow AF (g))$	$q$ is eventually achieved after $p$
$AG (p \Rightarrow AF (\neg g))$	$q$ eventually ceases after $p$
$AG (p \Rightarrow AG (q))$	$q$ is maintained after $p$
$AG (p \Rightarrow AG (\neg q))$	$q$ is avoided after $p$

There are two compelling reasons to use a query language like RQL. First, because the properties can be formulated concisely and precisely. RQL provides a well-defined concrete syntax leaving no room for ambiguities. Second, because there have been many efforts in developing efficient model-checking algorithms to verify Temporal Logic formulas<sup>4</sup> within large state-event spaces. A verification scheme taking RQL as a basis could benefit from these already existing algorithms.

## CONCLUSIONS

The SMV paradigm also constitutes an useful tool for the verification of reliability and safety-related properties of dynamic systems. Being a bottom-up approach, the SMV paradigm is more useful during late stages of the design phase. In summary, the primary advantages of SMV are:

- Event-sequences, which represent the behavior of the system, are *automatically synthesized* from the (RDL) specification of the system.
- The modeling framework allows a very comprehensive translation of interactions among components and subsystems, including human actions.
- Events, Common Cause Failure, and Shocks can be modeled explicitly.
- Non-conventional reliability-related verifications can be conducted using RQL. Temporal relationship which are not easily expressed using conventional approaches, can be formulated naturally in RQL.
- Even though the modeling framework is based upon Petri nets, the analyst does not need to understand the intricacies related to this particular mathematical structure. User's interactions are performed exclusively through

the languages RDL, the specification language, and RQL, the query of verification language.

Of course, the SMV paradigm has also some limitations. One of them is that RDL lacks hierarchical structure ("Object-Orientedness"). This makes the description of large systems somewhat cumbersome. However, RDL has to be taken as a prototype tile within a larger picture. Specifying a system via RDL is not the end itself of this paradigm. Rather, what is sought is to verify the behavior of a dynamic system. Obvious extensions to RDL in the syntactical realm or even of a graphical nature are possible, and could be used within the essentially same framework.

## REFERENCES

1. J. Peterson, "*Petri Net Theory and the Modeling of Systems*," Prentice-Hall, ( 1981).
2. W. Reisig, "*Petri Nets: an Introduction*," Springer, New York, (1985).
3. Tadao Murata, "Petri nets: properties, analysis and applications," *Proceedings of the IEEE*, 77, pp. 541-580, (April 1989).
4. E. Clarke *et al.*, "Automatic verification of finite state concurrent systems using temporal logic specifications," *ACM Transactions on Programming Languages and Systems*, pp. 244-263, (August 1986).
5. J. Cyrano Ruiz, "*A Unified Paradigm for specifying, modeling, and verifying dynamic systems*," Ph.D. Dissertation, Center for Reliability Engineering, University of Maryland, College Park, (1993).
6. Patrick D.T. O'Connor, "*Practical Reliability Engineering*," third ed., John Wiley and Sons, (1991).
7. K. C. Kapur and L. R. Lamberson, "*Reliability in Engineering Design*," John Wiley and Sons, Inc., (1977).
8. Mohammad Modarres, "*What Every Engineer Should Know about Reliability and Risk Analysis*," Marcel Dekker, Inc., (1993).
9. Alfred Aho and Ravi Sethi and Jeffrey Ullman, "*Compilers: Principles, Techniques, and Tools*," Addison-Wesley Publishing Company, (1986).
10. Rene David and Hassane Alla, "*Petri Nets and Grafecet: Tools for Modelling Discrete Event Systems*," Prentice Hall International (UK) Ltd., (1992).
11. Anthony Galton, "*Temporal Logics and their applications*," Acad. Press, Harcourt Brace Jovanovich, Publishers, (1987).
12. M. Ben-Ari *et. al.*, "The temporal logic of branching time," *Proc. eighth ACM Symp. on Principles of Programming Languages*, pp. 164-176, (1981).
13. A. Sinachopoulos, "Logics for Petri-nets: partial order logics, branching time logics and how to distinguish between them," pp. 9-14, (August 1989).
14. Emerson and Srinivasan, "Branching time temporal logic," *Proc. of the REX School Workshop 1988 on Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency*, Springer-Verlag, (1989).
15. Antti Valmari, "*State space generation: efficiency and practicality*," Ph.D. Dissertation, Tampere University of Technology, Finland, Publication 55, (1988).

