INL/CON-19-56636-Revision-0

Hazard Analysis of Digital Engineered Safety Features Actuation System in Advanced Nuclear Power Plants Using a Redundancy-Guided Approach

August 2020

Han Bao, Hongbin Zhang, Tate Shorthill

Changing the World's Energy Future

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

INL/CON-19-56636-Revision-0

Hazard Analysis of Digital Engineered Safety Features Actuation System in Advanced Nuclear Power Plants Using a Redundancy-Guided Approach

Han Bao, Hongbin Zhang, Tate Shorthill

August 2020

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

Proceedings of the ASME 2020
International Conference on Nuclear Engineering
ICONE28-POWER2020
August 2-6, 2020, Anaheim, CA, USA

ICONE28-POWER2020-10381

HAZARD ANALYSIS OF DIGITAL ENGINEERED SAFETY FEATURES ACTUATION SYSTEM IN ADVANCED NUCLEAR POWER PLANTS USING A REDUNDANCY-GUIDED APPROACH

Han Bao[1], Tate Shorthill[2], Hongbin Zhang[1]

[1] Idaho National Laboratory, Idaho Falls, ID
[2]University of Pittsburgh, Pittsburgh, PA

ABSTRACT

Replacing the existing aging analog instrumentation and control (I&C) systems with modern safety control and protection digital technology offers one of the foremost means of performance improvements and cost reductions for the existing nuclear power plants (NPPs). However, the qualification of digital I&C systems remains a challenge, especially considering the issue of software common-cause failures (CCFs), which are difficult to address. With the application and upgrades of advanced digital I&C systems, software CCFs have become a potential threat to plant safety because most redundant designs use similar digital platforms or software in the operating and application systems. With complex designs of multilayer redundancy to meet the single-failure criterion, digital I&C safety systems (e.g., engineered safety-features actuation system [ESFAS]) are of a particular concern in the U.S. Nuclear Regulatory Commission (NRC) licensing procedures. This paper applies a modularized approach to conduct redundancy-guided systems-theoretic hazard analysis for an advanced digital 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 triggers of potential single points of failure in the design of digital safety systems in advanced plant designs.

Keywords: Common cause failure, digital safety system, redundancy-guided, hazard analysis

1. INTRODUCTION

Most existing nuclear power plants (NPPs) rely on traditional analog instrumentation and control (I&C) systems for monitoring, control, and protection functions. In addition to susceptibility to certain environmental conditions, the primary concern with extended analog systems arises from the effects of aging.[1] With the industrial base largely moving to digital systems, the operation and maintenance of NPPs involves managing issues, including the lack of needed analog spare parts, increasing maintenance costs, and the loss of vendor support. Compared with existing analog I&C systems, digital I&C systems have significant functional advantages, such as reliable system performance in terms of accuracy and computational capability, high data-handling and storage capabilities to fully measure and display operating conditions, and improved capabilities.[2] Therefore, in the last few years, the United States (U.S.) nuclear power industry initiates replacement of existing aging analog systems with digital I&C technology and develops new designs for advanced plants using digital I&C systems in integrated control rooms to provide modern control and protection systems.

In 1997, the National Research Council listed several challenges to successfully implement these new digital I&C systems into existing NPPs.[1] Considering that the application of new digital technology also introduces new potential software-based hazards in critical safety and control functions, underlying technical infrastructure and regulatory frameworks require some changes because much of the experience from analog technology may not be suitable for the applications of digital I&C. Some technical problems have been identified from the applications of digital I&C in NPPs, such as common-cause failure (CCF) in software, commercial dedication of hardware and software, and the possible lack of on-site plant experience with the new technology and systems. Meanwhile, the licensing process for regulatory review and approval for digital I&C systems and modifications to existing systems is difficult, time-consuming, and largely customized for different designs because the industry and regulators have less experience with this new technology. The process is further hampered by a lack of consensus on issues underlying the evaluation and adoption of digital I&C technology. To be consistent with defense-in-depth (DiD) principles,[3] some independent and redundant safety systems are designed to initiate automatic actions to prevent and mitigate accident conditions if non-safety systems fail to maintain the plant

within normal operating conditions. Therefore, these I&C safety systems, such as engineered safety features (ESF) systems, are of a particular concern in U.S. Nuclear Regulatory Commission (NRC) licensing procedures.

