Probabilistic Risk Assessments of Digital I&C in Nuclear Power Plant

Li Shi (I&C Electrical System, Altran Solutions Corp), Robert Enzinna (Risk & Reliability Engineering, AREVA NP), Steve Yang (I&C V&V, AREVA NP), Scot Blodgett (I&C Electrical System, Altran Solutions Corp)

Tel: 770-689-7031, Email: LShi@altransolutions.com

Abstract:

Key issues associated with the characteristics of the digital system are discussed in this paper. These issues are: Understanding the failure modes of the digital components, the fault coverage of the digital systems (e.g., the portion of the failure rate that are self-monitored and non self-monitored), the treatment of software (SW) reliability/common cause failure(CCF), the hardware failure data and planning ahead for integration with the overall plant PRA.

The modeling techniques corresponding to each of the issues above are discussed and summarized in this paper. These approaches are realistic and conservative. It also shows that by relying upon good engineering judgment and simplified modeling techniques, the NPP risk importance of a digital I&C system can be estimated with relative low cost.

The discussed and summarized methods are suitable for estimating the probabilistic risk of digital instrumentation and control (I&C) systems in nuclear power plants (NPP) for design certification (DC) and combined operating license (COL) applications at both new plants and operating plants.

Key Words: I&C, CCF, PRA, NPP

1. INTRODUCTION AND PURPOSES:

In selecting methods for modeling of digital I&C in PRA, it is important to recognize the context of the digital I&C with respect to the functions it provides in the overall plant design, not only focusing on the quality of the platform software and hardware but also considering the effect of the failure of the digital I&C on the specific safety functions that the PRA is modeling. Therefore, the key issue of the PRA modeling is to understand the potential failure modes, effect and failure hazard of the digital I&C system for a specific application [reference /1/]. Many deterministic design features such as the fail safe, fault tolerance, fault coverage (e.g., the portion of the failure rate that are self-monitored and non self-monitored), redundancy, defense-in-depth and diversity related design practices all contribute to the outcome of the failure mode and effect analysis.

Most modern digital control system consist both hardware and software. Therefore, both the software and hardware should be treated in the digital I&C PRA. However, due to the fact that the software resides on the hardware (i.e., the center processor unit), the computer processor hardware (with appropriate common cause failure (CCF) factors) provides a good boundary for PRA modeling of the software. The processor may exist at the signal acquisition, conditioning, processing, communications or output levels within the digital system. The alternative approach is to attach the software CCF probability to the hardware upon which it resides and treat it as a CCF of the hardware. The CCF probabilities of software will consider the case of hardware that shares common software, whether it is common operating system (OS) or application software [reference /2/].

There are two categories of I&C hardware component failure rates, one category of data is from the field experience, the other is the calculated failure rates or the theoretical failure rate, the latter is usually resulted from the design and prototype phase of an I&C hardware product. Understanding which set of data to use under different circumstances can lead to conservative estimation while lowering the cost of the digital I&C PRA analysis.

The scope of the nuclear plant PRA generally involves the characterization of risk as core damage frequency (CDF) and large early release frequency (LERF) (as surrogates for latent and early fatality risks, respectively, for operating light-water reactors). Large release frequency (LRF) is used as a risk metric for light water reactor (LWR) design certification (DC) and combined operating license (COL) applications. Plant perturbations such as initiating events could challenge the safety I&C systems. The failure of the safety I&C system could lead to core damage and or radioactivity release [reference/3/]. Therefore, nuclear safety digital I&C PRA is an important input to the overall plant PRA and effort for integration with the overall plant PRA should be planned well ahead.

The purpose of this paper is to discuss each of the key issues presented above in detail and present the modeling techniques corresponding to each of the issues. The

presented approaches are realistic, conservative where needed, with the objective of demonstrating that by relying upon good engineering judgment and simplified modeling techniques, the NPP risk importance of a digital I&C system can be estimated with relative low cost.