## TOWARDS A TAXONOMY OF SYSTEM FAILURES

J. Cyrano Ruiz and Mohammad Modarres

Center for Reliability Engineering  
Department of Materials and Nuclear Engineering  
University of Maryland, College Park, MD 20742, U.S.A.

### INTRODUCTION

There exist several system assurance methodologies to identify, understand, predict, correct, and avoid system failures. Many new techniques are constantly proposed. Despite ongoing progress, system failures have caused several disasters in the recent past. This situation is unlikely to significantly improve in the foreseeable future. One of the reasons is that technical systems are called upon to perform increasingly complicated and crucial tasks in today's society. No imminent analytical breakthroughs that will eventually guarantee failure-free systems can be anticipated. Thus, the consideration of failures and their causes are and will continue to be important in the analysis of systems<sup>6</sup>.

Generally, system failures do not "*just*" occur randomly. They are the effect of some causes that may be traced back, if the necessary information is available. Failures are not solely "physical" failures (e.g., hardware break-down or wear-out, human errors, or software error). Causes for system failure may originate, as this paper will explain, in any of the phases of the so called: "*system life-cycle*." This cycle usually subsumes the phases of: specification, design, implementation, and operation.

The present paper discusses the "etiology" of failures (i.e., their causes) based upon this system life-cycle. This discussion leads to a generic taxonomy of system failures based upon their original causes. Classification of failures according to their causes is a topic that has been treated by several authors<sup>1,4,5</sup>. In this paper, special attention is paid so that the taxonomy be as *generic* as possible in order to contemplate a maximum number of different types of systems. For instance, software systems are very different in nature than, say, chemical systems. However, most systems share a similar framework for their life-cycle phases, with minor variations. With this assumption (along with its corresponding limitations), a classification of failures is developed in this paper.

### A GENERIC AND SIMPLE MODEL FOR THE SYSTEM LIFE-CYCLE

The process of developing technical systems, especially those of large scale and complexity, follows what is known as the "*system life-cycle*," involving different phases.

Even though these phases are usually listed sequentially, they may be interwoven with each other in practice. In fact, increasingly, there is a tendency to adopt a development scheme known as "Concurrent Engineering," which allow several phases to be conducted simultaneously so that propagation of problems is prevented. Therefore, different phases of the system life-cycle are not necessarily chronological, but are rather driven by a logical cause-consequence relationships.

Several models have been proposed to represent the system life-cycle. Some of these approaches introduce as many as eight or more major stages, while others identify fewer phases. As pointed out in the introduction, the number and nature of these phases is somewhat dependent upon the type of system in question. The description of the system life-cycle utilized in this paper is very generic. The purpose here is not to introduce a new modeling approach for the life-cycle. Rather, the intention is to focus on a simple model based on which a taxonomy of system failures can be suggested. The four major phases considered here are briefly summarized. For the interest of space, the description are presented in an abstract form.

*Specification :* Real-life requirements are carefully analyzed and translated into a set of formal descriptions. Likewise, general and specific goals and constraints are clearly identified. Subsequent phases in the system life-cycle will address the question of "are we developing the *system right*?" But this phase, in particular, poses and considers the more fundamental interrogation of: "are we developing the *right system*?"

*Design:* The functions that the system must perform, the proper level of performance, and the required interfaces are formulated. This develops into a full scale engineering design describing the overall architecture of the system and its components. Prototypes, simulations, and predictions may also be prepared to validate and assess the engineering design. Every function must be traceable to an element in the formal specifications. Also, reliability predictions may be conducted to assess the design.