For these reasons, the nuclear industry and regulators have concentrated considerable efforts on addressing the technical and regulatory aspects of digital qualifications, especially digital-based CCFs. CCFs have the potential to generate an unanalyzed event or sequence that may not be bounded by previous plant-accident analyses and, thus, to challenge plant safety.[4] A general conclusion from probabilistic risk assessments (PRAs) of commercial NPPs is that CCFs are significant contributors to the unavailability of safety systems.[5] Existing analyses on CCFs in I&C systems mainly focus on hardware failures. With the application of and upgrades to new digital I&C systems, software CCFs due to design defects in software, environmental hazards, and human errors have become a potential threat to plant safety because a major part of redundancy designs use similar digital platforms or software in the operating and application systems.

To deal with these challenges, the NRC has begun an update to its regulatory infrastructure and processes, starting in the late 1990s. NUREG/CR-6303 was published by the NRC in December 1994 as "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems." In it, a method was described to identify design vulnerabilities to common-mode failure for computer-based nuclear-reactor protection systems.[3] In October 1995, the NRC called attention to top-level system aspect requirements of digital I&C applications in NPPs, which were addressed in the general design criteria in Title 10 of the Code of Federal Regulations (CFR) 50, Appendix A.[6] NUREG/CR-6734 Vols.1 and 2, published in 2001, provided guidance for reviewing high-integrity software requirements documents in NPPs, which contained a set of 45 failures that illustrate the need for and importance of specific requirements-review guidelines.[7] NUREG/CR-7007, published in 2008 as "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," provided guidance to determine how much diversity in a safety system is needed to mitigate the consequences of potential CCFs identified in the evaluation of safety-system design features.[8] Next, some general observations on the consistencies and inconsistencies in how DiD has been defined and used were included in NUREG/KM-0009, "Historical Review and Observations of Defense-in-Depth."[9] In 2016, the NRC revised the Standard Review Plan (SRP) to fully adapt it and the associated regulatory guides to digital I&C systems.[10] Chapter 7 of the SRP provided guidance for the review of the I&C portions of (1) applications for nuclear reactor licenses or permits and (2) amendments to existing licenses.

Diversity and DiD analyses are proposed and performed using deterministic approaches while the NRC PRA policy statement encourages the use of risk information in all regulatory activities supported by the state of the art and data.[11] 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. Furthermore, deterministic guidance available in Chapter 7 of the SRP does not consider digital-system reliability quantitatively as part of determining the acceptability of a digital system for safety applications.[12] Currently, NRC continues to perform research that supports the development of licensing criteria to evaluate new digital I&C systems. According to guiding principles in SECY-18-0090,[13] 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, the NRC staff developed the Integrated Action Plan (IAP),[14] and it updates the plan as a living document. One of the goals of the IAP is to assist the 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.[14]

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. In 2019, Idaho National Laboratory (INL) initiated a project under the Risk-Informed Systems Analysis (RISA) Pathway of the U.S. Department of Energy's (DOE's) Light Water Reactor Sustainability (LWRS) program to develop a risk-assessment strategy for delivering a strong technical basis to support effective, licensable, and secure digital I&C technologies for digital upgrades/designs.[15] An integrated risk-assessment for digital I&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. According to the guidelines and requirements of the RADIC process, a redundancy-guided systems-theoretic approach was developed for hazard analysis that 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 was developed and previously applied for the hazard analysis of digital reactor-trip systems.[16,17]

Section 2 reviews technical approaches for hazard analysis of NPPs, and Section 3 describes the proposed approach for redundancy-guided systems-theoretic hazard analysis (RESHA). The application of the RESHA approach on an advanced digital ESFAS with complex, redundant, and diverse designs is illustrated in Section 4. Section 5 summarizes the main findings, conclusions, and future works.

