Relko Experience with Reliability Analyses of Safety Digital I&C

Jana Macsadiova[a*], Vladimir Sopira[a], Pavol Hlavac[a]
[a] RELKO Ltd., Bratislava, Slovak Republic

Abstract: The using of digital technologies is increasing in the operation of NPPs. Not only the new plants, but also the current generation of plants uses them due to upgrades of existing analog systems. It is regulatory requirement that the reliability is justified on objective basis. The objective of the digital system risk research is to identify and develop methods, tools and guidance for modeling reliability of digitals systems. The scope of this research is focused mainly on HW failures and limited reviews of SW failures and SW reliability methods. Due to many unique attributes of digital systems, a number of modeling and data collection challenges exist and there is no consensus on how the reliability models should be developed. The paper presents the methodology and overview of reactor protection system reliability analysis for safety digital instrumentation and control (I&C) in NPP. The digital I&C (RPS and ESFAS) play an essential role in the safe operation of nuclear power plants. The RPS forms part of the safety system that, for the purpose of ensuring reactor safety, monitors and processes the important process variables in order to prevent unacceptable conditions and maintain the conditions of reactor within safe limit. The RPS is usually divided into two parts: RTS – Reactor Trip System and ESFAS – Engineered Safety Actuation System. The RTS is designed to cause automatic interruption or slow-down of fission reaction on the detection of a number of accident situations. This is achieved by switching off the power supplies of the control rod driving mechanisms. The ESFAS is designed to cause automatic activation of different safety systems, e.g., to shut down the reactor, to inject water into the primary and/or secondary circuit in emergency conditions and prevent the radioactive release outside confinement during LOCA or transient. The paper also presents the detailed description of analyzed I&C system and the software of the system TELEPERM XS, which provides the digitalization, processing and evaluation. RELKO is working in this field since 1996 and was involved in reliability analyses of safety digital I&C systems, for NPPs in Slovakia, Hungary, Sweden, Germany and Finland. The results of reliability analyses have shown us that properly designed safety I&C systems can be very reliable from the dangerous failure (failure on demand) point of view. The frequency of spurious actuation is also very low. The main concern of this paper is to present the methodology of digital reactor protection system reliability analysis used in RELKO Ltd.

Keywords: Digital I&C, reactor protection reliability analysis, RPS - RTS, ESFAS.

1. INTRODUCTION

The Reactor Protection System (RPS) plays essential role in the safe operation of nuclear power plants. The RPS forms part of the safety system that, for the purpose of ensuring reactor safety, monitors and processes the important process variables in order to prevent unacceptable conditions and maintain the conditions of reactor within safe limit. The RPS is usually divided into two parts: RTS – Reactor Trip System and ESFAS – Engineered Safety Actuation System.

The RTS is designed to cause automatic interruption or slow-down of fission reaction on the detection of a number of accident situations. This is achieved by switching off the power supplies of the control rod driving mechanisms (CRDMs). At power operation the control rod groups are raised. The CRDM clutches are held onto the threads of the control rods by the continued energizing of electro-magnets (each control rod has its own electro-magnet). The RPS is in a state whereby the electromagnets are all energized, and plant conditions are being monitored. The activation of Reactor Protection simultaneously removes the supplies energizing the electro-magnets of all the rod groups. This has the effect of letting all the groups to fall together, by gravity, into the reactor core.

[*] macsadiova@relko.sk

The ESFAS is designed to cause automatic activation of different safety systems, e.g., to shut down the reactor, to inject water into the primary and/or secondary circuit in emergency conditions and prevent the radioactive release outside confinement during LOCA or transient.

The upgrades of safety-related protection systems at operating NPPs and use of digital I&C systems in new nuclear power plants, it becomes very important to develop reliability methods for quantifying digital instrumentation and control systems. Due to many unique attributes of digital systems, a number of modeling and data collection challenges exist and there is no consensus on how the reliability models should be developed.