*Implementation:* The various components and subsystems are engineered (or obtained through procurement and subcontracting). Also, integration of the individual entities takes place. If necessary, human training also takes place. Testing (which sometimes is considered a separate phase) may also be performed for validation purposes, and may assess the levels of reliability and quality.

*Operation:* The system finally performs its intended function during a mission time. Apart from the "normal operation," other events may take place during this phase, such as: preventive/corrective maintenance, logistics delays, and unpredicted or abnormal events.

## POSSIBLE SHORTCOMINGS DURING THE LIFE-CYCLE PHASES

Experience has shown that shortcomings may exist in any of the previous phases, and can be carried over until they are detected in subsequent stages. For instance, a study based on a U.S. Air Force software system<sup>2</sup>, suggests that failures are primarily due to shortcomings in the early life-cycle phases (specification and design) and to poor system



integration. In this particular case, actual failures originating in the implementation phase were responsible for a mere 7% of all failures. Clearly, the exact percentages may vary from one type of system to another, but the fact is that causes for failures may be introduced in any of the phases. To avoid ambiguity, we will refer to the shortcomings in each phase by different names:

- *Flaws*: Shortcomings occurring during the *Specification* phase.
- *Faults*: Shortcomings occurring during the *Design* phase.
- *Defects*: Shortcomings occurring during the *Implementation* phase.
- *Errors*: Shortcomings occurring during the *Operation* phase.

All these shortcomings will be analyzed and illustrated in the following sections. Here, we try to explain their role and relationship to the system life-cycle.

We understand the subtleties in the meaning that these terms may have in different contexts. The terms: "flaws," "faults," and "defects" are frequently used interchangeably but they have different connotations<sup>3</sup>. On the other hand, the use of the term "error," may be less conventional. Here, an "error" refers to any unplanned event or condition, during operation, that may result in a failure, depending on the system "robustness." In that sense, errors may thus be considered "hazardous or unwanted events or conditions." For instance, an operator pressing the wrong key, or opening the wrong valve would be an error using this terminology. Whether or not this particular error will cause a failure is highly dependent upon the system's characteristics, and conditions at the time of the error.

More generally, any of the previous types of shortcomings *may* (but do not necessarily *have to*) cause system failures. Shortcomings originating in one phase, may propagate to the next one, but they may also be detected, and rejected in the next phase. Thus, for instance, a "fault" (i.e., a design shortcoming) does not necessarily translate into a "defect" (i.e., an implementation shortcoming). Also, for instance, "defects" are not necessarily the result of "faults." "Defects" can be caused by purely implementation shortcomings (e.g., poor integration or manufacturing). Table 1 summarizes the different aspects of the system life-cycle including the types of shortcomings in each phase.

Table 1. The cause-effect chains of the system life-cycle

MOTIVATION	Synthesize Requirements	⇒	Define Objectives, Goals, Structure & Functions	⇒	Make it Happen	⇒	Utilize the System
LIFE-CYCLE PHASES	↓		↓		↓		↓
	Specification	⇒	Design	⇒	Implementation	⇒	Operation
	↓ ↑		↓ ↑		↓ ↑		↓ ↑
SHORTCOMINGS	Flaws		Faults		Defects		Errors

## THE LIFE-CYCLE FAILURE SPACE

As mentioned in the introduction, the process of Concurrent Engineering has become pervasive in complex system development efforts. It has become more difficult to set the limits of each life-cycle phase because they tend to be conducted simultaneously. However, this development process of concurrent engineering does not (or should not) eliminate specific responsibilities for the failure or success of each phase. Experience shows that in order to ensure reliability and quality of the process, accountability is a key factor. This section expands the nature and relationship of the different life-cycle shortcomings introduced in the previous section. Figure 1 depicts what can be called the "*Life-Cycle Liability Failure Space*." In this space, any point represents a failure, and its location indicates its cause.

