Lessons Learned in PRA Modeling of Digital Instrumentation and Control Systems

Richard W. Rolland III[a], Raymond E. Schneider[b]
[a] Westinghouse Electric Company LLC / PWROG, USA, *rollanrw@westinghouse.com*
[b] Westinghouse Electric Company LLC / PWROG, USA, *schneire@westinghouse.com*

Abstract: As the existing nuclear plant fleet ages and evolutionary plants are added to the nuclear plant generation capacity, analog safety systems that have been the mainstay of nuclear plant protection systems have started to become obsolete. These obsolescence issues are causing analog systems to be replaced with digital systems. The digital replacements offer several advantages over the analog counterparts including the ability to self-diagnose failures and online testing of systems. While these features increase the overall reliability of the system and reduce maintenance costs, they increase the complexity of the system. Additionally, digital systems have the possibility of global failures from common cause failure of software. It is helpful to build a PRA model for the digital system to fully understand the risk impact of the analog to digital transition. The complexity and relationships among the diverse and redundant system components introduces challenges to modeling of these systems.

This paper discusses developing a digital I&C PRA model and explores the lessons learned in its development. Specifically, the paper focuses attention to the role of the failure mode and effects analyses, availability of detailed hardware and software failure data, the interaction of internal system diagnostics on system unavailability, and potential treatment of environmental conditions. Of particular importance, the paper discusses the potential treatment options for hardware and software related common cause failure. Based on a larger number of similar components within a digital system, the potential impact of common cause failure scenarios has increased compared to analog systems. Methods for appropriate modeling and for addressing challenges to common cause failures will be discussed.

Keywords: Probabilistic Risk Assessment, Digital I&C, Software Reliability, Common Cause Failure

1. INTRODUCTION

Technology improvements in digital systems have allowed for plants to install and take credit for digital instrumentation and control (DI&C) systems with the goal of improving safety and reliability compared to the analog instrumentation and control (AI&C) systems. As AI&C systems continue to age, DI&C systems have begun to replace AI&C systems due to the expenses of maintaining AI&Cs systems and the improved reliability benefits identified for DI&C systems.

As DI&C systems are being installed in nuclear power plants as replacements to AI&C systems, the level of detail and modeling best practices within the probabilistic risk assessment (PRA) model has become a topic of interest for DI&C retrofits in Generation II plants.

The Pressurized Water Reactors Owners Groups (PWROG) has piloted a replacement DI&C safety features sequencer (SFS) system in a Generation II plant. Southern Nuclear Operating Company provided support as the pilot plant for this effort. The specific intent of this effort was to develop a PRA representation of the digital SFS, as well as to provide lessons learned that may be applied to modeling of future DI&C replacement systems. This paper will discuss the highlights of the resulting DI&C modeling efforts along with future steps to improve upon DI&C PRA modeling.

2. DIFFERENCES BETWEEN AI&C AND DI&C

While AI&C systems are simple and reliable, DI&C systems generally provide noticeable improvements compared to their AI&C counterparts. Some benefits include (1) additional system redundancy including intra-train redundancy, and (2) the ability to perform on-line self-diagnostics including the ability to detect local failures. These features are intended to enhance system reliability and reduce out of service time by quick identification of issues within the DI&C system.

Although DI&C systems have significant benefits as mentioned above, their reliance on a common suite of software controlling both the overall operating system and local actuation logic represents a key dependency that needs to be addressed. This relatively high reliance on software can lead to scenarios where a single software error could be propagated not only within the train but within the entire system. If similar inputs at around the same time are provided, as would be expected absent external signal failures, these similar inputs could result in a universal system failure from the common software between trains. Design and software verification processes are employed to minimize this, although the potential for common cause failure of software cannot be entirely eliminated. Therefore, the proper determination on the identification of and treatment of software failures within the DI&C PRA model is an important element in assessing the reliability of the DI&C system.

