LWRS LIGHT WATER REACTOR SUSTAINABILITY

Common Cause Failure Evaluation of High Safety-significant Safety-related Digital Instrumentation and Control Systems

Han Bao, Idaho National Laboratory
Hongbin Zhang, Terrapower
Tate Shorthill, University of Pittsburgh
Edward Chen, North Carolina State University
Svetlana Lawrence, Idaho National Laboratory

The Probabilistic Safety Assessment & Management conference, PSAM 16
Honolulu, Hawaii
06/27/2022

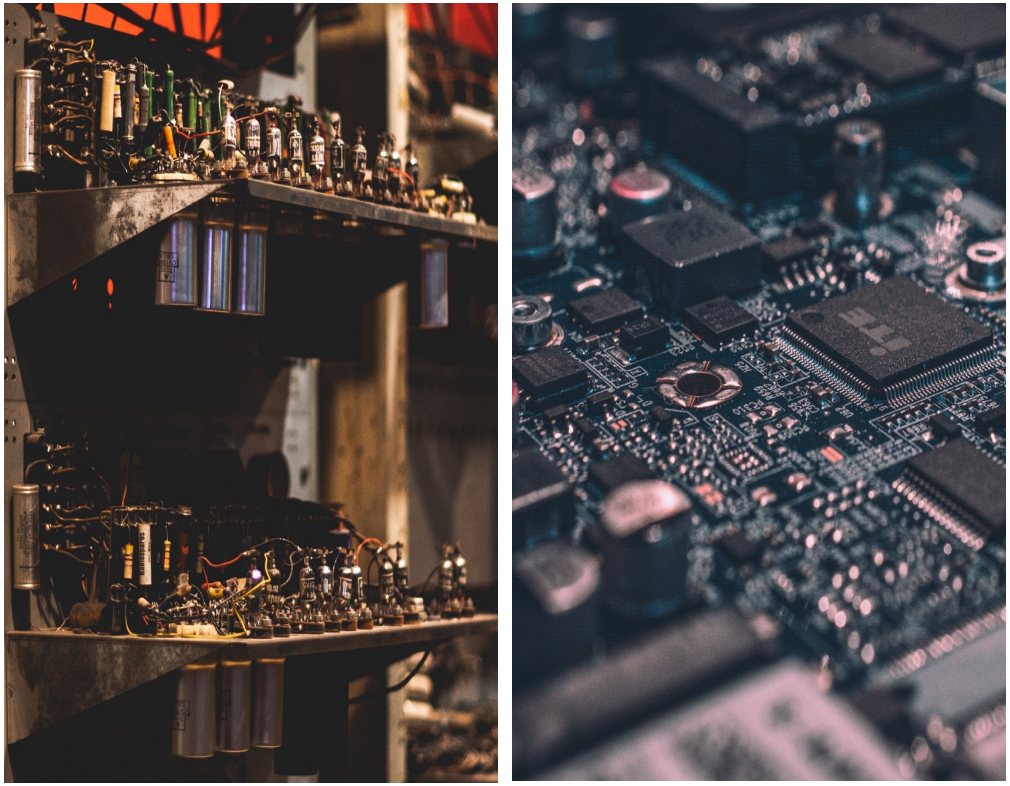
To Support the Transition to Digital Instrumentation and Control (DI&C)

Benefits of DI&C systems:

- Reliable system performance in terms of accuracy and computational capability
- High data-handling and storage capabilities to fully measure and display operating conditions
- …

Technical barriers for the implementation of DI&C systems in nuclear power plants (NPPs):

- The unique characteristics of digital systems
- The potential for software based common cause failures (CCF)
- The time-consuming licensing process for regulatory review and approval for DI&C system designs and upgrades
- A lack of consensus on issues underlying the evaluation and adoption of DI&C technology



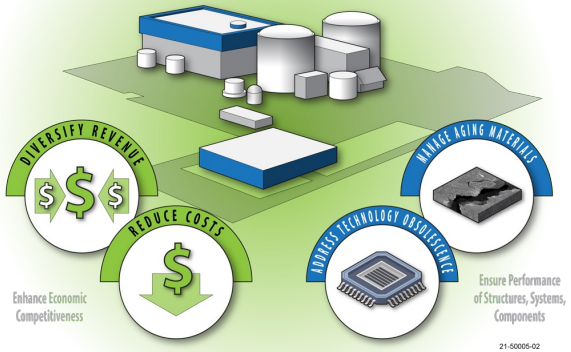
Analog I&C vs. Digital I&C
Images from Unsplash.com