During reconstruction of J. Bohunice V1 and V2 NPP the relay based RPS was replaced by new programmable electronic system. The new RPS was designed and constructed by Siemens and AREVA on the basis of TELEPERM XS. The use of a programmable safety I&C system implemented with TELEPERM XS allows improved design of the reactor trip system, emergency core cooling system, emergency diesel actuation and reactor power limitation measures. The design of the I&C system structure, the use of quality products providing high availability, consistent application of qualified and proven equipment, featuring of self-reporting of faults in combination with periodic testing of all components – all this results in increased reliability.

Similar TELEPERM XS systems have been successfully implemented in the instrumentation and control systems of nuclear power plants worldwide. Currently about 2660 TELEPERM XS processor modules are installed in 74 units of nuclear power plants (43 NPPs in 16 countries), which have already a cumulated operating time of more than 214 million hours [1].

RELKO performed reliability analyses of safety digital I&C systems (TXS 1st and 2nd generation, TXP, Iskamatic B, Teleperm C, EDM, Yokogawa-ProSafe-RS). For our customers (SIEMENS, FRAMATOM ANP, AREVA, ProCS) we prepared reliability analyses and calculated system unavailability and frequency of spurious actuation of RPS for NPPs in Slovakia, Hungary, Sweden, Germany and Finland.

The main concern of this paper is to present the methodology of digital reactor protection system reliability analysis performed in RELKO Ltd.

2. OVERVIEW OF RELIABILITY ANALYSES

The reliability analyses are usually divided into several sections described below.

2.1 Description of the system

This section contains detailed description of analyzed I&C system (e.g. RPS, RTS, ESFAS, RLS, DG etc.). The reactor protection system involves the reactor trip system and the engineered safeguard features actuation system (ESFAS), inclusive of emergency power supply. The control rod interlock function and reactor power limitation system are also included within the safety related systems. The reactor protection system and the limitation functions are implemented by means of the same equipment. This equipment comprises programmable instrumentation and controls provided extensively with functions for self-reporting of faults on a processor basis and at the control level. The simplified structure of the digital safety I&C train is shown in Fig. 1.

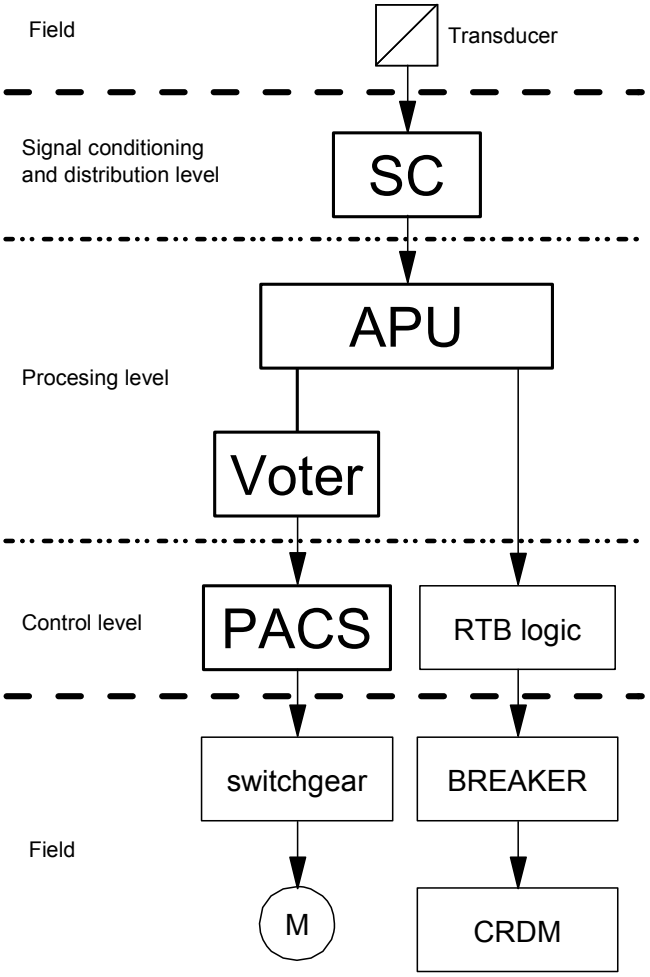

Figure 1: The Typical Simplified Digital Safety I&C Train Structure

The system consists of 2, 3 or 4 physically separated redundancies, which are in principle identical. Initiation signal of one redundancy can trip the reactor independently of the other. Each redundancy can be built in two or three trains structure. Each train comprises:

- Initiation level (measuring channels and sensor signal processing)
- Data acquisition and processing level
- Actuation signal level (e.g., modules for CRDM actuation, ESFAS component actuation switchgears, etc.)