These modeling techniques and methods are suitable for estimating the probabilistic risk of digital instrumentation and control (I&C) systems in nuclear power plants (NPP) for use in applications at both new plants as well as operating plants.

2. FAILURE MODES AND EFFECTS OF THE DIGITAL COMPONENTS

The most important safety I&C systems of a nuclear power plant are the Reactor Protection System (RPS) and the Engineering Safety Features Actuation System (ESFAS).

The RPS is a system designed to monitor plant parameters related to safe plant operation and to trip the reactor when allowable operating parameters for safe operation are exceeded. The primary objective of the RPS is to protect the fuel and fuel cladding from damage. The RPS also assists in protecting against reactor coolant system (RCS) damage caused by high RCS pressure by limiting energy input to the system. By limiting energy input, the RPS also provides protection for the reactor building (RB).

The ESFAS monitors selected variables associated with the reactor and RB, which are indicative of a major loss of coolant accident (LOCA) and automatically initiates corrective action, should any of the monitored variables (RB pressure or RCS pressure) reach safety setpoint values. The primary function of the ESFAS is to provide protection for the nuclear fuel cladding and help maintain the integrity of the RB.

The digital I&C system designed to performs the protection uses primarily binary output modules to actuate the protection device (reactor trip relays, trip breaker, valves, switches, motors, etc). The principle of the safety related I&C applications design philosophy will be to fail-safe. For example, the RPS system outputs are usually designed to be de-energize-to-trip, while the ESFAS system outputs are usually designed to be energize-to-trip. The PRA should consider the potential failure modes and effect of a module's digital output (fails high, fails low, fails as-is, etc) and assess its applicability to the risk of concern. Certain failure modes can be eliminated from consideration if not credible or not applicable to the modeled consequence, e.g. fails low of the digital output module might be a concern for the ESFAS system, but not a concern for the RPS system if only the failure on demand probability is modeled, because fails low is a fail safe mode of the RPS system. "For the failure rate of a digital I&C system module, it is the analyst's choice whether to parse out the failure probability by failure mode, or take a conservative "all-modes" approach. However, parsing of the failure probability into failure modes may require a more detailed evaluation of the module internals or its operational history." [Reference /1/] Therefore, some conservative assumptions may be worth taking to reduce the cost of PRA effort.

Detailed analysis of the hardware failure reveals that not all failure modes of the hardware module are 100% self monitored or 100% non-self monitored. The percentage of failures that are self-monitored (i.e., self-revealing) versus non-self-monitored (or periodic surveillance test-revealed) is an important concept and referred as "Coverage" in the PRA analysis. The determination of the "coverage" data of the digital I&C module usually involves detailed failure mode and effect analysis of the module on the electronic component or parts level.

The "coverage" drives which mathematical unavailability model (repair-time model, test-interval model, or both) is used for each module and what modeling complexity and balance of conservatism to take in order to model the whole system [reference /2/]. Our experience shows that the module level unavailability (the building blocks of the system unavailability) is very sensitive to the "coverage" data, therefore, the effort involved in the justification and documentation of the module level "coverage" shall not be compromised.

Another distinctive feature of the modern digital I&C system is the fault-tolerant designs. Fault-tolerance is the built-in capability of the system to continue function in the presence of a limited number of hardware or software faults. Self monitoring and fault-tolerant features are characteristics of modern digital I&C systems [reference /4/]. For example, consider a three-channel system with 2-of-3 redundancy. The corresponding fault tree logic for this would typically consist of failure of 2-of-3 channels if No fault-tolerant features or No self monitoring capability exist (System fails if two or more channels fail). However, for a fault tolerant design with self monitoring capability, if all of the two channel's failure can be self monitored, the signal transmitted from these channels will be tagged as fault by the system and be excluded from the voting logic, the 2-of-3 safety digital I&C system will be able to continue function in the presence of two self monitored faults. The typical fault-tolerate logic works this way: For a covered (self monitored) fault of one of the inputs, the typical fault-tolerant program would tag the failed signal as faulty and exclude the faulty input and adjust the redundancy to 1-of-2. An additional covered (self monitored) fault might reduce the redundancy to 1-of-1. Hence, for covered (self monitored) faults, the failure logic in the fault tree may be more accurately modeled as 3-of-3 instead of 2-of-3, resulting in orders of magnitude of availability increase.