Light Water Reactor Sustainability (LWRS) Program

LWRS Goal

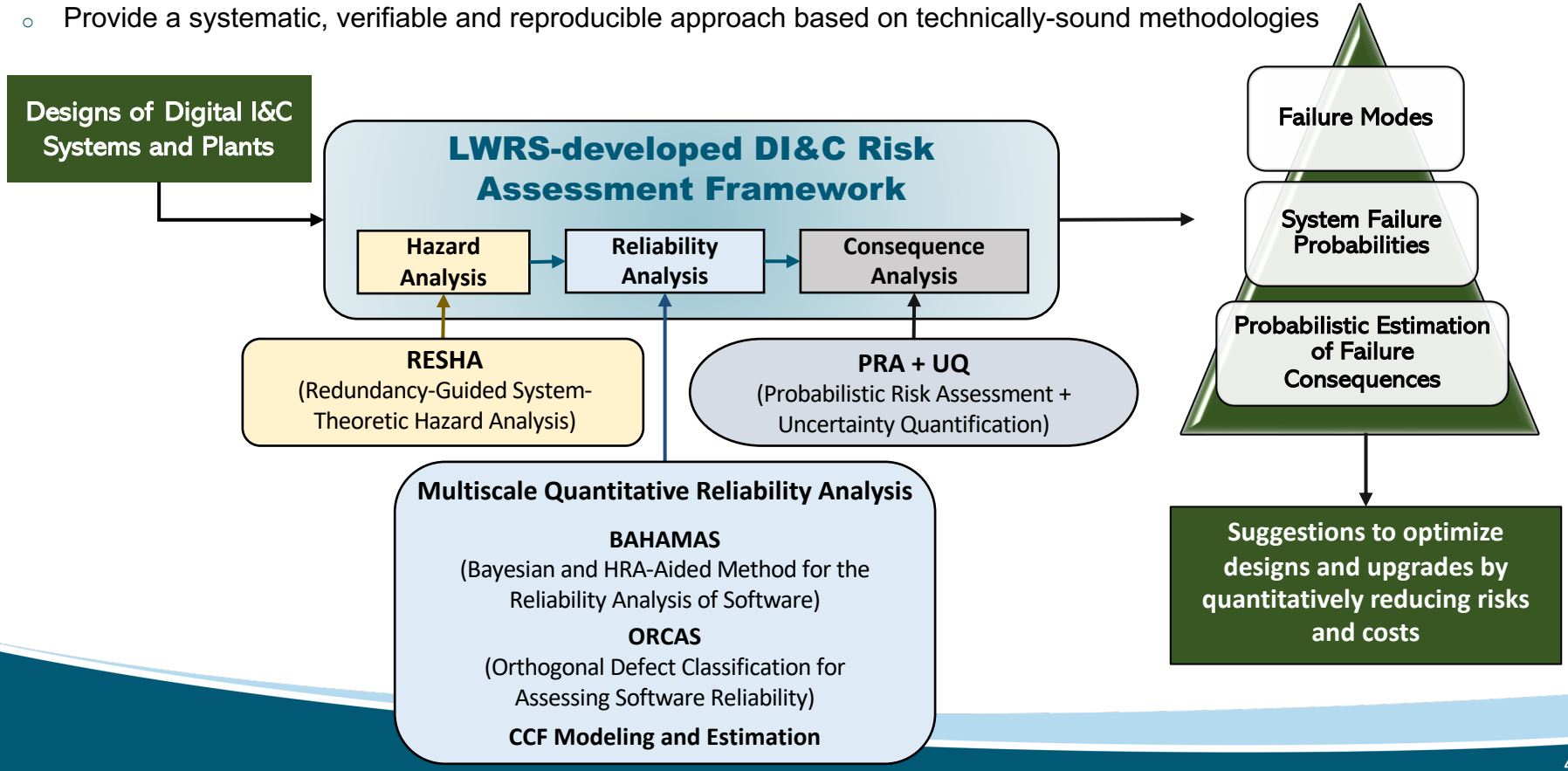
Enhance the safe, efficient, and economical performance of our nation's nuclear fleet and extend the operating lifetimes of this reliable source of electricity

Plant Modernization	Enable plant efficiency improvements through a strategy for long-term modernization
Flexible Plant Operation & Generation	Enable diversification and increase revenue of light water reactors by extracting electrical and thermal energy to produce non-electrical products
Risk Informed Systems Analysis	**Develop risk assessment methods and tools to optimize the safety, reliability, and economics of plants**
Materials Research	Understand and predict long-term behavior of materials in nuclear power plants
Physical Security	Develop technologies and the technical bases to optimize physical security postures



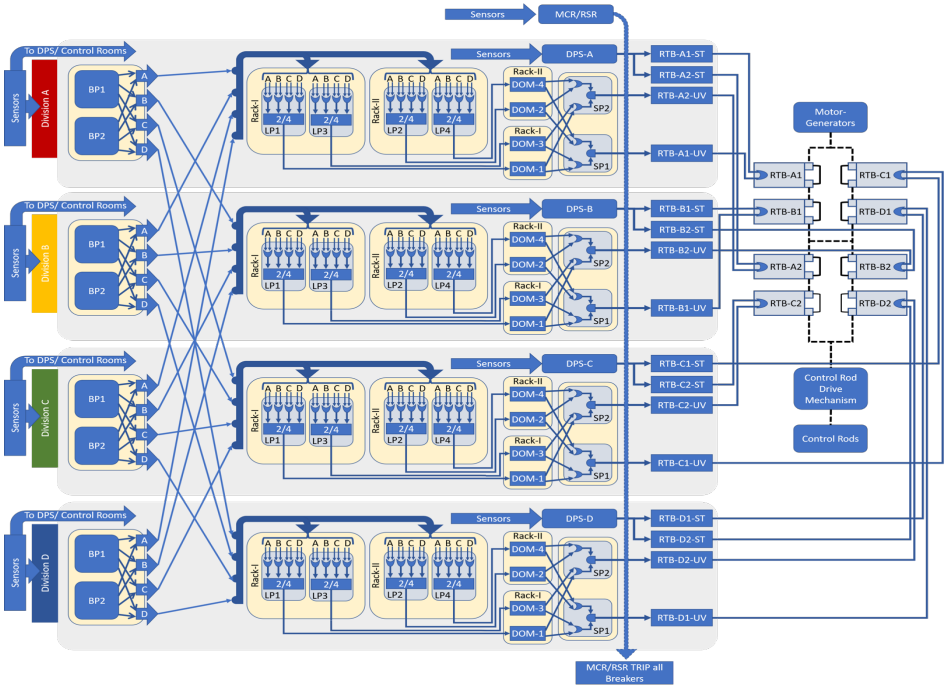
A Risk Assessment Framework for Digital I&C Systems

- **Goals of LWRS-RISA Efforts on Digital I&C (DI&C) Risk Assessment:**
  - Develop an advanced risk assessment framework to support industry's transition from analog to digital technologies for safety-related I&C systems
  - Develop an integrated capability to perform risk-informed and performance-based analysis of various DI&C design architectures.
  - Provide a systematic, verifiable and reproducible approach based on technically-sound methodologies