The measuring channels monitor the process variables in each redundancy. Initiation criteria for the formation of actuation signals are acquired via analogue initiation channels and converted to electrical parameters. This permits continuous checking by cross-comparison. The system TELEPERM XS provides the digitalization, processing and evaluation. The limit values are evaluated logically and gated to actuation signals, stored and, in certain cases delayed. The formation of limit signal is performed in the processing computers by majority voting (e.g., 2 out of 3, 2 out of 4 or 2 out of 6). There are three or four initiation signals of the same type for every initiation criterion. The data acquisition computers and processing computers communicate with each other via communication processors. For the system-internal data transmission between different trains the fibre-optic cables are used, which allow galvanic isolation and immunity to electronic interference between trains of a redundancy.

In order to decrease the influence of possible software and hardware common cause failure the CPUs are not synchronized and processing of measured parameters for RPS is realized in two independent diversities. Different software is running in the CPUs of each diversity. For the initiation of reactor trip

diverse initiation variables are used for each design basis accident and diverse initiation functions are performed by independent equipment.

The computers exchange information signals with conventional equipment via binary input and output modules. The output signals of the processing computers are gated in the downstream direction that the failure cannot interfere neither plant operation nor block the safety function. Every redundancy is usually of three-train design, so that three output signals are available in each redundancy. The output signals from three processing computers undergo majority voting (in the relay based actuation section).

The test arrangements of the system permit periodic on-line and/or off-line tests to be performed at the frequency needed to verify that system reliability goals are met. The reactor protection system is structured such that faults are largely self-reporting which is mainly performed by comparison of measured data and signals in the computers. In digital processing self-reporting of failures is achieved using test software and repeatedly running test programs in the acquisition and processing computers. Self-monitoring is implemented as a continuous test in the processor modules. It is executed on all processor modules, and cyclically checks the correct functioning of hardware components. The basic aim of self-monitoring is to achieve a maximum detection rate for hidden hardware faults. Typical tests are parity, memory, CPU tests and bus monitoring. In order to keep the probability of passive faults of actuation section low, periodic testing checks the function of this equipment.

The system description section contains always a detailed description of the analyzed digital I&C equipment and modules (e.g., Analog signal modules, Signal multipliers, Overvoltage protection modules, Fusing modules, Digital and analog input modules, Digital and analog output modules, Processor units, Communication modules and processors, Priority actuation modules, etc.).

2.2 The software

The software of the TELEPERM XS system is divided into:

- Off-line software for engineering, verification, configuration, testing and maintenance. This software is running on the service unit respectively the computer networks for system monitoring independent of plant operation and do not contribute to the execution of I&C functions.
- On-line software which is executed on the function processors of the system and directly realizes I&C function, communication and online self-monitoring during plant operation. The on-line software is subdivided in application software, runtime system and operating system software.

The application software, i.e. the part of the on-line software is realizing the engineered functionality, consists of: Function block modules (the pre-programmed and qualified basic components of the software in the automation path). The modules execute elementary I&C functions (for example the logical functions AND, OR, 2 out of 4, etc) and Function diagram modules and function diagram group modules.

On these levels the function block modules are interconnected to I&C function diagrams. Exactly one software module is generated for every function diagram (function diagram module). It contains the calls of the function block modules of all function blocks used on the function diagram in an algorithmically correct sequence. The function diagram module ensures the correct parameterization of the function block modules and realizes their interconnection.

All function diagram modules which run during the same cycle time on a single function processor are connected to a function diagram group module that implements the correct call sequence of the function diagram modules and the interchange of signals among function diagrams. On function processor these function diagram modules are called by the runtime environment. The runtime

environment is part of the runtime system. It reads and checks all input information and controls the execution of the function diagram modules, communication and the output of the computed results (output signals) to the downstream function processors or via input / output modules. The runtime environment of each function processor is configured by a code generator according to the information in the project data base.