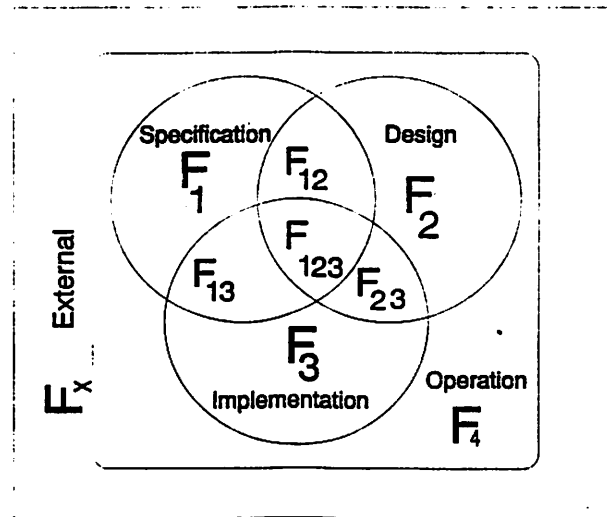


Figure 1. The Life-Cycle Liability Space

As Figure 1 shows, there are several areas which represent the following types of failure root causes:

- $F_1$ : Caused exclusively by the *specification* phase.
- $F_2$ : Caused exclusively by the *design* phase.
- $F_3$ : Caused exclusively by the *implementation* phase.
- $F_4$ : Caused exclusively by the *operation* phase.
- $F_x$ : Caused exclusively by *external factors*.
- $F_{12}$ : Caused by a conjunction of *specification* and *design* phases.
- $F_{13}$ : Caused by a conjunction of *specification* and *implementation*.
- $F_{23}$ : Caused by a conjunction of *design* and *implementation*.
- $F_{123}$ : Caused by *specification*, *design*, and *implementation*.

$F_1$ ,  $F_2$ ,  $F_3$ ,  $F_4$ , and  $F_x$  are called failure primary root-cause because there are the result of a single phase or cause, and not a combination like the other types of failures.

Some of the previous types of root causes are more easily understood than others. For reasons of space, more time will be devoted to the less evident ones. In some instance, real-life examples are also provided to better illustrate the impact of a specific type of shortcoming. The next section describes the "primary" failure root causes, i.e.,  $F_1$ ,  $F_2$ ,  $F_3$ ,  $F_4$ , and  $F_x$ . They are termed "primary," because they are the result of shortcomings that can occur in a single phase (or by single events). This is opposite to other types of failures,

(e.g.,  $F_{12}$ ,  $F_{23}$ , etc . . . ) which are produced by a combination of shortcomings in different phases. While reading the following description of primary root causes, the reader may perhaps think that the description has omitted something. However, the item that he/she may be contemplating is likely to be listed in the section dealing with the non-primary root causes.

## THE PRIMARY FAILURE ROOT CAUSES

### Failures of Type $F_1$

Shortcomings occurring during this phase fall in one of the following categories:

<i>Consistency:</i>	Elements of the specification are in conflict with each other, or with governing requirements and/or constraints.
<i>Correctness:</i>	Specifications are plainly <i>against</i> the user's <i>implicit</i> or <i>explicit</i> expectations (for instance, safety-related expectations, or purely capability-related requirements).
<i>Completeness:</i>	Some of the user's needs that should have been made explicit are completely absent from the specification (they cannot be even inferred from the specifications).
<i>Fictitiousness:</i>	An element in the specifications has been arbitrarily and unnecessarily imposed. In other words, these fictitious specifications are those which cannot be traced back to <i>legitimate</i> explicit or implicit user's requirements.

Raheja<sup>4</sup> relates an interesting real-life incident involving this type of root-causes. An X-ray machine was allowed to generate 80 times the recommended radiation dose. Three patients were killed. However, the manufacturer insisted that the X-ray machine operation did not prevent high radiation doses because the hospital that purchased the machine did not *ask for* it. The case was eventually brought to a court that finally ruled in favor of the hospital. The manufacturer was held liable for not meeting *implied safety expectations*. From the previous classification viewpoint, in this case the specification of an X-ray machine violated the "correctness" criterion because the machine operated *against* user's implied expectations.