3. THE TREATMENT OF SOFTWARE (SW) RELIABILITY/COMMON CAUSE FAILURE (CCF)

For software reliability, there are two categories of CCF that need to be considered: CCF of the operating system (OS) software and CCF of the application software [reference /2/]. CCF of the OS is a hypothetical failure that is assumed to cause catastrophic failure of all of the processing computers. CCF of the application software is a postulated failure that may affect software functions or groups of related software functions that are common to redundant computer processors and share algorithms, sensor inputs, and signal trajectories.

The OS used in the nuclear I&C platforms are generally supported by a mature operating history, which allows statistical inference methods to be used to assess this part of the software CCF. However, to defeat software CCF, the OS is also very important for its role in limiting the propagation and the severity of application software failures.

Specific features of the real time OS, such as strictly cyclic operation, static memory allocation, and constant bus loading, are used to ensure reliable and predictable performance of the OS and behavior that is free of interference from the application program. These features are designed to ensure that application software failures caused by special loading (operation outside of anticipated limits), unanticipated input signal trajectories (change of input signals over time), or other application program design errors (e.g., incorrect setpoints, specification errors) will not affect the OS, and hence propagate a failure to redundant or diverse functions. With these OS defensive measures, it is unlikely that an application software failure will propagate to a diverse function via the OS, even if the diverse function is on the same processor; it is even less likely if the diverse function is on an independent processor or subsystem.

Industry topical report [reference /4/] and industry standards for safety-related digital I&C design [references /5/] discuss the value of these design features in more detail:

- independence of channels and communication networks for redundant channels and diverse systems,
- physical separation of redundant channels and diverse systems,
- separation of OS software and application software,
- fault tolerant design of application software (do not propagate missing or erroneous data),
- fiber optics (no propagation of energy-related failure),
- deterministic program execution,
- strictly cyclic processing,
- asynchronous operation,
- static memory allocation, (no dynamic memory allocation),
- constant bus loading (processing and communication buses), and
- No process-driven interrupts.

Of the real time operating system (OS) features, strictly cyclic operation, and constant loading of communication and processing buses are arguably the most important with respect to quantification of OS failure probability. For a reliability assessment of a strictly cyclic digital operating system, it makes no difference to the system whether the safety function is a closed-loop control system that acts on the process continuously or is a standby safety function. The cyclic digital I&C system is always active and always processing the same amount of data. This is an important difference from a hardwired analog system that is in standby until an actual demand occurs or tests are run. An actual system demand puts no more stress upon the OS than any other cycle. These features ensure transparency of the OS to plant conditions and transients. They prevent a leading

cause of failure that plagues standard computer systems (such as used in office systems and some automation systems), which occurs when "special loading" taxes the OS capacity. Also, since the OS failure rate is not dependent upon plant conditions, it can be assumed to be constant and the calculation of OS unavailability may be based upon observed failure rates.

Other important features are static memory allocation and asynchronous operation. These are used to combat other leading causes of standard computer system failures. Operating experience in standard digital I&C systems indicate that interference between the OS and the application program data (due to dynamic memory allocation) and faults in releasing system resources (time dependencies due to internal system clock) are leading causes of failure, which are alleviated by static memory allocation and asynchronous operation [reference /4/].

The robust design and defensive features of a real time OS platform with a mature operating history provide assurance that the OS failure probability is minimal. For a typical real time OS system, the computer processor modules may have millions of operating hours of experience, and a probability distribution such as chi-squared can provide an upper bound failure rate.

CCF of application software requires both a latent defect that can cause functional failure, and a trigger in the signal trajectory that activates the defect in multiple channels simultaneously. Much research has been attempted in various industries to predict the number of defects in application software systems before they are deployed, using various software metrics related to size and complexity. However, there are problems with that approach, including inability to quantify the relationship between the number of defects and the failure probability, which is related to the difficulty in predicting the triggering mechanisms.