The remaining processing time of each cycle is used for the execution of the cyclic self-monitoring. The cyclic self-monitoring is a software program with the task of locating faults in the I&C hardware. Detected faults are signaled and appropriate reactions are executed by the runtime environment or in same cases with the aid of special programs. For this purpose the cyclic self-monitoring has interfaces to the runtime environment and the exception handler. The tasks of the exception handler are the treatment and display of exceptional states and if necessary a controlled restart or permanent stop of the function processors with a reset of the input / output modules to a defined state.

All engineering work involved in the engineering and operation of TELEPERM XS systems is performed with the aid of SPACE. A function diagram editor, code generators as well as verification and validation tools are integrated in SPACE. Engineering, software generation and the verification and validation process are thoroughly formalized and automated. This means that all plant-specific data on hardware and software is specified on function and hardware diagrams in graphic form with the aid of the engineering system and is stored in a central data base. On the basis of this data entire plant-specific software code is generated by means of automatic generators. This engineering data is also the basis for the complete documentation on functions and location.

The creation of function diagrams with the SPACE editor and the related tools for consistency check ensure that the specification is free of errors.

An important part of system description section in the reliability analysis report are the descriptions of Interaction with other systems, Electrical power supply, Human interactions and Operation, testing and maintenance.

2.3 Failure models and data

The section includes a detail description of failure modes and effects of all modules included in the reliability analyses. The possible failures of modules are usually divided into different failure modes. Important characteristics of failures of I&C modules are: failure detection and failure effect on system function. Following failure modes and failure effects are usually recognized:

- Active failures – change of logical signal at the output of the module without change at the input (indicated at the module itself or indicated by external module). These failures can cause both unavailability or spurious actuation of affected system train.
- Passive failures – no change of logical signal at the output of the module with changing of signals at the input (indicated at the module itself, indicated by external module or failure detection is possible at periodical tests). Passive failures cannot cause spurious actuation but they can cause failure on demand
- Passive failures without influence of module function in case of demand (typically non-functional failures).

The modules failure modes and reliability data are usually prepared by manufacturer. They are analyzed from point of view of failure mode and failure effect. Two types of reliability data are used: module specific statistical data (early studies) and theoretical data compiled from detail module analysis (module components, statistical evaluation, effect of operational temperature or other conditions, etc.). The report provides an overview of the failure modes of the electronic modules of the system platform, including the overall failure rate of the module, and estimated rates for the indicated failure modes. The report also includes an assessment if the failure modes are self-announcing (i.e. detected by module-specific or engineered self-monitoring features), or not self announcing. For a

significant part of modules, the information relies on the results of detailed failure mode and effect analyses. For the remaining modules, failure modes and related failure rates are provided based on engineering assumptions. These assumptions are documented in the report. The failure rates are usually determined for the environmental temperature of T = 40°C (air inlet temperature at the subrack). This is a conservative approach because the failure rate decreases for lower temperature. The failure rates are provided on the basis of the "parts stress" calculations which have been performed for the modules in the framework of the qualification procedure.

The system TELEPERM XS enables to identify immediately large part of possible failures of its components. Therefore, the failure rates of these components are divided into detected and undetected failure modes. Hardware failures are detected and signaled spontaneously by the self-monitoring, which also operates cyclically, and by mutual monitoring of computers redundant to each other. The fault tolerance features implemented in the system software ensure that the effects of a fault are always limited to the smallest possible area.

For each module are evaluated total and channel specific failure rates. Typical module failures effects: Wrong signal, Signal frozen, Signal out of range, Function termination, blocking of communication, non-functional failures, etc. Each failure effect is than evaluated for:

- possibility to cause or to participate in the analyzed system failure (for example, passive failures cannot cause spurious actuation, active failures causing spurious actuation are usually detected)
- possibility to detect/identify module failure and repair/replace the module during operation
- addressed the repair time (MTTR), test interval.

The specific characteristic of computer based I&C is active status processing. It means, the function blocks for signal voting logic (e.g., 2 out of 4, 2.Min/2.Max) are designed in a way that processing results in the following: signals that have been marked error status as being false lead to different output results – voting can be automatically changed by the computer. The consequences of this processing are shown in the Table 1. In order to remove some impossible failure combinations (mainly of detected and undetected failures), standard fault tree modeling must be changed. For example, standard 2 v 4 gate has to be replaced with "AND" and "OR" gates with different inputs (combinations of detected and undetected failures).

Table 1 Possible Failures of 2/4 Function Block with Active Status Processing

Status of input signals			Status dependant voting	Status in the fault tree model	Comment
Undetected failure	Intact	Detected failure			
-	3	-	2 v 3	Intact	
-	2	1	1 v 2	Intact	
-	1	2	1 v 1	Intact	
-	-	3	Detected failure	AND gate, 3 detected input failures (alarm in MCR)	1 MCS of 3rd order No automatic actuation. Manual actuation is not considered in the FT model
1	2	-	2 v 3	Intact	
1	1	1	1 v 2	Intact	
1	-	2	1 v 1	3 AND gates, combinations of 2 detected and 1 undetected input failures	3 MCS of 3rd order
2	1	-	2 v 3	Gate 2 out of 3 undetected input failures	3 MCS of 2nd order
2	-	1	1 v 2	Gate 2 out of 3 undetected input failures	Covered by gate above
3	-	-	2 v 3	Gate 2 out of 3 undetected input failures	Covered by gate above

2.3.1 Software failures

The impact of software failures on a system break down is minimized in the digital I&C system because the development of the software is executed by the aid of a qualified tool and the design procedure is subjected to quality assurance and V&V. The probability of software faults is further reduced by other features such as cyclical program execution, as well as the extensive tests which the system is subjected to in the factory acceptance test. The independent software failure probability q = 1.0E-4 is applied for the reliability model (undetected failure of software installed in a single computer).

2.3.2 Consideration of Common Cause failures

CCFs are multiple failures attributable to a common cause. CCFs regarding their mechanism can lead to failure of several or all components of the same type and structure. To minimize or eliminate the effect to the system function special measures are applied, for example:

- use of divers equipment and components,
- high degree of automatic self-monitoring, which allows to eliminate time dependent causes of failures,
- physical separation of redundant structures,
- cyclic testing with time delay of redundant equipment,
- the relative operation time of computers in different redundancies is moved,
- diversification of activation criteria for each accident,
- exclusion of the signal transfer between computers of different diversity,
- application of three (four) redundancies for signal processing,
- permanent auto testing for hardware and software error detection, etc.

Application of these measures enables to eliminate or minimize the effect of CCF induced errors.

CCFs are possible as hardware CCF or as software CCF. Common cause failures in the software can result from: Faulty specifications for the application software, Faulty code generation for the application software or Faulty identical software components in the firmware (operating system, driver or compiler, etc.). Regarding the specifics of digital I&C, it is necessary to take into account common failures of all computers operated under same environment and failures of all computers direct communication connection. The applied CCFs lead to failure of all corresponding computers in the same redundancy or diversity. The considered probability of common cause failure is 1.0E-5 per demand.

2.4 Fault tree model assumptions

This reliability analysis section contains detailed description of assumptions taken into account during FTA analysis. The assumptions are oriented to all analyzed signals, functions or actuation criteria. The assumptions are usually described separately for unavailability calculation per demand and calculations of frequency of spurious actuation. The assumptions contain mainly: Initial operational mode of the unit, Analyzed system boundary (measuring channels, actuation level, monitoring and service systems boundary, manual interactions, power supply boundary, ventilation, air conditioning, etc.), Monitoring and auto-monitoring assumptions, Success criteria, Software failure assumptions and CCF assumptions.

2.4.1 Fault tree models for unavailability calculations

Reliability analysis of reactor protection system is usually performed using widely used fault tree method. Average unavailability per demand is calculated for different initiating events (design basis accidents) during full power operation for reactor trip signals and for engineered safeguard feature

actuation system signals. The analytical calculations are performed using PSA software tool RiskSpectrum.

The analysis is performed taking into account actuation level (failures of transducers inclusive power supply, analogue and digital signal conditioning). Inside the programmable electronic system all hardware and software equipment of TELEPERM XS is considered which could endanger the signal acquisition and processing. Because the failure of TELEPERM XS power supply cannot cause failure of reactor trip system, it is considered only for ESFAS signals. And finally, at the actuation level the voting devices were taken into consideration.

The reliability analysis contains detailed description of FTA analysis model for unavailability calculation. It usually includes detailed description of the reliability model logic, simplified FT structure, FTA analysis results (e.g., resulting unavailability per demand, minimal cut sets, importance, sensitivity and uncertainty calculation, dominant contributors to the system unavailability and recommendations to the system reliability improvement. Detailed FT for all safety important actuation signals (RTS, ESFAS, RLS, DGC, etc.) includes approximately 1000-2000 FT pages and 4000-7000 basic events.

2.4.2 Fault tree models for spurious actuation

It contains detailed description of FTA analysis model for spurious actuation. It usually includes description of model logic, simplified FT structure, FTA analysis results, resulting probabilities and frequencies of spurious actuation per year, minimal cut sets, importance, sensitivity and uncertainty calculation, dominant contributors to the spurious actuation and recommendations to the system reliability improvement. Detailed FT for all safety important actuation signals (RTS and ESFAS) includes approximately 100 – 200 fault tree pages and 1000-2000 basic events.

3. RESULTS

The results of the reliability analysis are the following: unavailability per demand and frequency of spurious actuation or MTBF, dominant contributors to the unavailability and spurious actuation and recommendations for improvement. An important part is the comparison of regulatory requirements to results reached. There requirements are well established for failure probabilities:

- reactor trip system < 1.0 E-5 per demand,
- for single train of ESFAS $< 1.0 – 2.0$ E-3 per demand.

The results of detailed digital I&C reliability analyses can be used as inputs for probabilistic safety assessment (PSA) of the plant. In the unit PSA, it is required to address the failure of reactor trip functions, failure of engineered safeguard actuation functions. The spurious actuation of RPS or ESFAS can have influence on frequency of initiating events.

The detailed reliability model of digital I&C safety system has to be reduced (simplified) for use in a PSA. This is caused due to the significant size of the detailed I&C reliability model. The following main approaches can be used for simplification of the model:

- use of super-components,
- truncation of independent branches with very low probabilities,
- independent subsystems can be addressed as basic events.

However, the simplification must not lead to loss of dependencies. The sources of dependencies are mainly in the measurement channels, power supplies, actuation levels and common cause failures.

4. CONCLUSION

The using of digital technologies is increasing in the operation of NPPs. Not only the new plants, but also the current generation of plants uses them due to upgrades of existing analog systems. It is regulatory requirement that the reliability is justified on objective basis.

The objective of the digital system risk research is to identify and develop methods, tools and guidance for modelling reliability of digitals systems. The scope of this research is focused mainly on HW failures and limited reviews of SW failures and SW reliability methods.

The software does not fail. It does exactly as it is programmed. Given identical inputs, it produces identical outputs every time. It does not have wear out related failures. The possible SW failures have to be eliminated by extensive standardized process of Validation & Verification.

The results of reliability analyses have shown us that properly designed safety I&C systems can be very reliable from the dangerous failure (failure on demand) point of view. The frequency of spurious actuation is also very low.

References

[1] Winkler, M.: I&C Modernization Projects in Nuclear Power Plants - AREVA NP GmbH, Presentation at IAEA Workshop I&C Modernization Projects in NPPs, July 2012, Erlangen

[2] Sopira, V. et al.: Reliability analysis of the reactor trip and engineered safeguard actuation system for unit 3 of J.Bohunice V2 NPP – RELKO report RELKO 1R0703, Rev.1, February 2004, Bratislava

[3] Graf, A.: Safety Instrumentation and Control Systems for Nuclear Power Plants-Reliability Aspects and Feedback of Experience. – Siemens/KWU, IFAC 2000

[4] Sopira, V. et al.: Reliability analysis of reactor protection system (RTS, DRTS) and Engineered safety actuation system (ESFAS) for Mochovce NPP MO34 – RELKO report 1R0310, Rev.1, February 2004, Bratislava

[5] Sopira, V. et al.: Reliability analysis of reactor protection system and engineered safety features actuation system for the Renewal of I&C Systems at Loviisa NPP Unit 1 – RELKO report RELKO 1R0211, Rev.2, February 2012, Bratislava