Value Proposition: Evaluating Various Digital Architectures

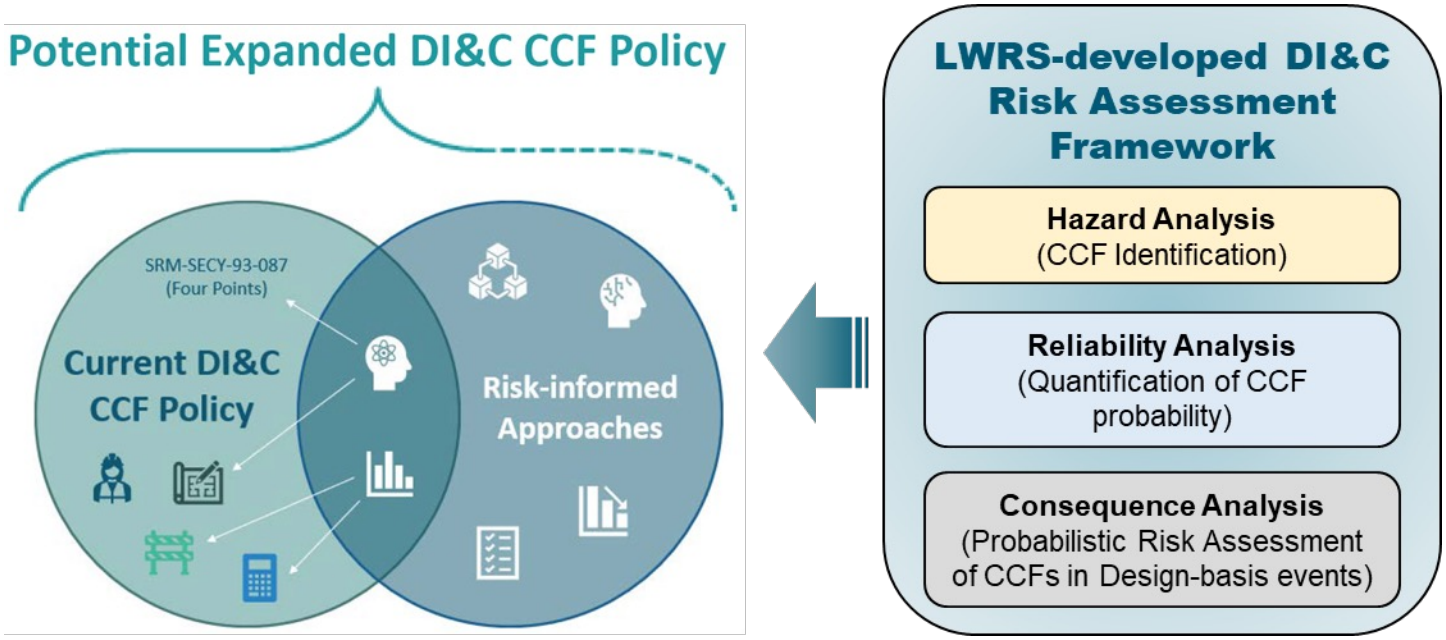
- **The framework** aims to support vendors and utilities with optimization of design solutions from economical perspectives GIVEN the constrain of meeting risk-informed safety requirements.
  - **Quantitative Risk Analysis**
    - Software and Hardware Failure Probabilities → DI&C System Failure Probability → ΔCDF / ΔLERF
  - **Risk-Informed Design**
    - Management strategy of CCFs
      - All elimination vs. selective elimination
    - Level of redundancy
      - 4 divisions vs. 2 divisions
      - 4 vs. 2 local logic processors per division
    - Level of diversity
      - Design: Analog? Digital? A combination of both?
      - Software: Design requirements, programming language, etc.
      - Hardware Equipment: Manufacturers, designs, architectures, etc.



A Four-Division Digital Reactor Trip System

Value Proposition: Addressing CCF Considerations

- **This risk assessment framework** is expected to provide technical bases and risk-informed insights for **addressing CCF considerations** for safety-critical DI&C systems.



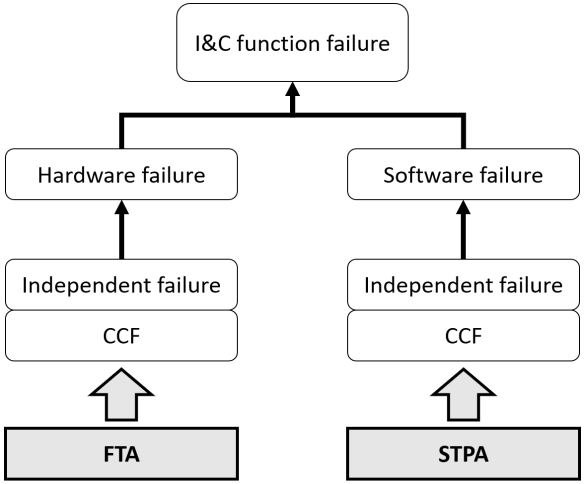
Left: The NRC staff's plan to expand the current NRC policy for addressing CCFs
Right: Risk-informed capabilities developed in the LWRS risk assessment framework.

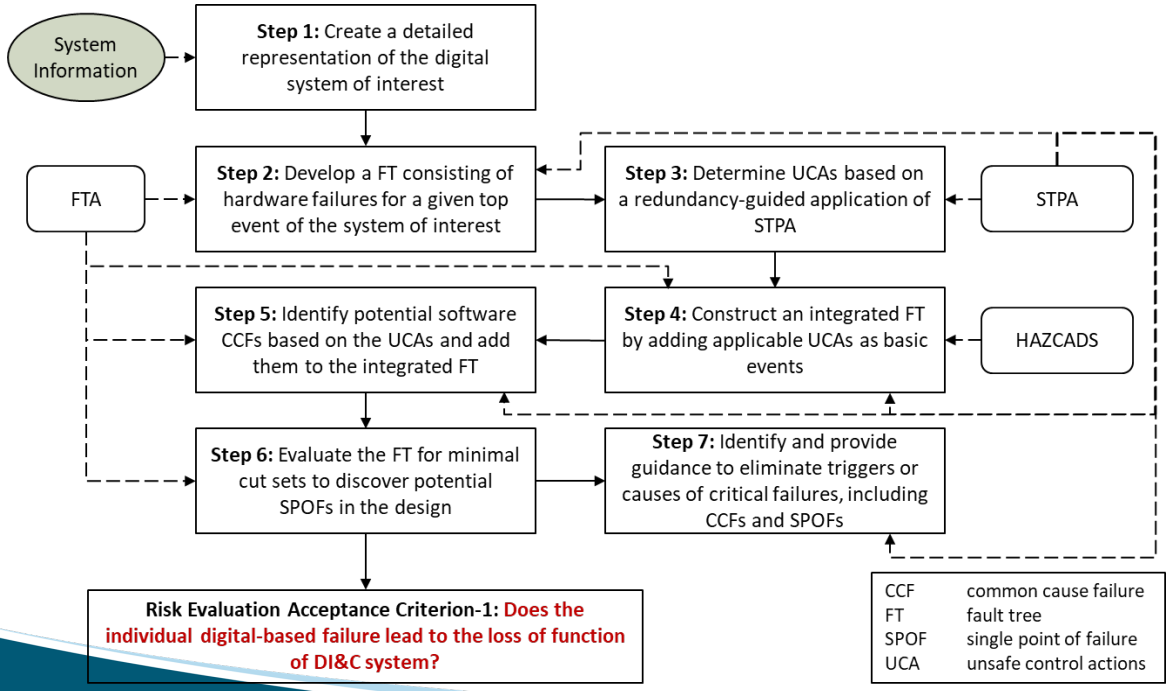
The link for the NRC public meeting: https://www.nrc.gov/pmns/mtg?do=details&Code=20220075.

(I). Redundancy-guided System-theoretic Hazard Analysis (RESHA)

Hazard analysis in RESHA:

- Incorporates the concept of combining FTA, STPA and HAZCADS.
- Reframes STPA in a redundancy-guided way to address CCF concerns in highly redundant DI&C systems.
- Identifies failures in Type II interactions (between different components of a DI&C system).



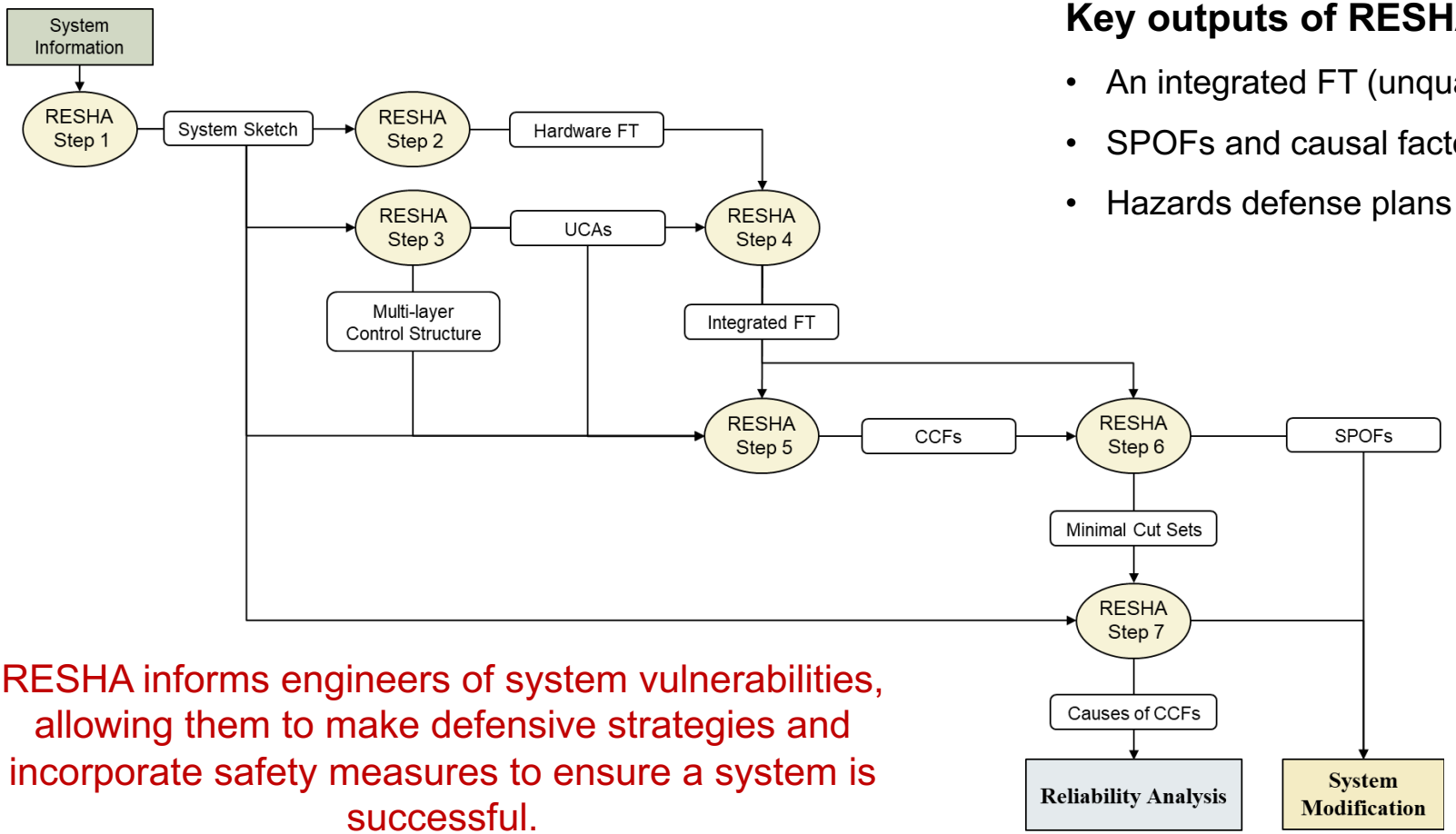


Workflow of the Redundant-guided System-theoretic Hazard Analysis (RESHA)

A presentation by Edward Chen:

- Session M21: Digital I&C
- Monday, 15:30-17:00
- "Failure Mechanism Traceability and Application in Human System Interface of Nuclear Power Plants using RESHA"

RESHA Information Flow

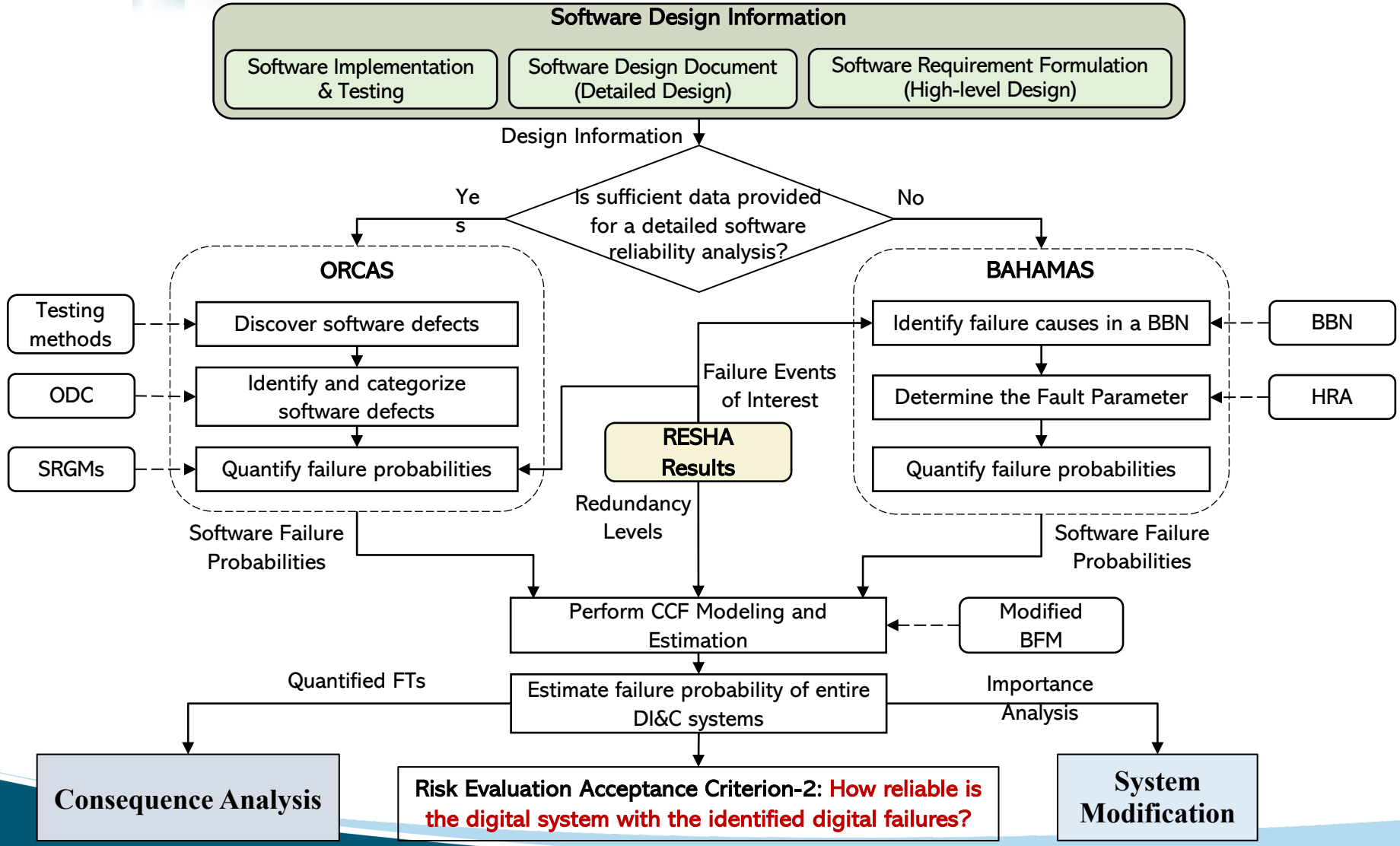


Key outputs of RESHA:

- An integrated FT (unquantified)
- SPOFs and causal factors
- Hazards defense plans

RESHA informs engineers of system vulnerabilities, allowing them to make defensive strategies and incorporate safety measures to ensure a system is successful.

(II). Multiscale Quantitative Reliability Analysis



Quantitative Software Reliability Analysis

- **Two methods developed in this project:**
  - **BAHAMAS (**Bayesian and HRA-Aided Method for the Reliability Analysis of Software)
    - Developed for the conditions with limited testing/operational data or for reliability estimations of software in early development stage.
    - Provide a rough estimation of failure probabilities to support the design of software and target DI&C systems.
  - **ORCAS** (Orthogonal Defect Classification for Assessing Software Reliability)
    - Developed for the conditions with sufficient testing/operational data.
    - A relatively accurate estimation of software failure probabilities can be provided.

	BAHAMAS	ORCAS
Applicable conditions	• Limited testing/operational data • For reliability estimations of software in early development stage	• Sufficient testing/operational data • For reliability estimations of software in development or testing stage
Key assumption	Software failures can be traced to human errors in the software development life cycle	Sufficient data is available through testing (e.g., T-Way testing)
Ways to identify root causes	STPA + BBN + HRA in SDLC	STPA + ODC + Metric-based methods
Ways to quantify failure rates of root causes	HRA in SDLC	Software reliability growth modeling

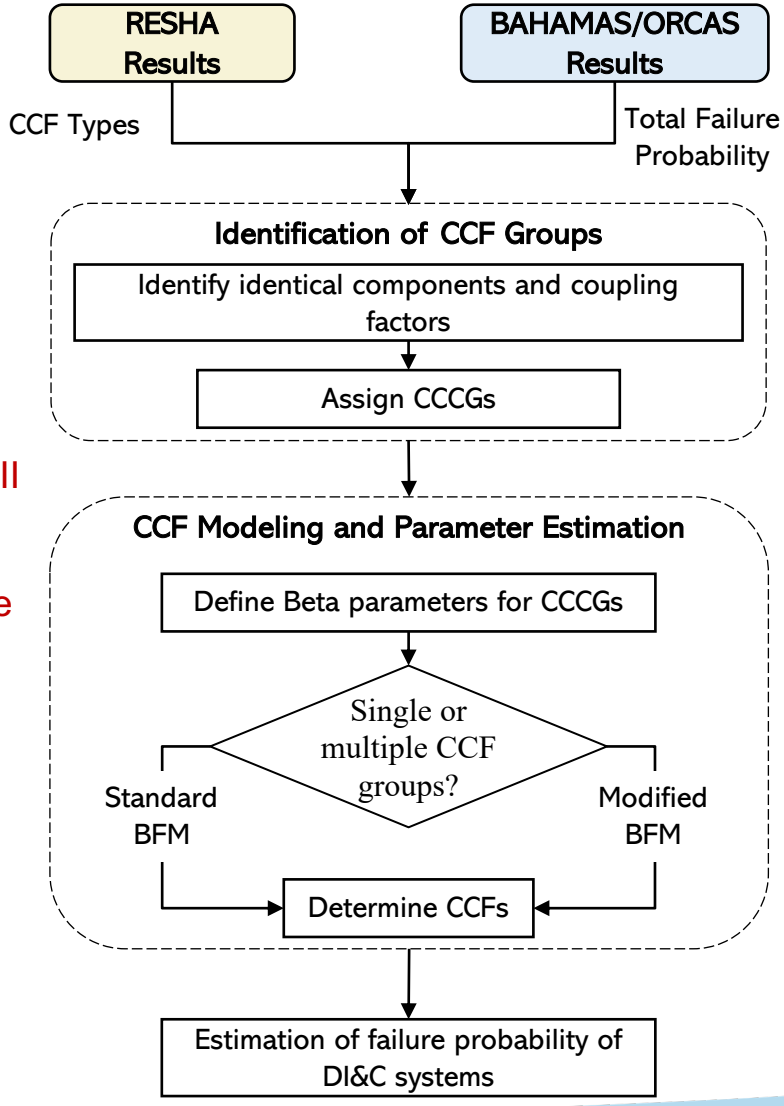
A presentation will be given by Edward Chen:
- Session Th05: Modernization Through Risk-Management
- Thursday, 10:30-12:00
- "Application of Orthogonal-Defect Classification for Software Reliability Analysis"

BNN	Bayesian Belief Network
ODC	Orthogonal Defect Classification
HRA	Human Reliability Analysis
SDLC	software development life cycle

CCF Modeling and Estimation

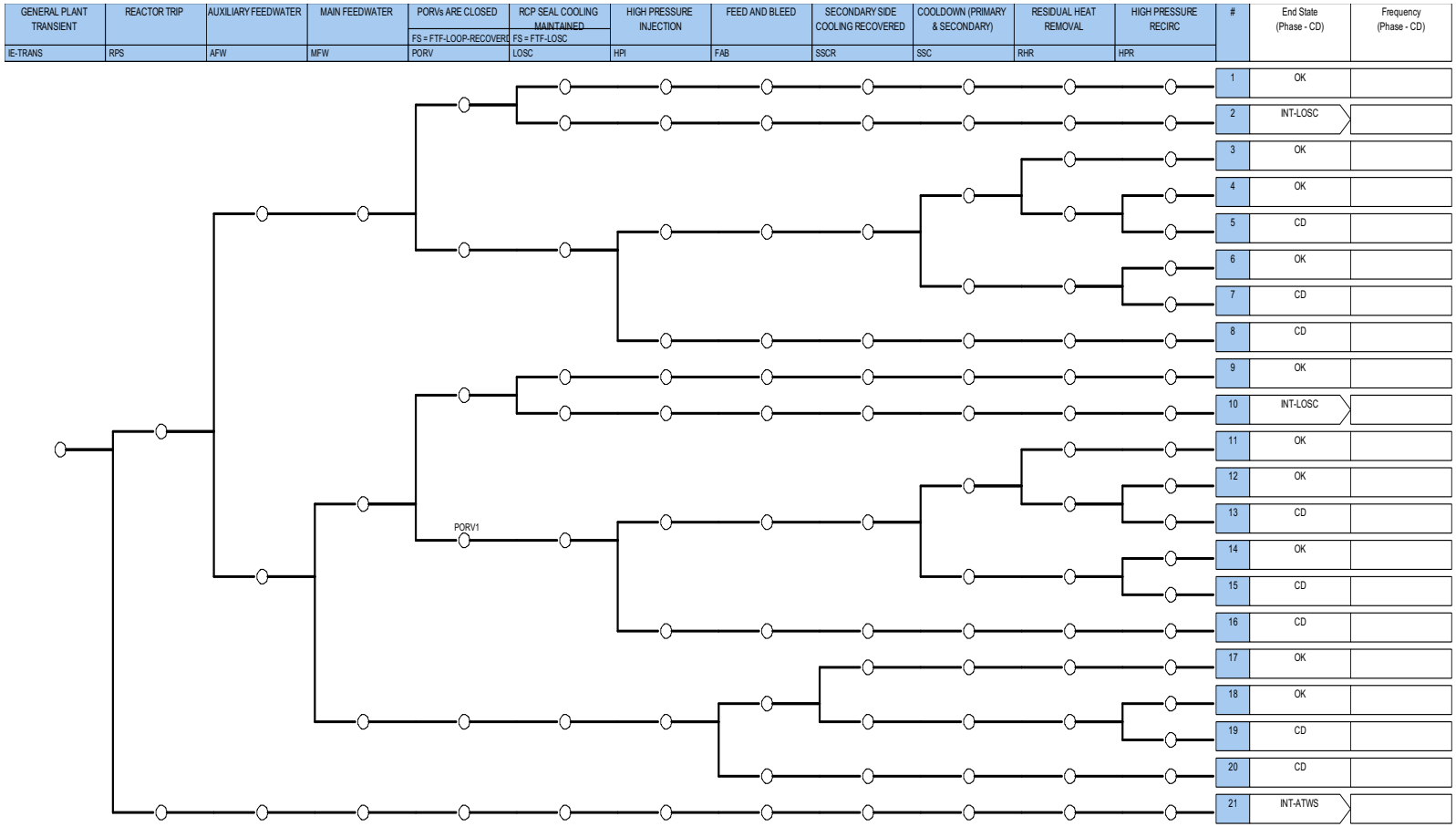
- A CCF modeling approach is developed for software CCF modeling and estimation based on a modified Beta-factor method (BFM) and a Partial Beta-factor approach (PBF).

- A presentation will be given by Tate Shorthill:
  - Session Th22: Safety Assessment Software and Tools III
  - Thursday, 15:30-17:00
  - "An Application of a Modified Beta Factor Method for the Analysis of Software Common Cause Failures"



(III). Consequence Analysis

- Consequence analysis can be performed **by calculating CDF after considering integrated FTs of digital I&C systems** to the original event tree models.



A General PWR Transient Event Tree

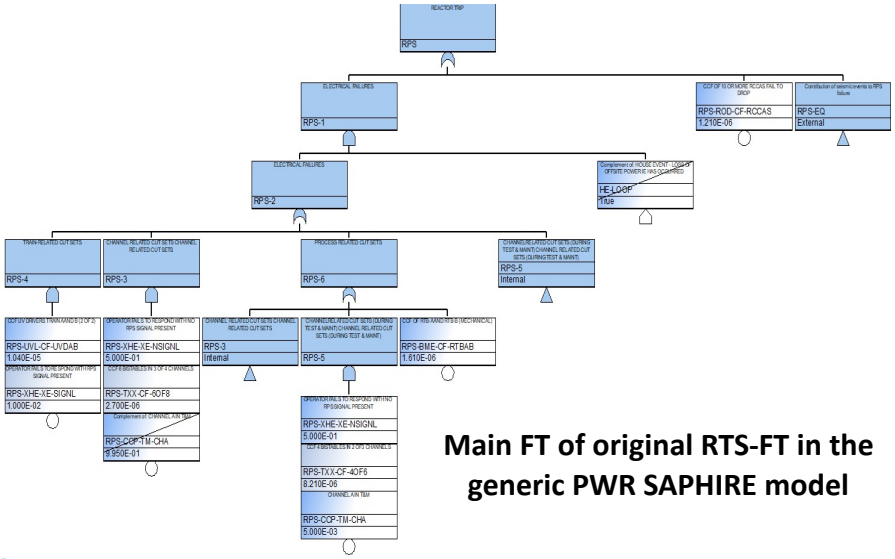
Original and New Fault Trees for Reactor Trip System

Cut sets for the original RTS-FT

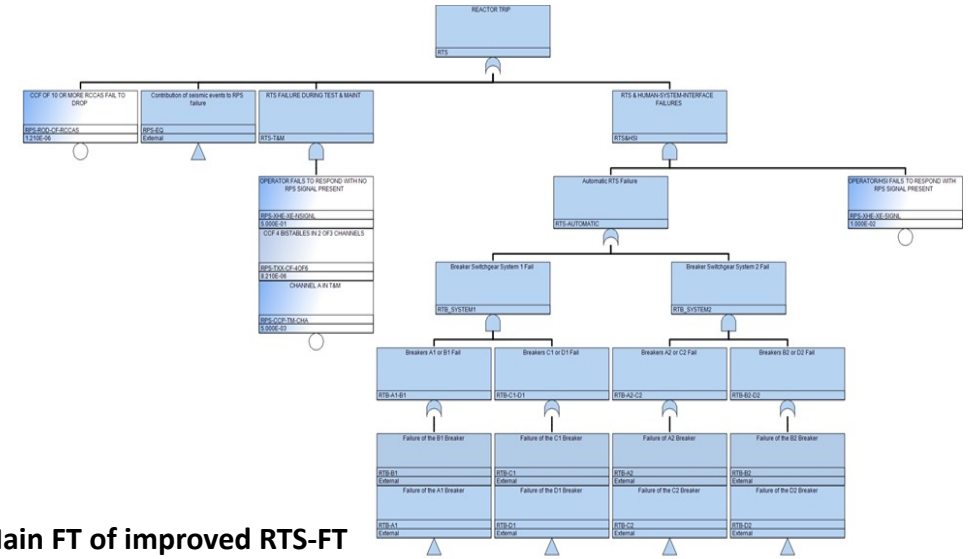
#	Prob.	Total %	Cut Sets
1	1.610E-6	37.55	RPS-BME-CF-RTBAB
2	1.343E-6	31.33	RPS-CCP-TM-CHA, RPS-TXX-CF-6OF8, RPS-XHE-XE-NSIGNL
3	1.210E-6	28.22	RPS-ROD-CF-RCCAS
4	1.040E-7	2.43	RPS-UVL-CF-UVDAB, RPS-XHE-XE-SIGNL
5	2.052E-8	0.48	RPS-CCP-TM-CHA, RPS-TXX-CF-4OF6, RPS-XHE-XE-NSIGNL
Total	4.288E-6	100	-

Cut sets for the new RTS-FT

#	Prob.	Total %	Cut Sets
1	1.210E-6	95.25	RPS-ROD-CF-RCCAS
2	2.052E-8	1.62	RPS-CCP-TM-CHA, RPS-TXX-CF-4OF6, RPS-XHE-XE-NSIGNL
3	1.976E-8	1.56	RPS-XHE-XE-SIGNL, RTB-SYS-2-HD-CCF
4	1.976E-8	1.56	RPS-XHE-XE-SIGNL, RTB-SYS-1-HD-CCF
Total	1.270E-6	100	-



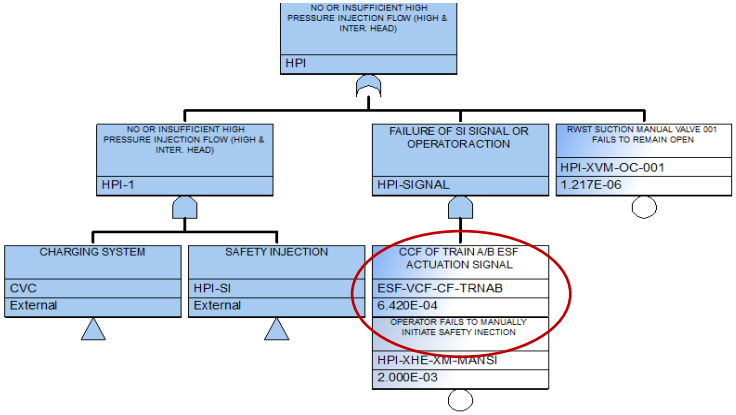
Main FT of original RTS-FT in the generic PWR SAPHIRE model



Main FT of improved RTS-FT

Original and New Fault Trees for ESFAS

- In the original generic PWR SAPHIRE model, ESFAS failure is presented using a CCF of the ESF actuation signals in both Train A and B (a 2-division ESFAS).
- Compared with the original ESFAS-FT, the new ESFAS-FT has:
  - A complicated logic to match the 4-division digital ESFAS structure.
  - A significantly reduced failure probability.
- **Software CCFs in the new ESFAS-FT do not significantly affect the reliability of digital ESFAS** because of the high-redundant design and high reliability of PLC-based digital components.
- All the **failure probabilities of these safety features have been reduced** due to the decrease of ESFAS failure probability.



Main FT of HPI failure in the generic PWR SAPHIRE model where CCF of analog ESFAS is considered.

Cut sets for the new ESFAS-FT

FT Name	Prob.	# of Cut Sets
New ESFAS-FT	2.600E-5	13
Original ESFAS-FT	6.420E-4	1

Comparison of the top events with original ESFAS-CCF basic event and improved ESFAS-FT

Top Event	Probability		# of Cut Sets	
	Original	New	Original	New
Failure of AFW	1.487E-5	1.240E-5	1539	1551
Failure of AFW-ATWS	2.367E-4	2.343E-4	906	918
Failure of HPI	1.104E-5	9.803E-6	1163	1172
Failure of LPI	8.416E-4	2.258E-4	1567	1579

Comparing CDFs of Different I&C System Architectures

- By adding the integrated FTs of the 4-division digital RTS and ESFAS into the PRA models, the safety margin increased by the digitalization of safety-critical I&C systems are quantitatively estimated.
  - RTS failure probability is half-reduced from 4.288E-6 to 1.270E-6.
  - LPI (low-pressure injection) failure probability greatly decreases from 8.416E-4 to 2.258E-4 due to the improvement of ESFAS fault tree.
- Results show the CDFs have been greatly reduced by introducing highly redundant safety-critical digital I&C systems.
- The proposed framework has the capability for the risk evaluation of various I&C design architectures by estimating respective system reliability and plant safety.

Event Trees	Original CDF	New CDF	Δ CDF	Δ CDF/ Original CDF
INT-TRANS	1.073E-6	5.795E-7	- 4.935E-7	- 46.2%
INT-SLOCA	7.784E-8	7.509E-8	- 2.720E-9	- 3.53%
INT-MLOCA	6.279E-7	4.984E-7	- 1.247E-7	- 20.6%

Conclusions and Future Work

To deal with the technical issues in addressing potential software CCF of safety-critical DI&C systems of NPPs, **the LWRS-developed framework** provides:

- A common and modularized platform for I&C designers, software developers, plant engineers, and risk analysts to efficiently prevent and mitigate risk by identifying crucial failure modes and system vulnerabilities, quantifying DI&C system reliability, and evaluating the consequences of digital failures on plant responses.
- A technical basis and risk-informed insights to assist the NRC and industry in formalizing relevant licensing processes relevant to CCF issues in safety-critical DI&C systems.
- An integrated risk-informed tool for vendors and utilities to meet the regulatory requirements and optimize the D3 applications in the early design stage of safety-critical DI&C systems.

Future work:

- Improve current framework and complete demonstration cases on the evaluation of various safety-critical DI&C design architectures in terms of safety assurance and economic efficiencies.

Sustaining National Nuclear Assets

http://lwrs.inl.gov