The probability analysis of application software CCF is, therefore, subjectively based on the quality of the application software development life cycle process and the characteristics of the platform design. The application software CCF estimation encompasses the probability of software defects (specification errors, incorrect set points) introduced during development or maintenance, and the probability of a triggering mechanism due to an unanticipated input signal trajectory or special input signal loading that is outside of anticipated limits.

To assess digital I&C application software common-cause failures in the PRA, the design and life cycle features are assessed qualitatively. Features are identified in designing digital I&C systems that reduce both the potential for latent software defects and the probability of CCF triggers. These include features of the application software development process, such as exclusive use of qualified software functional blocks, automation tools, and rigorous verification and validation (V&V) engineering. It also includes OS features that preclude CCF triggers and eliminate failure modes that plague lesser systems, such as memory conflicts, special loading, and interference from application software errors. OS defenses to reduce triggers and failure propagation, and

functional diversity to prevent or mitigate the consequences of failures in the presence of hazards etc [reference /2/].

Characteristics of the application software development life-cycle process that ensure low probabilities for both latent faults as well as triggering mechanisms include:

- The application software development process is robust and of high quality,
- Rigorous V&V methodology is used,
- Configuration management after deployment is robust (including control of software versions, setpoint changes, spares),
- Standardized software development tools and function libraries,
- Exclusive use of pre-defined and rigorously qualified function block libraries for application programming,
- Clearly defined rules for use of the software functional blocks (including exception handling),
- Thorough coverage of pre-operational testing,
- Comprehensive exception handling,
- Deterministic program execution,
- Strictly cyclic operation, and
- OS defensive measures (see section on OS above).

For PRA and reliability analysis, the probability of an application software CCF is assigned subjectively based on the quality of the software development lifecycle process and the characteristics of the OS platform design. This application software CCF estimate encompasses the probability of defects existing in the software due to design errors (specification errors, incorrect set points) introduced during development or during maintenance, as well as the probability of a triggering mechanism due to an unanticipated input signal trajectory or special input signal loading that is outside of anticipated limits. Software design features employed by the OS platform, such as reusable software (i.e., function block libraries), not only reduce the probability of error, they also reduce the uncertainty in the subjective estimates.

The application software qualities discussed above are comparable to those for safety integrity level four (SIL-4) risk targets from IEEE 1012-1998 [reference /6/], which suggests a probability of 1e-4 to 1e-5 for failure of the system to perform its design function on demand by IEC Standard 61508 [reference /7/].

3. UNDERSTANDING THE HARDWARE COMPONENT FAILURE RATES

There are two categories of I&C hardware component failure rates, one category of data is collected through the field experience, and the other category is the calculated failure rates or the theoretical failure rate.

The field failure rate data is obtained either through vendor data collection program or industrial database program, see [reference /8/].

The calculated failure rate is based on experience values for the failure rates of the different components, e. g., capacitors, integrated circuits, circuit boards etc. of which the product consists. The result, the expected failure rate, provides data for reliability analysis, warranty questions, spare parts management, etc. Together with the field failure rate, the calculated failure rate is the basis for the hardware failure rate. Our experience indicates that the theoretical data (calculated failure rates) is usually several times more conservative than the field data (field failure rates) for the same hardware component. In practice, not all components' field failure rate is readily available for the PRA model, partially due to the lack of field data records, partially due to the fact that some of the components are relative new and have no failures being observed yet. In this case, maximizing utilization of the theoretical data will result in conservative estimation while ensuring the same modeling basis. This will facilitate the comparison and sensitivity analysis down the path of design.