3. OVERVIEW OF PILOT SAFETY FEATURES SEQUENCER

This pilot modeled a digital SFS that replaced an analog SFS at the plant. The digital SFS provides for actuation of the diesel generator if loss of offsite power occurs and/or a safety injection signal is received. Additionally, the SFS provides for proper load-shed and sequencing of engineered safety features equipment in the scenario of loss of offsite power and/or a safety injection signal to prevent overloading the bus or the diesel generator.

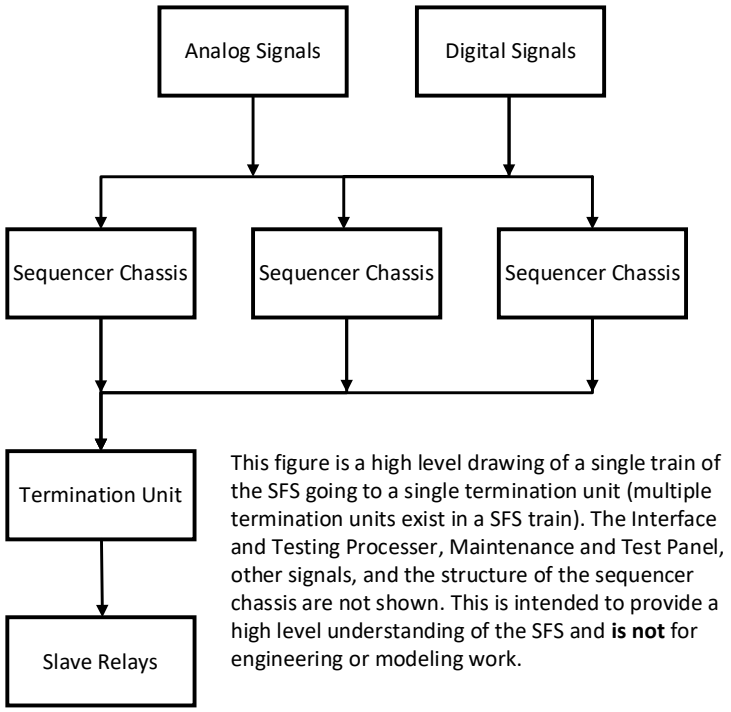

Figure 1: High-Level Diagram of the SFS

As seen in the high-level design in Figure 1, the digital SFS receives both analog and digital signals to respond to events that require diesel generator initiation or sequencing of equipment. These signals are evaluated in the sequencer chassis, which consist of three chassis per SFS train. Each of these sequencer

chassis transmits an output signal to the termination unit that then performs voting logic of the signals from the chassis to determine if an output signal to the slave relays should be transmitted. The SFS has an interface and test processor that is used for performing online testing and providing alarming capabilities for the system. In addition, there is a maintenance and test panel that is used for maintenance and testing capabilities. The SFS is supported by a power distribution system similar to AI&C systems and also has supported cabinet cooling within the system.

4. FAILURE MODES AND EFFECTS ANALYSIS

A critical aspect of modeling the DI&C system is the need for the identification of single and multiple component failures that can compromise the function of the system. This information is typically available from the DI&C system failure modes and effects analyses (FMEA).

The FMEA provides a comprehensive assessment of the failure modes of the components within the digital system being examined, helping the analysts to identify those pathways that could lead to a failure of the DI&C system functions. The FMEA can also be used to simplify the DI&C model by enabling the analysts to screen components that are not impacting the safety features of the DI&C system. For example, a visual interface for maintenance activities would generally not be considered to impact the safety features of the digital system.

A component can consist of multiple sub-components that, when integrated into a single component, supports a function. This integrated component can be identified as a potential failure mode of the function within the FMEA and used as a basis for modeling the single integrated component rather than separate sub-components. When choosing to model at higher levels (e.g., a component that consists of multiple sub-components), it is important to identify if there are sufficient modeling details to prevent conservative results while avoiding unnecessary complexity in the model (refer to Section 5.3).

4.1. Binning Components in the FMEA

It is helpful to bin components in the FMEA into categories based on whether the component causes a safety function failure by itself, with other component failures, or if the component failure does not cause a safety function failure. During the piloting effort, if a component was associated with a safety function failure, it was evaluated for modeling within the PRA model. If the component does not impact the safety functions of the system, it generally screens out of the PRA modeling as having no significant impact to the risk of the system. The use of binning helps in identifying the PRA modeling structure of potential failure modes that can lead to a degraded state for the DI&C system.

The binning process and examination of the FMEA provided information on the level of redundancy in the pilot system. Since DI&C redundancy and support for specific functions can be complex including redundancy within components itself, a detailed FMEA provides for understanding the structure of the system prior to I&C system engineer interviews.

4.2. Evaluation of Testing Features in the FMEA

As identified during the SFS piloting effort, DI&C systems may have multiple testing features that can identify failures of a component within the system and alert the operators to a system failure. Direct modeling of these components may not be necessary since the failure themselves do not directly fail a safety component (i.e., they prevent the repair of it). Exclusion of these components, on the other hand, lead to conservative results in not considering the automatic testing features of the DI&C system. To resolve this, I&C vendors generally have data for the probability of detecting a failure based on the reliability of the automatic testing features. The probability of detection can be included as factor in the calculation of the unavailability of specific components that are tested rather than explicitly modeling testing components. This allows for credit to be taken to repair the SFS.

4.3. Redundancy within the Digital System

Safety-related DI&C systems tend to be designed with multiple redundant pathways within the system itself. Therefore, there may be multiple logic checks within a train, or even within a component, to reduce the probability of failure to perform system functions. These additional pathways and degradation of the pathways are identifiable within the FMEA. Due to the level of redundancy, explicit modeling of all redundant pathways can potentially overwhelm the model and result in unnecessary complications and loss of insight into the system behavior. Therefore, these redundancies should be considered in a way that best identifies their separation while not creating significant increases in modeling complexity.

For example, a component may process several channels and each channel may be evaluated with a specific set of sub-components. These sub-components that support an individual channel can require support from other sub-components that have redundancy and are shared between channels. A component may have a high percent of the failures related to sub-components that support all of the channels. In this scenario, separation of the component into individual channels may not have a significant impact on the failure rate of the component and would increase model complexity. As the FMEA is evaluated along with the data analysis, the modeling detail that would provide beneficial results in division into sub-components becomes apparent.

4.4. Temperature Limits on Digital Systems

The FMEA should have identification of fans and other support systems for cooling in the DI&C system. It is generally advisable to include the fans located internal to a component within the component failure rate if it is associated with the failure of the component; this is generally within the failure rate provided by I&C vendors. For individual fan components within the system, the FMEA may describe that its failure does not lead to the failure of the system but increases the temperature within the system and can lead to increased failure rates of components. Therefore, determining whether the fan should be modeled should take into account if there are significant failure rate differences at higher temperatures for those DI&C components.

Additionally, temperature operating conditions of the DI&C system may be dependent on the successful operation of heating, ventilation, air conditioning (HVAC) / room cooling systems. Failure of these systems may result in a temperature increase that can lead to a failure of the DI&C system, or at a minimum impact system reliability since DI&C components are more susceptible to failure at higher temperature (refer to Section 5.2). As described in Section 3.2.4.1 in PWROG-18027-NP [1], evaluation of HVAC screening in PRA models should examine the impacts of elevated temperatures on DI&C systems. If the HVAC / room cooling system support becomes a significant contributor to the failure of the DI&C system, reevaluation of temperature effects on the system can be addressed in PRA modeling refinements.

5. HARDWARE FAILURE RATES OF DIGITAL COMPONENTS

As DI&C components have generally had fewer hours of operation than AI&C components, the amount of data for DI&C components can be limited. I&C vendors have begun to collect data on their DI&C components that can be used to identify expected failure rates of those components. Generic data sources may not have data for specific DI&C components and/or data sources may be conservatively biased, or not directly applicable to the installed environments. Therefore, it is advantageous to discuss with the I&C vendor to determine the most appropriate component data.

5.1. Challenges with DI&C Data

Hardware failure data is generally available from I&C vendors and can be used as a starting point. During evaluation of the data collected for the pilot SFS, it was discovered that it can be difficult to identify whether the failure is due to hardware or software based on the recorded data. For example, if

a failure in a component occurs and the replacement of the component requires rebooting of the system, the component failure may have been caused by a software failure that could have been fixed from a reboot of the system rather than the replacement of the component. The historical challenge in the complete characterization of failure data for DI&C components is being overcome by more recent data gathering criteria. Even if the hardware data includes several mischaracterized software related failure events, the data is conservatively bounded with respect to hardware failures.

5.2. Temperature Effects on Digital Component Failure Rates

As seen throughout the use of digital computing, temperature dependence on hardware components is an important aspect with regards to their long-term reliability. Since exposure to elevated temperatures over the lifetime of a component impacts its reliability, a bounding estimate of a failure to a component can be established by assuming the maximum temperature within the operating limit range as the temperature experienced. The maximum temperature operating limits are usually identified within the technical specifications of the DI&C system and can be provided by the I&C vendor. In the pilot example, the I&C vendor provided a modifier that is applied to the failure rate between the component failure under normal operating temperature conditions and the component failure under the maximum operating temperature within the technical specifications. Although conservative, this is anticipated to take into account the range of operating temperatures experienced by the system. Further evaluation of temperature effects on digital components could be necessary as DI&C PRA modeling best practices develop. For example, evaluation of digital failure data may be able to provide an approximate failure rate over the lifetime of these components with the assumption that the data collected is an appropriate representation of the average operating temperature experienced.

5.3. Estimation of Failure Rates and Detailed Modeling of Digital Components

Digital components are generally a collection of smaller individual sub-components that when combined provide the functions desired for the component. Due to this, digital components can have their failure rates estimated based on the failure data of sub-components within the component if there is not sufficient data from observed performances.

There are several software programs that can be used to estimate failure rates of electronic sub-components that I&C vendors use to estimate risk of components. For example, the **217Plus™**[*] calculator [2] is a tool used to estimate the failure rate of DI&C / electronic components. After acquiring this failure rate data for sub-components, a reliability block diagram can be created. A first estimate of the component failure rate may use the parts count method which was originally identified for electronic component failure rate estimations in Appendix A in MIL-HDBK-217F [3]. The parts count method sums the failure rates of each of the sub-components within a component together to predict the failure rate. Although simple to estimate, the parts count method can lead to conservative estimations in cases with significant redundancy within the component as identified in the pilot. Detailed modeling of the sub-component interactions can be undertaken, but this is only beneficial if it is determined that the component in question is a significant contributor to risk and there is sufficient redundancy within the component (e.g., redundancy of sub-components) as this increases the complexity of the PRA model.

As illustrated in Figure 1, SFS chassis output signals are directed towards one of the termination units. It is in the termination unit that SFS chassis output signals are further evaluated and an output signal is generated to the slave relay if voting logic criteria is met. During the pilot, the termination unit was identified as having the parts count method used for its estimation of failure data which had conservatism from this approach. For this example, it was concluded that sub-division to the individual channel level would not provide a significant impact to the failure rate of the termination unit. Instead, the failure rate is driven by other sub-components within the termination unit that are shared between

[*] 217Plus is a trademark or registered trademark of Quanterion Solutions Incorporated. Other names may be trademarks of their respective owners.

the channels but have redundancy that was not previously accounted for. Therefore, detail modeling of these sub-components may be useful in reduction of the failure rate of the termination unit.

In summary, sub-component modeling decisions should be driven by a clear improvement of the failure rate calculated compared to the simpler parts count method; otherwise the increased complexity of the model quickly counterbalances the benefit of detailed modeling. If sub-component modeling is completed, the most appropriate way to detail model the sub-components to provide a reduction in failure rates should be examined as certain additional modeling details (e.g., evaluation at the channel level) may not provide an impact to the failure rate of the component.

5.4. Unavailability

DI&C data was represented via unavailability of components in the piloting effort. This allowed for repair times, identification of errors due to testing, and other aspects of the components to be accounted for. For example, due to the use of unavailability, several automatic testing features are represented by a probability of detection which identifies the chance a component failure is detected. This probability of detection can be taken into account in the calculation of unavailability. There are other aspects to this unavailability calculation including the amount of time to repair or replace a component given a detection of a failure. The structure of how unavailability of the components is calculated allows for a more refined analysis on the chance a component is out of service during an accident. I&C vendors generally have information on calculation of the unavailability for their DI&C components.

6. COMMON CAUSE FAILURE

Common cause failure in digital systems can be separated into two categories: (1) hardware common cause failure, and (2) software common cause failure. Each of these common cause failures have a unique aspect to manage when it comes to digital components although both are challenged by data availability.

6.1. Hardware Common Cause Failure

There is minimal common cause failure data available for DI&C systems. On the positive side, there are few simultaneous common cause failures recorded for digital hardware components; although the data that is recorded generally lacks details on the failure. This provides a challenge in identifying the proper modeling techniques for DI&C modeling. An approach for modeling of DI&C systems for hardware common cause failures was to identify a beta factor failure rate from the methodology in Annex D in IEC 61508-6 [4]. In the pilot application, beta factor failures rates were used due to limited data availability. These were determined to be overly conservative for the analysis for systems with significant redundancy since the beta factor model assumes common cause fails all trains. The larger common cause component groups is an additional challenge for DI&C systems.

To address these limitations, other CCF approaches were examined. It was determined that the “shock model” CCF approach (also referred to as the binomial failure rate) that is identified in Annex D in IEC 61508-6 [4] may be more appropriate. Annex D in IEC 61508-6 [4] uses the beta factor as an input to approximate the data for the “shock model” CCF approach if data is not available. This allows for a more refined approach where CCF is evaluated on the basis of how many components within the same common cause component group fail, rather than all of them failing. Using the “shock model” with the beta factor assumptions to develop the CCF factors is planned to be examined in proposed future piloting work.

6.2. Software Common Cause Failure

Software failure is unique in the sense that common cause failure may be more pronounced depending on the impact of the software error. For example, if a signal is sent to identical processors in multiple trains, similar inputs can result in the same output failure and lead to a failure of the entire system. This

leads to a modeling decision on how to properly evaluate software failures. Further complication arises from the fact that software failures are not always readily identified within recorded failure data of components (e.g., restarting of the system may reset a software error but not be logged as a software error when analyzing data on system and component failures).

For the pilot system completed, the impact of software failures on system reliability was conservatively represented by a single software basic event that fails the entire system. This bounding estimate was established from available reference system design information associated with the evaluation and determination of the safety integrity level (SIL) of the SFS system. The SFS is designed in accordance with procedures to ensure a higher SIL requires that the software have a higher reliability and is assumed to have a lower chance of failure. Annex D in IEC 61508-7 [5] further describes the failure rates based on the SIL.

Realistic treatment of software failures is complex. The United States Department of Energy (DoE) has begun work on new processes for more realistically identifying and quantifying software failures (refer to INL/EXT-21-64039 [6]). Evaluation and piloting of these DoE methods has been identified as a potential path forward to improve software failure estimates. One of the research topics in the industry is how to appropriately separate out the software failures within the system. In other words, how much of the software should be a system-wide failure, multiple train failure, or component-level failure is an ongoing discussion and has to be further examined. It is expected that insights from the DoE analysis can reduce conservatisms in the current treatment of software failure and provide for potential best practices with a more realistic path forward for software failure estimates.

7. MODEL INCORPORATION

As a result of the high number of potential modeling links in DI&C systems, it is important to take the level of system model complexity into account during development of the model and how this impacts the level of effort to complete system model linking. Specifically, when incorporating the DI&C model into the plant PRA model, one should consider the multiple links between the previous AI&C system and the rest of the PRA model. In the example of the SFS pilot, the AI&C system had dozens of links at the channel level between the system model and the rest of the PRA model. These link each supported individual channels for actuation of equipment and had to be separately identified and properly associated with the DI&C system channel during model incorporation, including the correct termination unit and the correct SFS logic. Additionally, external system interactions (e.g., loss of HVAC to the room containing the SFS) should be evaluated.

8. RESULTS

The pilot DI&C system was incorporated into the plant model and quantified. From the results, it was determined that there were conservatisms in the process that had to be further evaluated. Most of the SFS contribution to CDF and LERF were from cutsets with failures due to the CCF of the hardware, CCF of the software, and the termination unit and supporting components to the termination unit. From this, lessons learned were identified on aspects of the model that could be improved upon. The three main improvements identified were reducing conservatisms in the hardware CCF, software failures, and detailed modeling of certain components.

Use of the beta factor method for hardware leads to overly conservative results in the plant due to the higher risk importance of safety related DI&C systems. Since there is limited data availability regarding quantification of CCF factors, future piloting efforts are proposed to estimate CCF through the use of the beta factor as an input into the “shock model” as described in Annex D in IEC 61508-6 [4].

The software failures are also a significant contributor to the overall risk of the digital SFS. Existing approaches used in the SFS in software reliability modeling is believed to be conservative. Future efforts are therefore proposed to examine the new software failure approaches identified by DoE [6]. Specifically, identification of realistic software failure rates and CCF separation.

Several DI&C components within the SFS used the parts count method in estimating the failure rate of the component. The parts count method is conservative in most scenarios and can have an impact on the results of the PRA model. In the scenario components are significant contributors to risk of the DI&C system, the failure rate of the component may have to be examined in more detail by enhancing the model to account for the level of redundancy within the integrated component itself. In these scenarios, additional information from the I&C vendor may be required to break up the modeling of the integrated component into sub-components. The identification of when this is useful and guidelines of best practices in modeling at the sub-component level is a topic of further interest.

As DI&C continues to evolve, these proposed improvements are planned to be examined to further the capabilities of DI&C PRA modeling.

9. CONCLUSION

This paper discusses the DI&C efforts that have been undertaken in piloting current practices in DI&C PRA modeling of a typical SFS and associated lessons learned. Additionally, proposals for future improvements in modeling DI&C systems have been identified for potential future piloting activities. As DI&C PRA modeling continues to be developed and implemented in the industry, it is expected that additional DI&C PRA modeling lessons learned will be developed to allow for a more transparent and structured DI&C PRA modeling process in the industry.

Acknowledgements

The authors would like to thank:

- The PWROG for their support in funding the piloting efforts that have led to this paper's development and for PWROG members providing comments and feedback on the pilot.
- Southern Nuclear Operating Company that supported piloting of this effort and providing feedback and comments.
- Taeyong Sung from Southern Nuclear Operating Company for his feedback and comments to improve the analysis and lessons learned during the PWROG piloting effort.
- Al Denyer, Jeremy Sawyer, and Terry Tuite from Westinghouse Electric Company LLC for their I&C support in piloting the SFS.
- International Electrotechnical Commission (IEC) for their guidance documents referenced in this paper [4, 5].
- Department of Energy (DoE) for their new guidance that may be used to improve software failures in future pilots [6].
- Quanterion Solutions Incorporated for development of the **217Plus™** calculator [2].

References

[1] J. Beckton, "*Loss of Room Cooling in PRA Modeling*," PWROG-18027-NP, Revision 0, Westinghouse Electric Company LLC / PWROG, 2020, Pittsburgh.

[2] "***217Plus™**:2015 Notice 1 Spreadsheet Calculator*," Quanterion Solutions Incorporated, 2017.

[3] "*Military Handbook: Reliability Prediction of Electronic Equipment*," MIL-HDBK-217F, Change Notice 2, United States Department of Defense, 1995.

[4] "*Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*," IEC 61508-6, Edition 2.0, International Electrotechnical Commission, 2010, Geneva.

[5] "*Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures*," IEC 61508-7, Edition 2.0, International Electrotechnical Commission, 2010, Geneva.

[6] H. Bao, T. Shorthill, E. Chen, H. Zhang, "*Light Water Reactor Sustainability Program: Quantitative Risk Analysis of High Safety-significant Safety-related Digital Instrumentation and*

Control Systems in Nuclear Power Plants using IRADIC Technology," INL/EXT-21-64039, United States Department of Energy, 2021.