### Failures of Type $F_2$

The design phase is one of the most intensive in the system life-cycle. For large and complex systems the design phase demands an exceedingly high level of organization, technical competence, and tones of common sense. Typical shortcomings during this phase are: inadequate redundancy in the design to ensure the desired levels of reliability, poor planing of managerial information systems (including report of failures), deficient data processing systems, miscalculation in structural design, etc. Techniques such as: Fault Trees (FT), Reliability Block Diagraming (RBD), Event Trees (ET), Failure Mode Effect and Criticality Analysis (FMECA), are utilized to assess and identify weaknesses in the design.

### Failures of Type $F_3$

In the implementation phase, in which the design is brought to reality, several engineering-related shortcomings may occur. For instance, a poor integration, use of poor quality parts, manufacturing defects, introduction of "bugs" in software coding, are typical shortcomings during this phase.

## Failures of Type $F_4$

At this stage the system is operating in the field. Many unplanned incidents may put risk the proper and safe operation of the system. Clearly, this type of shortcomings is very dependent upon the kind of system in question. Examples are: corrosion, fatigue, defective interactions among components, perceptual, decisional, and executional human malfunctions.

## Failures of Type $F_x$

These are failure induced by external agents or challenges to the system. Examples of them, are earthquakes, fire, use of equipment within unreasonable ranges outside the specification limits, sabotage, etc. For every system, designers must, of necessity, accept a certain amount of risk, even if it is very low. Eliminating risks costs money, time, and human resources. There are practical limits to the levels of reliability and safety that can be achieved. These limits are dictated by real-life constraints. For instance, an elevator may be designed to withstand a maximum weight of, say, two thousand pounds. Despite possible reasonable safety margins, the designer implicitly accepts the fact that the elevator should not be able to withstand a weight of, say, twelve thousand pounds. In this case, for instance, if the elevator fails due to a completely unreasonable load, a failure of type  $F_x$  has occurred. Therefore, failures of type  $F_x$  may always occur in practice.

## NON-PRIMARY ROOT CAUSES: THE COLOSSUS EFFECT

This is a general discussion referring to failures of type:  $F_{12}$ ,  $F_{23}$ ,  $F_{13}$ , and  $F_{123}$ . In going from one phase to the next, the work of one team may leave room for potential errors. In other words, the first team leaves room for interpretation (justifiable or not), and the next team makes wrong decisions. We called them: "Concessions Of Liberty Of Subdue and Subvert Uncertain Statements" (COLOSSUS).

## Failures of Type $F_{12}$

Failures of type  $F_{12}$ , are caused by the COLOSSUS effect between the specification and design phases. First, it is important to realize that in these cases, the "liability" is shared between the two phases (this is the case, in general, with the COLOSSUS effect). Also, one must realize that none of the following types falls into the classes of purely  $F_1$  or purely  $F_2$  root causes previously described. In the case of  $F_{12}$ , COLOSSUS effects may be triggered by:

- |                       |   |
|-----------------------|---|
| <i>Murkinness:</i>    | Specifications may be formulated in such a way that even if they do not contain errors, they are very difficult to interpret, because they are too complex, or simply because they may even be ambiguous.   |
| <i>Vagueness:</i>     | If certain elements in the specification are too vague, the designing team may interpret it in an incorrect way. For instance, if the specification asks for: "a high level of reliability," the designing team could interpret this "high level" as being, say, 0.99. But, does a reliability of 0.99, really meet the requirements? |
| <i>Lack of Vigor:</i> | Crucial requirements are not given the proper emphasis in their formulation. For instance, a requirement can prescribe that a certain water-pump in the system be diesel-operated.  |

Suppose that this system is going to be used in an environment where no electricity is available. Then, the "diesel-operated" portion of the pump specification becomes crucial. To avoid unwanted assumptions (e.g., use of an electrically-operated water-pump with the same capabilities), the specification must place the right "vigor" in the portion where the requirement asks specifically for a fuel-operated-type.

### Failures of Type $F_{23}$

In this case, the COLOSSUS effect between the phases of design and implementation can be triggered by: murkiness, vagueness, and no vigor: as previously explained, but making the necessary adaptation of terms. In this case, we could also observe a *lack of practicality*, occurring when a given design does not take into consideration practical aspects. This may force the implementing team to take unsafe or unreliable alternatives.

### Failures of Type $F_{13}$

This type can occur when the specification team has direct access to the implementation team (e.g. as in the case of Concurrent Engineering). Then the implementation team may try to get extra specifications directly from the specification team. This may cause COLOSSUS effects similar to the ones producing failures of type  $F_{12}$ .

### Failures of Type $F_{123}$

These failures happen when COLOSSUS effects originate during the specification phase, but remain *latent* during the design phase, and are propagated into the implementation phase. The design team should have detected the COLOSSUS effects and rectify them before they were passed to the next phase.

### Failures Resulting from other Combinations

Finally, combinations of  $F_4$  with any of the previous types are not explicitly shown in Figure 1. This is done for the sake of clarity, to avoid a factorial explosion of the various cases. However, it must be realized that failures of type  $F_4$  can be due to "purely" operational shortcomings (as the ones described in the previous section), but also COLOSSUS effects with previous phases. For instance, in a cooling system an operator may open the wrong valve but this may be caused to unclear or inadequate labeling of the valves in the procedure that he/she follows.

## APPLICATIONS

A generic classification of failure causes has been proposed during the system life-cycle. Apart from contributing to a better understanding and appreciation of failure causes, this classification provides a good starting point for several areas of applications:

- The approach for Root Cause Analysis is hardly unique. However, traditionally, this analysis has been *reactive* in nature. That is, a comprehensive investigation of the causes for failures is conducted only *after* the failure has occurred. A classification like the one proposed in this paper promotes what can be called a: "Predictive" Root Cause Analysis. This

classification may serve as a basis for identifying possible hazards in the system-development cycle. The classification can be utilized to promote: checklist, assumption analysis, COLOSSUS analysis.

- The classification also provides a construct for a more refined statistical counting of system failures. Usually, failures are classified and counted based solely upon the criticality of their effect. This kind of statistical information provides very little use to improve the system. With classifications of the type proposed here, failures can be counted based upon their etiology. This allows a more meaningful feedback for designers and engineers.
- It can also be used to assess current assurance technologies used in a specific project and identify the weak points and the strong points. Based upon the proposed classification, we realize that failure root cause analysis may be more complex than it appears at first sight. Only an effective use of a comprehensive combination of assurance technologies can guarantee that all types of life-cycle shortcomings will be addressed.
- This type of classification could be used as part of what is known as "*forensic engineering*." The expertise of forensic engineers is requested to settle legal disputes among customers, contractors, engineers, designers, and others. One of the main objectives is to determine who is responsible for system failures. Figure 1, which shows the Life-Cycle Liability Failure Space, establishes unambiguous and understandable guidelines to reach that end.

The generic classification of failures developed in this paper is a reminder that failure analysis transcends the operational and physical realms. Behind each tangible system failure, usually stands a lack of planning, calculation, or anticipation. As it has been said: "it is not the 'stuff,' it is the man."

## REFERENCES

1. J. P. van Gigch, "Modeling, metamodeling, and taxonomy of system failures," *IEEE Transaction on Reliability*, R-35:2, pp.131-136, (June 1986).
2. Sheldon et. al., "Reliability measurement: from theory to practice," *IEEE Software*, July, (1992).
3. IEEE Standard Glossary of Software Engineering Terminology, IEEE Std. 729-1983, Los Alamitos, Calif., (1983).
4. D. Raheja, "Assurance Technologies: Principles and Practices," McGraw-Hill Inc., (1991).
5. Barry W. Boehm, "Verifying and Validating Software Requirements and Design Specifications," *IEEE Software*, pp. 75-88, January (1984).
6. Modarres, M. L. Chen, and M. Danner, "A knowledge-based approach to root-cause failure analysis," Proc. of the Expert Systems Applications for the Electric Power Industry Conf., Orlando, FL, June (1989).