4. PLANNING FOR INTEGRATION WITH WHOLE PLANT PRA

Overall Plant PRA is typically expressed by metrics of core damage frequency (CDF) and large early release frequency (LERF) (as surrogates for latent and early fatality risks, respectively, for operating light-water reactors). Large release frequency (LRF) is used as a risk metric for LWR DC and COL applicants. These metrics are defined in a functional sense as follows:

Core damage frequency is defined as the sum of the frequencies of those accidents that result in uncovery and heatup of the reactor core to the point at which prolonged oxidation and severe fuel damage are anticipated and involving enough of the core, if released, to result in offsite public health effects.

Large early release frequency is defined as the sum of the frequencies of those accidents leading to rapid, unmitigated release of airborne fission products from the containment to the environment occurring before the effective implementation of offsite emergency response and protective actions such that there is the potential for early health effects. (Such accidents generally include unscrubbed releases associated with early containment failure shortly after vessel breach, containment bypass events, and loss of containment isolation.) To provide the risk perspective for use in decision-making, a Level 1 PRA is needed to provide CDF. A limited Level 2 PRA is needed to address LERF and a full Level 2 to address LRF [reference /3/].

The safety digital I&C is part of the overall plant safety equipment that is relied upon to remain functional during the design basis events, therefore, the quantitative probabilistic measure of the safety digital I&C provides the inputs to the overall plant probabilistic risk analysis. As a good practice, measures should be implemented during the reliability analysis of the digital I&C to facilitate integration to the whole plant PRA model. This is especially true for the upgrade project, where a PRA model may already being maintained for the existing I&C equipment.

These facilitation measures include but are not limited to: probability measurement selection, PRA tool selection, and interface equipment reliability treatment.

For the probability measurement selection, as depicted above, the prevalent measurement unit for the overall plant PRA is usually the undesired event frequency, which is the product of certain undesired probabilities (unavailability for the repairable equipment) and initiation event frequency. Therefore, usage of unavailability (failure on demand) or spurious trip/actuation frequency as the probability measurement of the digital I&C equipment serves the purpose.

For the new NPP applications, it is important to ensure that the same tool is used across different PRA organizations if the design is a collaborated effort. For the upgrade application, it is important that the PRA engineers utilize the same tool as how the existing plant PRA is maintained.

For the provided equipment that serves the interface between the digital I&C system and the plant equipment (e.g. sensors, relays, etc), it is important to clarify in the scope of the analysis whether these equipments are included in the scope of the digital PRA, if not, a list of failure rates of the these equipments should be provided to facilitate the integration process.

4. CONCLUSION

This paper discusses and summarizes several key issues related to modeling the PRA of nuclear safety digital I&C systems and presents the probability risk quantification techniques corresponding to each of the issues. The presented approach is a realistic methodology, and conservative where needed. It also shows that by relying upon good engineering judgment and simplified modeling techniques, the NPP risk importance of a digital I&C system can be estimated with relative low cost.

Acknowledgements

I would like to express my gratitude to Bob Enzinna, Steve Yang and Lionel Bates for their assistance during my work as a system and analysis engineer at AREVA NP. This work will not come to fruition without their help.

I would also like to express my gratitude to Scot Blodgett for the constructive comments and suggestions provided before conclusion of this work.

5. REFERENCES

[1] "Modeling of Digital I&C in Nuclear Power Plant Probabilistic Risk Assessments," white paper by Nuclear Energy Institute digital I&C working group, July 2, 2007.

[2] Software Common-Cause Failure Probability Assessment, "6th International Topical Meeting on Nuclear Plant Instrumentation Control and Human Machine Interface Technology (NPIC&HMIT 2009)

[3] Regulatory Guide 1.200, March 2009 "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities"

[4] AREVA NP Inc., Topical Report EMF-2110(NP) (A) Revision1, TELEPERM XS: A Digital Reactor Protection System, Siemens Power Corporation, May 2000.

[5] IEEE Standard 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

[6] IEEE Standard 1012-1998, "IEEE Standard for Software Verification and Validation"

[7] IEC-61508, "Functional safety of electrical / electronic / programmable electronic safety-related systems (E/E/PES)

[8] IEEE Standard 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems"