INL/CON-21-61822-Revision-0

INTEGRATED RISK ASSESSMENT OF DIGITAL I&C SAFETY SYSTEMS FOR NUCLEAR POWER PLANTS

June 2021

Hongbin Zhang, Han Bao, Edward Quinn, Tate Shorthill

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-21-61822-Revision-0

INTEGRATED RISK ASSESSMENT OF DIGITAL I&C SAFETY SYSTEMS FOR NUCLEAR POWER PLANTS

Hongbin Zhang, Han Bao, Edward Quinn, Tate Shorthill

June 2021

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

INTEGRATED RISK ASSESSMENT OF DIGITAL I&C SAFETY SYSTEMS FOR NUCLEAR POWER PLANTS

Hongbin Zhang and Han Bao
Idaho National Laboratory
2525 Fremont Ave, Idaho Falls, ID, 83402, USA
Hongbin.Zhang@inl.gov, Han.Bao@inl.gov

Tate Shorthill
Department of Mechanical Engineering and Materials Science, University of Pittsburgh
3700 O'Hara Street4200 Fifth Ave, Pittsburgh, PA 152601
ths60@pitt.edu

Edward Quinn
Technology Resources, Dana Point, CA
tedquinn@cox.net

[Digital Object Identifier (DOI) placeholder]

ABSTRACT

Upgrading the existing analog instrumentation and control (I&C) systems to state-of-the-art digital I&C (DI&C) systems provides the foremost means to improve performance and reduce costs for existing light-water reactors (LWRs). However, qualification of digital technologies remains a challenge—especially the issue of software common cause failure (CCF), which has been difficult to address. Existing analyses of CCFs in I&C systems mainly focus on hardware failures. With the application and upgrading of new DI&C systems, design flaws could cause software CCFs to become a potential threat to plant safety, considering that most redundancy designs use similar digital platforms or software in their operating and application systems. With complex multi-layer redundancy designs to meet the single failure criterion, these I&C safety systems are of particular concern in U.S. Nuclear Regulatory Commission (NRC) licensing procedures. In 2019, the Risk-Informed Systems Analysis (RISA) Pathway of the U.S. Department of Energy's (DOE's) Light Water Reactor Sustainability (LWRS) Program initiated a project to develop a risk assessment strategy for delivering a strong technical basis to support effective, licensable, secure DI&C technologies for digital upgrades and designs. An integrated risk assessment for the DI&C (RADIC) process was proposed for this strategy to identify potential key digital-induced failures, implement reliability analyses of related digital safety I&C systems, and evaluate the unanalyzed sequences introduced by these failures (particularly software CCFs) at the plant level. This paper summarizes these RISA efforts in the risk analysis of safety-related DI&C systems at Idaho National Laboratory.

Key Words: digital I&C, risk assessment, common cause failure, hazard analysis, reliability analysis

1 INTRODUCTION

Digital upgrades and plant modernization efforts offer the foremost path to performance and cost improvements of nuclear power plants (NPPs) (Thomas and Scarola 2018). Despite decades of experience with analog systems, the technical challenges associated with their continued use (e.g., signal drift, high maintenance costs, obsolescence, lack of industrial suppliers) have caused the nuclear industry to move toward digital instrumentation and control (DI&C) in favor of integrated circuitry and the modern microcontroller (National Research Council 1997). Compared with analog systems, DI&C systems offer significant advantages in the areas of monitoring, processing, testing, and maintenance (Hashemian 2011) (Chu, et al. 2010). Notwithstanding the immediate attraction, the nuclear industry has been slow to adopt safety-rated DI&C because each new design must be shown to maintain or improve the status quo by means of a risk assessment (National Research Council 1997). Though many of the concepts for the risk assessment of analog systems carry over, DI&C systems present unique challenges. In 1997, the National Research Council detailed several technical challenges for the implementation of DI&C systems. Those relating specifically to the present work are: (1) the system aspects of digital systems; (2) the potential for software-based common cause failures (CCFs); and (3) the need for a risk assessment method tailored to DI&C systems (National Research Council 1997).

The system aspects of DI&C involve issues that extend beyond individual components and even beyond the function of the system itself. The challenge with using these system aspects is discussed in NUREG/CR-6901. Digital systems exhibit two types of interactions—Type 1: the interactions of a DI&C system (and/or its components) with a controlled process (e.g., NPP); and Type 2: the interactions of a DI&C system (and/or its components) with itself and/or other digital systems and components (Aldemir, et al. 2006). Kirschenbaum et al. provide a useful summary of these concerns in their own work on the investigation of digital systems (Kirschenbaum, et al. 2009). Common or redundant components are often utilized as a backup to ensure system reliability. However, the improper application of redundant features can leave a system vulnerable to CCFs, which arise from the malfunction of two or more components, or functions, due to a single failure source (Thomas and Scarola 2018) (Wierman, Rasmuson and Mosleh 2007). In order to make redundancy designs effective, diversity is employed, providing an alternative technology, method, technique, or means to achieve a desired result (U.S. Nuclear Regulatory Commission 1979). The diverse protection helps to eliminate the common features necessary for a CCF. Some general observations on the consistencies and inconsistencies in how defense-in-depth (DiD) has been defined and used were included in NUREG/KM-0009, "Historical Review and Observations of Defense-in-Depth" (U.S.NRC, Historical Review and Observations of Defense-in-Depth 2016). In 2016, the NRC revised the Standard Review Plan (SRP) to fully adapt it and the associated regulatory guides to DI&C systems (U.S.NRC, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition — Instrumentation and Controls 2016). Chapter 7 of the SRP provided guidance for the review of the instrumentation and control (I&C) portions of: (1) applications for nuclear reactor licenses or permits and (2) amendments to existing licenses. These reports provide a basis for dealing with CCFs. The need remains to identify the most significant CCFs to focus the application of diversity in design.

Diversity and DiD analyses are proposed and performed using deterministic approaches while the NRC probabilistic risk assessment (PRA) policy statement encourages the use of risk information in all regulatory activities supported by the state of the art and data (U.S.NRC, Use of Probabilistic Risk Assessment Methods in Nuclear 1995). Activities to develop digital system models have been in process for some time; however, no approaches have been generally accepted for digital system modeling in current NPP PRA efforts. Currently, the NRC continues to perform research that supports the development of licensing criteria to evaluate new DI&C systems. According to guiding principles in SECY-18-0090 (NRC 2018), published in 2018, a DiD analysis for reactor trip systems and engineered safety features should be performed to demonstrate that vulnerabilities to a CCF have been identified and adequately addressed, either by a design-basis deterministic approach or best-estimate approach. Recently, in January 2019, NRC staff developed the Integrated Action Plan (IAP) (U.S.NRC, Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure 2019). It updates the plan as a living document. One of the goals of the IAP is to assist NRC staff in performing regulatory reviews and I&C system inspections in more efficient, effective, consistent, and risk-informed ways. In addition, industry is seeking a more risk-informed, consequence-based regulatory infrastructure that removes uncertainty in requirements and enables technical consistency (U.S.NRC, Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure 2019). Therefore, a need clearly exists to develop a risk assessment strategy to support quantitative DiD analyses for assuring the long-term safety and reliability of vital digital systems and reducing uncertainties in costs, time, and support integration of digital systems in the plant. Many efforts from regulatory, industrial, and academic communities have been made for risk analysis of DI&C systems, but there is no consensus method for the software reliability modeling of digital systems in an NPP.

In FY-2019, the Risk-Informed Systems Analysis (RISA) Pathway of the U.S. Department of Energy's (DOE's) Light Water Reactor Sustainability (LWRS) program initiated a project to develop a risk assessment strategy for delivering a strong technical basis to support effective, licensable, and secure DI&C technologies for digital upgrades/designs (Bao, Zhang and Thomas, An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants 2019). An integrated risk assessment for the DI&C (RADIC) process was proposed for this strategy, which aims to identify key digital-induced failures, implement reliability analyses on related digital safety I&C systems, and evaluate the unanalyzed sequences introduced by these failures (particularly software CCFs) at the plant level. More details are included in Section 2. According to the guidelines and requirements of the RADIC process, an approach for REdundancy-guided Systems-theoretic Hazard Analysis (RESHA) was developed in FY-2020. It aims to help system designers and engineers address digital-based CCFs and qualitatively analyze their effects on digital system vulnerability. It also provides a technical basis for implementing future reliability and consequence analyses of unanalyzed sequences and optimizing the use of DiD analyses in a cost-effective way. This approach has been developed and applied for the hazard analysis of digital reactor trip system (RTS) and engineered safety features actuation system (ESFAS). Relevant description and case studies are shown in Section 3. A method for reliability assessment of digital control systems with consideration for the quantification of CCFs is described in Section 4, which is defined as a BAyesian and HRA(human reliability analysis)-Aided Method for the reliability Analysis of Software (BAHAMAS). Section 5 summarizes the conclusion and future work on risk assessment of DI&C systems.

2 RISK ASSESSMENT PROCESS FOR DI&C SYSTEMS

The overall goal of developing an integrated risk assessment approach is to deliver a strong technical basis to support effective, licensable, and secure technologies for digital I&C upgrades/designs. To deal with the expensive licensing justifications from regulatory insights, this technical basis is instructive for nuclear vendors and utilities to effectively lower the costs associated with digital compliance and speed industry advances by: (1) Defining an integrated risk-informed analysis process for digital I&C upgrade, including hazard analysis, reliability analysis, and consequence analysis; (2) Applying systematic and risk-informed tools to address CCFs and quantify responding failure probabilities for digital I&C technologies; (3) Evaluating the impact of digital failures at the individual level, system level, and plant level; (4) Providing insights and suggestions on designs to manage the risks, thereby supporting the development, licensing, and deployment of advanced digital I&C technologies on NPPs.

It is critical for the viability of a nuclear power fleet to upgrade digital I&C (e.g., safety and non-safety-related) systems in existing NPPs within a cost-effective and regulatory acceptable way. One key outcome of this project is to perform a plant-specific risk assessment to provide a sustainable scientific support for enabling industry to balance the digital-related risks, costs, reliability, and safety.

The RADIC process includes two phases: risk analysis and risk evaluation. Risk analysis aims to identify hazards of digital-based SSCs, estimate their failure probabilities, and analyze relevant consequences by performing hazard analysis, reliability analysis, and consequence analysis. The results from the risk analysis are compared with the specific risk-acceptance criteria in the risk evaluation. The schematic of the risk-assessment strategy for digital I&C systems is displayed in Figure 1. The tasks of the RADIC process are to evaluate whether the risk from digital failures can be accepted at the individual, system, and plant levels.

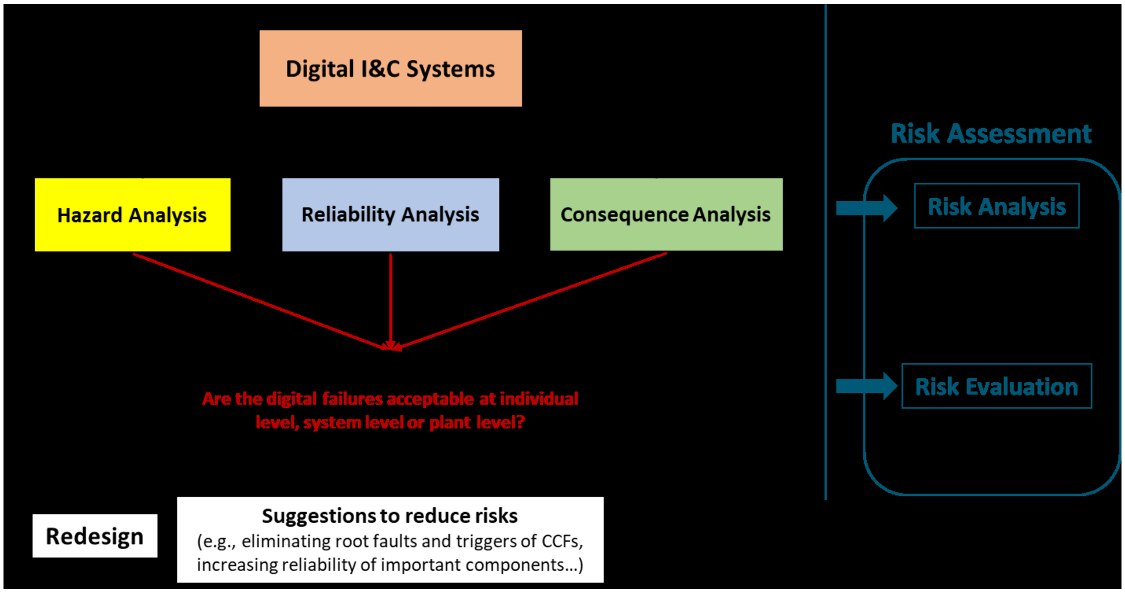

Digital I&C Systems
Risk Assessment
Hazard Analysis
Reliability Analysis
Consequence Analysis
Risk Analysis
Are the digital failures acceptable at individual level, system level or plant level?
Risk Evaluation
Redesign
Suggestions to reduce risks
(e.g., eliminating root faults and triggers of CCFs, increasing reliability of important components…)

Figure 1. Schematic of RADIC process.

As the first part of risk analysis, hazard analysis needs to identify all potential software failures and hardware failures. The acceptance criterion is defined as, "Does the individual digital failure directly lead to the loss of function of the digital system?" The key outcome of hazard analysis is the integrated fault tree that includes both hardware and software failures, and its cut set for the top event. The top event is normally set as the loss of function of the target digital system. The "individual digital failure" in acceptance criterion refers to every basic event in this integrated fault tree for this specific top event, which can be a hardware failure, software failure, or human error. If the occurrence of this individual failure (e.g., software CCF) can result in the top event regardless of the occurrences of other basic events, its risk is not acceptable for the acceptance criterion. Accordingly, a redundancy-guided systems theoretic approach was developed for safety-related digital I&C systems for supporting I&C designers and engineers to address both hardware and software CCFs, and to qualitatively analyze their effects on system availability. It also provides a technical basis for implementing following reliability and consequence analyses of unexpected software failures and recommending on the optimization of defense-in-depth and diversity (D3) analyses in a cost-efficient way. Targeting at the complexity of redundant designs in safety-related digital I&C systems, this approach integrates systems-theoretic process analysis (STPA) (Leveson and Thomas March 2018), fault tree analysis (FTA) and Hazard and Consequence Analysis for Digital Systems (HAZCADS) (Clark, et al. 2018) to identify software CCFs effectively by reframing STPA in a redundancy-guided way: (1) framing the complexity of the redundancy problem in a detailed representation; (2) clarifying the redundancy level using FTA before applying STPA; (3) building a redundancy-guided multilayer control structure; and (4) locating software CCFs for different levels of redundancy. This approach has been demonstrated and applied for the hazard analysis of a four-division digital RTS (Shorthill, et al. 2020) and a four-division, digital, engineered safety features actuation system (Bao, Shorthill and Zhang, Hazard Analysis for Identifying Common Cause Failures of Digital Safety Systems using a Redundancy-Guided Systems-Theoretic Approach 1 December 2020).

The second part in risk analysis is reliability analysis with the tasks of: (1) quantifying the probabilities of basic events of the integrated FT from the hazard analysis; (2) determining the optimal basic component combinations for prevention and mitigation; and (3) estimating the probabilities of the consequences of digital system failures. The respective acceptance criterion is defined as, "How reliable is the digital system with the identified digital failures existing?" According to Bao, Zhang, and Thomas, quantification of failure probabilities is the main outcome for both single failure events and consequences (Bao, Zhang and Thomas, An Integrated Risk Assessment Process for Digital Instrumentation and

Control Upgrades of Nuclear Power Plants 2019). For different designs and requirements from licensing regulators, the set point for reliability probability should integrate the efforts and experiences from industry, regulators, and researchers. Bayesian networks and CCF modeling methods are incorporated to estimate the failure probabilities of basic events, particularly the software CCFs.

As the third and final part, consequence analysis should be implemented to evaluate the impact of consequences of digital failures on plant responses. The respective acceptance criterion is defined as, "Are the consequences of individual digital failures acceptable at the plant level?" The main concern is that some software failures have the potential to initiate an unanalyzed event or scenario and, therefore, to create a threat to reactor safety, such as by core damage or a large early release. The PRA results from the previous reliability analyses are supposed to provide different risk-significant accident scenarios for the multi-physics best-estimate plus uncertainty analysis. The capability has been built by different platforms such as the INL-developed LOTUS (Zhang, et al. September 2018).

3 REDUNDANCY-GUIDED SYSTEM-THEORETIC HAZARD ANALYSIS

To deal with the complexity problem of redundancy and identify software CCFs effectively, the system-theoretic hazard analysis is proposed to integrate and reframe the STPA process in a redundancy-guided way as a seven-step process. The key outcomes of which are an integrated FT, including software failures and hardware failures, identified CCFs, and minimal cut sets to discover the single points of failure (SPOFs) leading to the loss of function of the entire digital system. SPOF refers to a situation in which a single part of a system fails, and the entire system loses function as a result. The proposed RESHA approach is illustrated in Figure 2. The steps of the RESHA approach are briefly described below.

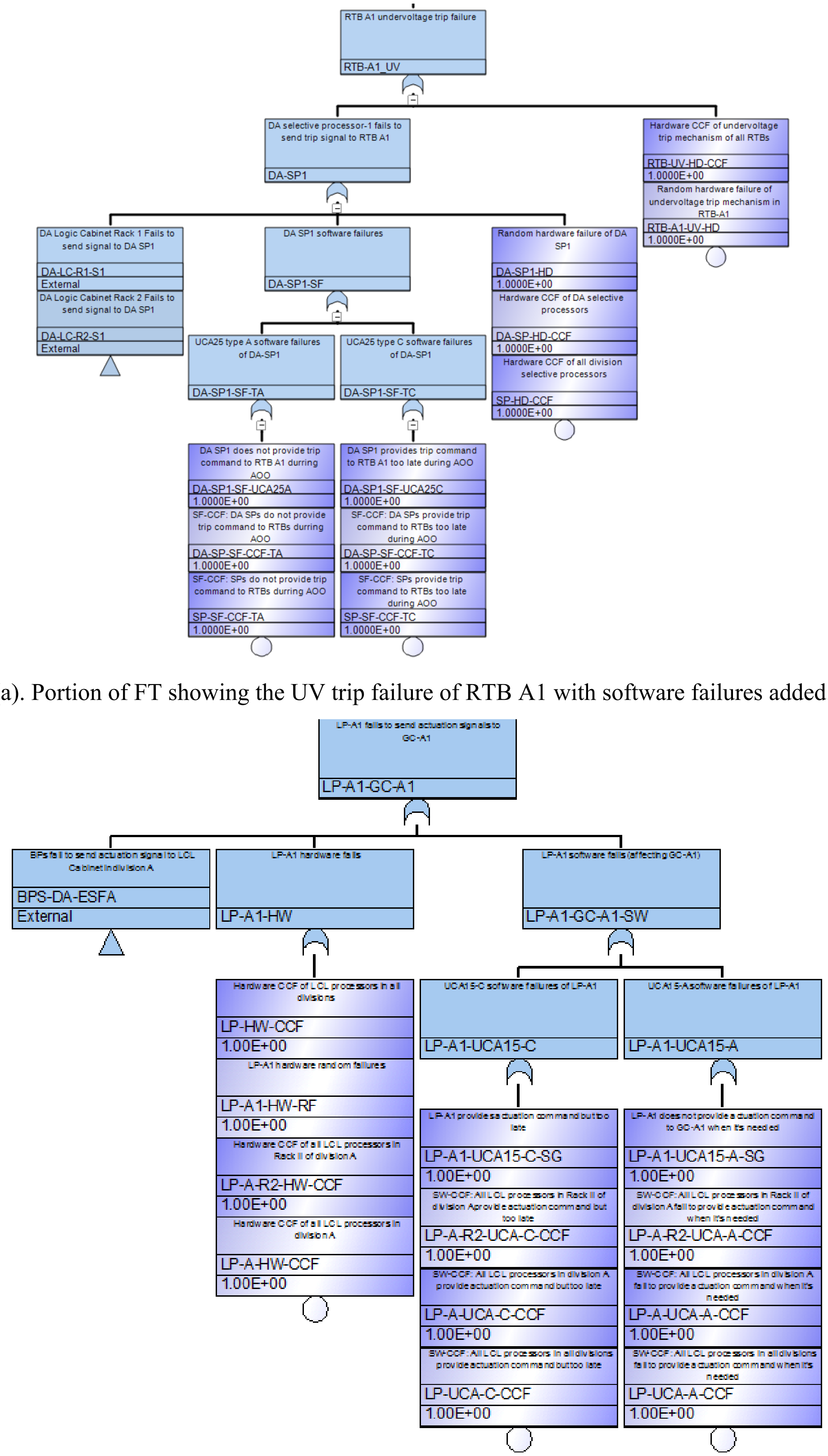
Figure 2. Workflow of the proposed RESHA approach.

The purpose of Step 1 is to establish a system sketch to serve as a blueprint for the hazard analysis. This is done by gathering system design information, including wiring, piping and instrumentation diagrams, existing logic diagrams, etc. This information is then used to create a system sketch, the main goal being to map out the processors, sensors, controllers, components, interactions, and connections of the system. The point of this step is not to necessarily fit everything into one diagram, but to gain a sufficient understanding of the system in order to complete the hazard analysis; the level of detail provided in this step lays out the foundation for the work. Based on the hardware representation created in Step 1, a FT is developed in this step to include hardware failures to the detailed level required for representing the loss of functions. For analysis of a digital system with redundancy designs, the structure of a hardware FT should follow the levels of redundancy from the division to the unit and to the module levels. This kind of redundancy-guided structure makes it convenient to add in a software failure identified in the next step. The probability quantification of each basic event is not required in this step and will be performed in the integrated reliability analysis. The main assumption for this step is that all software failures will be captured using STPA in Step 3. Therefore, only hardware failures will be included in FT.

In Step 3, part of the STPA process is applied to identify the unsafe control actions (UCAs) as potential software failures. There are four types of UCAs in STPA: (1) Control action is not provided when it is needed; (2) Control action is provided when it is not needed; (3) Control action is provided when it is needed, but too early, too late, or in a wrong order; (4) Control action lasts too long or stops too soon (only applicable to continuous control actions). In a digital system, all information exchanges—including the decision-making process of the controllers, control and implementation of control actions, performance of controlled process, and feedbacks from controlled process—have the potential to fail the function of the digital system when it is needed or send spurious signals that are not needed. These systematic failures could be initiated by the UCAs as a result of an unrealistic process model, an inappropriate control algorithm, an incorrect feedback, or outside information. Therefore, the potential software failures can be understood and analyzed by identifying these UCAs. To deal with the complexity problem of redundancy and to identify software CCFs effectively, control structure is built in a redundancy-guided way. The redundancy-guided multilayer control structure zooms in on systematic information exchanges on each redundancy level because CCFs are tightly connected with redundancy designs. Each control structure layer is created with numbered control actions and feedback signals until a final, redundancy-guided, multilayer control structure is created for the complete system of interest. In Step 4, applicable UCAs are selected and added into the hardware FT as the software failures. For a specific top event in the FT, some UCAs may be inapplicable. For example, if the top event of hardware FT is "ESFAS fails to actuate ESF components," Type 2 and 4 of UCAs are inapplicable since the control action of "sending actuation command" is needed, which is not a continuous action. If the top event is "unexpected actuations by ESFAS," only Type 2 is applicable. Considering the hardware FT and redundancy-guided multilayer control structure are tightly connected and consistent with each other, these applicable UCAs (software failures) can be incorporated into the hardware FT in parallel with the respective hardware failures.

After integrating UCAs into the hardware FT, the same types of UCAs, located in the same redundancy level, can be separated into independent failures and CCFs. In Step 5, software CCFs can be classified into different types depending on the redundancy levels: (1) software CCFs occurring in all divisions; (2) software CCFs occurring in all of the units in one division; and (3) software occurring in all of the modules in one unit. The classification of software CCFs depends on the software diversity of the digital system. In Step 6, as the main outcome of the systematic-theoretic hazard analysis, the minimal cut sets of the integrated FT should be calculated and evaluated to determine how many potential SPOFs have been added by considering the software failures. If the digital system has a low level of software diversity, the software CCFs occurring in all divisions could lead directly to the top event (e.g., the loss of function of the entire digital system), regardless of the contributions from other safety designs. Step 7 identifies and provides guidance to eliminate latent faults or triggers of CCFs.

Currently, RESHA has been demonstrated for the hazard analysis of a four-division digital RTS and ESFAS, which have similar structures to state-of-the-art digital systems in existing NPP designs (APR1400 Desing Control Document Tier 2. Chapter 7: Instrumentation and Controls 2018). Portions of FT for RTS and ESFAS failures with software failures are displayed in Figure 3. More details can be found in (Bao, Shorthill and Zhang, Hazard Analysis for Identifying Common Cause Failures of Digital Safety Systems using a Redundancy-Guided Systems-Theoretic Approach 1 December 2020) and (Shorthill, et al. 2020).


RTB A1 undervoltage trip failure
RTB-A1_UV
DA selective processor-1 fails to send trip signal to RTB A1
DA-SP1
Hardware CCF of undervoltage trip mechanism of all RTBs
RTB-UV-HD-CCF
1.0000E+00
Random hardware failure of undervoltage trip mechanism in RTB-A1
RTB-A1-UV-HD
1.0000E+00
DA Logic Cabinet Rack 1 Fails to send signal to DA SP1
DA-LC-R1-S1
External
DA Logic Cabinet Rack 2 Fails to send signal to DA SP1
DA-LC-R2-S1
External
DA SP1 software failures
DA-SP1-SF
Random hardware failure of DA SP1
DA-SP1-HD
1.0000E+00
Hardware CCF of DA selective processors
DA-SP-HD-CCF
1.0000E+00
Hardware CCF of all division selective processors
SP-HD-CCF
1.0000E+00
UCA25 type A software failures of DA-SP1
DA-SP1-SF-TA
UCA25 type C software failures of DA-SP1
DA-SP1-SF-TC
DA SP1 does not provide trip command to RTB A1 durring AOO
DA-SP1-SF-UCA25A
1.0000E+00
SF-CCF: DA SPs do not provide trip command to RTBs durring AOO
DA-SP-SF-CCF-TA
1.0000E+00
SF-CCF: SPs do not provide trip command to RTBs durring AOO
SP-SF-CCF-TA
1.0000E+00
DA SP1 provides trip command to RTB A1 too late during AOO
DA-SP1-SF-UCA25C
1.0000E+00
SF-CCF: DA SPs provide trip command to RTBs too late during AOO
DA-SP-SF-CCF-TC
1.0000E+00
SF-CCF: SPs provide trip command to RTBs too late during AOO
SP-SF-CCF-TC
1.0000E+00

(a). Portion of FT showing the UV trip failure of RTB A1 with software failures added.

LP-A1 fails to send actuation signals to GC-A1
LP-A1-GC-A1
BPs fail to send actuation signal to LCL Cabinet in division A
BPS-DA-ESFA
External
LP-A1 hardware fails
LP-A1-HW
LP-A1 software fails (affecting GC-A1)
LP-A1-GC-A1-SW
Hardware CCF of LCL processors in all divisions
LP-HW-CCF
1.00E+00
LP-A1 hardware random failures
LP-A1-HW-RF
1.00E+00
Hardware CCF of all LCL processors in Rack II of division A
LP-A-R2-HW-CCF
1.00E+00
Hardware CCF of all LCL processors in division A
LP-A-HW-CCF
1.00E+00
UCA15-C software failures of LP-A1
LP-A1-UCA15-C
UCA15-A software failures of LP-A1
LP-A1-UCA15-A
LP-A1 provides actuation command but too late
LP-A1-UCA15-C-SG
1.00E+00
SW-CCF: All LCL processors in Rack II of division A provide actuation command but too late
LP-A-R2-UCA-C-CCF
1.00E+00
SW-CCF: All LCL processors in division A provide actuation command but too late
LP-A-UCA-C-CCF
1.00E+00
SW-CCF: All LCL processors in all divisions provide actuation command but too late
LP-UCA-C-CCF
1.00E+00
LP-A1 does not provide actuation command to GC-A1 when it's needed
LP-A1-UCA15-A-SG
1.00E+00
SW-CCF: All LCL processors in Rack II of division A fail to provide actuation command when it's needed
LP-A-R2-UCA-A-CCF
1.00E+00
SW-CCF: All LCL processors in division A fail to provide actuation command when it's needed
LP-A-UCA-A-CCF
1.00E+00
SW-CCF: All LCL processors in all divisions fail to provide actuation command when it's needed
LP-UCA-A-CCF
1.00E+00

(b). Integrated FT for “LP-A1 fails to send actuation signals to GC-A1,” with relevant software failures added.

Figure 3. Portions of FT for RTS (a) and ESFAS (b) failures with software failures

4 INTEGRATED RELIABILITY ANALYSIS

The BAHAMAS workflow is discussed in this section, where each of the main methods mentioned in the approach is incorporated for the reliability analysis of a software system. As discussed in Section 1, the risk assessment of digital systems has been divided into three phases. Phase 2 provides quantification for the results found in Phase 1. Although it is the intention in Phase 2 for BAHAMAS to be flexible, much of its formulation is based on the results of a RESHA-based Phase 1 hazard analysis. Consequently, the subsequent approach to Phase 2 is tailored best to hazards identified by RESHA. BAHAMAS workflow and information flow are shown in Figure 4 and Figure 5, respectively.

Figure 4. BAHAMAS workflow.

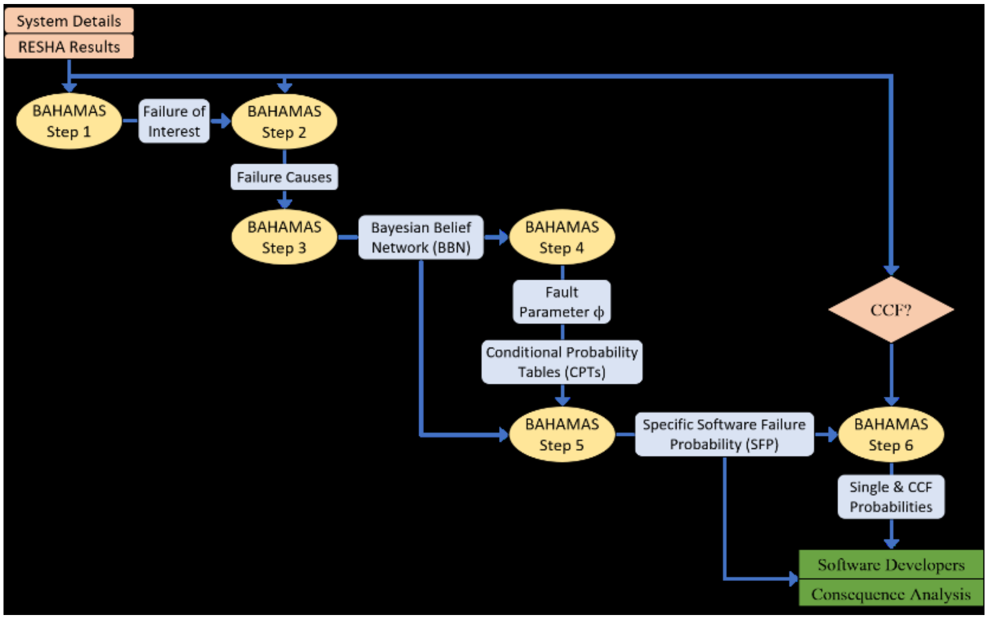


Figure 5. Flowchart showing the primary inputs and outputs of each step of BAHAMAS.

Step 1 of BAHAMAS is to select an event needing to be quantified from a qualitative study. This step assumes that some previous hazard identification work has been completed. The event of interest should include details of the controller, CA, and context. The purpose of Step 2 is to collect and organize information regarding the event of interest. In Step 1, the specific controller, action, and context of the event should have been identified. The analyst should then determine the dependencies, inputs, outputs, and components of the controller. Emphasis should be made to include all the components of the controller that have software or integrated software (firmware). Step 3 is focused on creating a Bayesian belief network (BBN) based on the causes identified in Step 2. The main idea of the BBN is to create an acyclic (i.e., without feedback) graphical network representing the relationships of interest. In this case, this means the relationships between root causes and probability of software failure. Step 4 determines the fault parameter by estimating the root node probabilities and generic software failure probability. Step 5 determines the probability for failure of interest by estimating specific software failure probability and evaluating single and CCF probability. A case study has been performed; more details can be found in future publications.

5 CONCLUSIONS AND FUTURE WORK

5.1 Conclusions

This work has provided a means to overcome technical challenges faced by the nuclear industry for the implementation of DI&C systems. A modularized approach to conduct RESHA for DI&C systems has been developed and demonstrated based on an advanced digital RTS and ESFAS with multilevel redundancy designs. Systematic methods and risk-informed tools are incorporated to address both hardware and software CCFs, which provide guidance to eliminate the causal factors of potential SPOFs in the design of digital safety systems in advanced plant designs. RESHA provided a means to identify software-based interactions and potential CCFs in highly redundant, state-of-the-art DI&C systems by fully incorporating redundancy into the hazard analysis process.

Embracing redundancy in the analysis allowed RESHA to meet its objectives in three ways: (1) defining a step-by-step approach for the hazard analysis of digital systems that can help engineers efficiently make design and risk mitigation decisions by providing them a means to systematically identify the most critical CCFs and hazards of DI&C systems; (2) identifying the critical hazards of a system, thereby allowing utilities to effectively manage the cost of safety-rated DI&C by strategically eliminating unnecessary design features; and (3) providing a technical basis for reliability analysis by identifying crucial failure modes and qualitatively determining their effects on system vulnerability. Ultimately, RESHA helps improve the design of highly redundant DI&C through a detailed qualitative hazard analysis.

The method also provides a technical basis for implementing cybersecurity, reliability, and consequence analysis on unanalyzed sequences and optimizing the use of DiD analysis in a cost-effective way. The application of RESHA requires users to have sufficient knowledge of relevant methods (e.g., FTA, STPA) and target systems. The identification of causal factors requires collaborations with relevant expert teams, such as system/software designers and engineers and human reliability analysts.

In addition, this work developed a novel method, BAHAMAS, for reliability analysis of DI&C systems. Software failure probabilities are quantified using an integrated approach that incorporates state-of-the-art BBN, HRA, and CCF modeling techniques. BAHAMAS also provides a means for analyzing new software systems where operational data is rarely available, as well as flexibility allowing an analyst to employ appropriate HRA methods or incorporate new or advanced methods to capture the desired details of any software development life cycle (SDLC). The case study relied on the use of THERP for the quantification of faults in the SDLC. THERP, while a classic and well-used method, is aging. Other HRA methods may prove to be better suited for the evaluation of SDLC. CREAM's applications for cognitive aspects, as well as SPAR-H's rapid quantification abilities, also present attractive investigations for future research. BAHAMAS has the potential to meet many of these attributes. By providing a clear method and allowing for flexibility in the use of HRA, the door has been opened to allow for reasonable assumptions for case-specific analysis. The method accounts for lifecycle activities and provides consideration for CCFs. Despite coming up short for verification and uncertainty, the method has the potential to undergo such actions. In addition, reliance on previous experience is flexible (e.g., may not require significant testing), and validation efforts would help clarify how much previous test experience is really required. Finally, some of the assumptions for the case study precluded the consideration of operational conditions; however, BAHAMAS can certainly incorporate environmental and other fault contributors into the BBN. Additionally, operational considerations—particularly, the interactions between the digital system and controlled processes—are partially accounted for by consideration of the process model and control algorithm. The process model and control algorithm account for relationships between various attributes of the control system and are used for the HRA analysis. In conclusion, BAHAMAS provides a flexible and useful tool for the quantification of DI&C system software failures and meets many of the desired attributes of an ideal quantitative software reliability analysis method.

5.2 Future Work

One area for future research of LWRS-RISA is to deal with the risk analysis for the Human System Interface (HSI) in DI&C modernization of existing NPPs. The HSI is one of the key advanced design features applied for modern DI&C systems of NPPs. Normally, it is designed based on a compact workstation-based system in the control room. The compact workstation provides a convenient operating environment to facilitate the display of plant status information to the operator so that operability is enhanced by using advanced display, alarm, and procedure systems. The HSI should have sufficient diversity to demonstrate DiD protection against CCF of the safety system. However, the vulnerability of HSI is affected by many factors, human errors, cyber-attacks, software CCFs, etc. Therefore, this work aims to identify, evaluate, and reduce these system vulnerabilities to support the licensing, deployment, and operation of the HSI designs.

Another future area for research is collaboration with industry partners and other programs to complete reliability studies and perform consequence analysis for state-of-the-art DI&C systems. An integrated reliability study and risk-informed consequence analysis will be performed for a representative digital RTS and ESFAS of existing plants with software CCFs and plant responses considered. This work complements other approaches being developed for deploying DI&C technologies and provides risk-informed insights to facilitate the adoption and licensing of safety-related and non-safety-related DI&Cs.

The third possibility for future work is uncertainty quantification and verification of RESHA and BAHAMAS. Finally, by integrating hazard analysis, reliability analysis, and consequence analysis together, the risk assessment strategy aims to: (1) help system designers and engineers to systematically address digital-based CCFs and quantitatively analyze their effects on digital system vulnerability and key plant responses; (2) improve existing PRA models for the industry by identifying and evaluating the risk associated with DI&C technologies; and (3) provide risk insights to address the licensing challenges facing DI&C upgrades.

6 ACKNOWLEDGMENTS

This submitted manuscript was authored by a contractor of the U.S. Government under DOE Contract No. DE-AC07-05ID14517. Accordingly, the U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. Government purposes. This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

7 REFERENCES

Aldemir, T., et al. *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments.* Ohio State University, Washington, DC: NUREG/CR-6901, U.S. Nuclear Regulatory Commission, 2006.

APR1400 Desing Control Document Tier 2. Chapter 7: Instrumentation and Controls. South Korea: Korea Electric Power Corporation; , Korea Hydro & Nuclear Power Co., Ltd;, 2018.

Bao, Han, Hongbin Zhang, and Kenneth Thomas. *An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants.* Idaho Falls, ID: Idaho National Laboratory, 2019.

Bao, Han, Hongbin Zhang, and Kenneth Thomas. *An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants.* Idaho Falls, ID: Idaho National Laboratory, 2019.

Bao, Han, Tate Shorthill, and Hongbin Zhang. "Hazard Analysis for Identifying Common Cause Failures of Digital Safety Systems using a Redundancy-Guided Systems-Theoretic Approach." *Annals of Nuclear Energy,* 148 (1 December 2020): 107686.

Chu, Tsong-Lun, Meng Yue, Gerardo Martinez-Guridi, and John Lehner. *Review of Quantitative Software Reliability Methods.* Brookhaven National Laboratory, 2010.

Clark, Andrew J., Adam D. Williams, Alice Muna, and Matt Gibson. "Hazard and Consequence Analysis for Digital Systems – A New Approach to Risk Analysis in the Digital Era for Nuclear Power Plants." *Transactions of the American Nuclear Society.* Orlando, Florida, USA, 2018. 11-15.

Hashemian, H.M. "Nuclear Power Plant Instrumentation and Control." In *Nuclear Power - Control, Reliability and Human Factors*, edited by Pavel Tsvetkov, 49-66. Intech, 2011.

Kirschenbaum, Jason, et al. "A Benchmark System for Comparing Reliability Modeling Approaches for Digital Instrumentation and Control Systems." *Nuclear Technology* 165, no. 1 (2009): 53-95.

Leveson, Nancy G., and John P. Thomas. *STPA Handbook.* March 2018.

National Research Council. *Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues.* Washington, DC: The National Academies Press, 1997.

NRC, U.S. *Plans for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls.* Washington, D.C.: U.S. NRC, 2018.

Shorthill, Tate, Han Bao, Hongbin Zhang, and Heng Ban. "A Redundancy-Guided Approach for the Hazard Analysis of Digital Instrumentation and Control Systems in Advanced Nuclear Power Plants." *arXiv.org*, 2020.

Thomas, Ken, and Ken Scarola. *Strategy for Implementation of Safety-Related Digital I&C Systems.* Idaho National Laboratory, Idaho Falls: Idaho National Laboratory, 2018.

U.S. Nuclear Regulatory Commission. *A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System.* Washington, DC: U.S. Nuclear Regulatory Commission, 1979.

U.S.NRC. *Historical Review and Observations of Defense-in-Depth.* Washington, D.C.: U.S. NRC, 2016.

U.S.NRC. *Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure* . Washington, D.C.: U.S.NRC, 2019.

U.S.NRC. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition — Instrumentation and Controls.* Washington ,D.C.: U.S.NRC, 2016.

U.S.NRC. *Use of Probabilistic Risk Assessment Methods in Nuclear.* Washington, D.C.: U.S.NRC, 1995.

Wierman, T. E., D. M. Rasmuson, and A, Mosleh. *Common-Cause Failure Databased and Analysis System: Event Data Collection, Classification, and Coding.* Idaho Falls, ID: NUREG/CR-6268, Rev. 1, Idaho National Laboratory, 2007.

Zhang, Hongbin, Ronaldo Szilard, Stephen Hess, and Rosemary Sugrue. *A Strategic Approach to Employ Risk-Informed Methods to Enable Margin Recovery of Nuclear Power Plants Operating Margins.* Idaho Fall,s ID: Idaho National Laboratory, September 2018.