2. TECHNICAL APPROACHES

For a digital-based I&C system, the failure of the I&C function results from either a hardware or a software failure. There are two types of digital systems in an NPP: non-safety systems, such as the feedwater control system, and safety systems, such as the RPS. Traditional failure-mode effect analysis (FMEA) or fault-tree analysis (FTA) has been widely applied to identify the hardware failure modes. However, the interactions between the digital systems and the rest of the plants, and the interactions between the internal components of one digital system and other digital systems often result in new systematic failure modes that are difficult to discover using FMEA or FTA.[12] A major concern in the licensing of new digital designs is the uncertainty and potential risk resulting from CCFs in I&C software, particularly in digital safety systems, which have multilayer redundant divisions, units, and modules compared to non-safety systems. NRC staff reviews of failure modes provided in [18] have observed, "FMEA does not address CCF when a CCF is rooted in some systemic cause such as an engineering deficiency, it is pervasive (i.e., its effects cannot be pinpointed or isolated, but could occur at many hard-to-find places)."

Several factors lead to many successful methods for analyzing failure modes in traditional analog systems not applicable to identifying the software hazards in digital systems. First, software does not fail randomly, as does hardware. Software can be designed and programmed without any physical support needed. Generally, software failures are systematic; however, a software fault can be activated into a software failure by a random hardware failure. Besides, the failure modes of digital systems are different from analog ones. Because redundant designs in digital systems use identical software or digital platforms, redundant designs are not effective. They can fail due to the same design defects or changes in the operational environment. In fact, most of the serious accidents caused by software issues have involved defects in the requirements, not in the implementation process of these requirements.[19] Software performs correctly in the sense that it successfully conducts its requirements, but the requirements themselves may be unsafe due to their incompleteness. Besides, the undocumented assumptions made during the original development of software may be inappropriate for the unexpected new conditions in the operating environment. Considering that software failure may be triggered by a random hardware failure, the requirements for hardware reliability should also be reconsidered and be more rigorous than the ones in analog systems.

Therefore, in this proposed RESHA approach, a relatively new hazard-analysis method, systems-theoretic process analysis (STPA), is applied to identify the software failures for digital I&C systems. In 2012, STPA was applied to evaluate the safety of a digital main steam-isolation valve in an evolutionary power reactor (EPR).[20] STPA describes how undesired outcomes (e.g., losses) can result from inadequate enforcement of constraints (e.g., controls) on the design, development, and operation of systems to achieve desired objectives. After the identification of software failures, especially software CCFs, another method called hazard and consequence analysis for digital systems (HAZCADS) is applied to construct an integrated FT by adding applicable software failures as basic events into the existing hardware FT. HAZCADS is a recent advancement in hazard analysis by combining FTA and STPA, which is developed jointly by EPRI and Sandia National Laboratories.[21]

Both STPA and HAZCADS are general guidelines for the identification of software failures and the construction of an integrated FT. Both have been applied for safety and security analysis; however, they do not provide details to deal with the complexity of redundant design in the application process, which is greatly applied in digital safety systems such as ESFAS. To deal with the complexity problem of redundancy and identify software CCFs effectively, STPA is reframed in a redundancy-guided way, which is represented in (1) framing the complexity of 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.

3. METHODS

To deal with the complexity problem of redundancy and identify software CCFs effectively, the system-theoretic hazard analysis is proposed to integrate and reframe 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 the 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 1. The steps of the RESHA approach are briefly described in this paper, and more details can be found in [17].

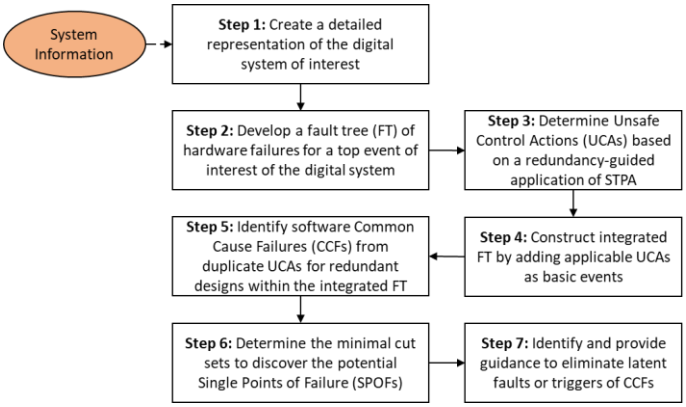

Figure 1. Workflow of the proposed RESHA approach

Step 1: Create a detailed hardware representation of the digital system of interest.

In this step, detailed information on the structure and functions of the digital system of interest should be collected, gathered, and classified. Normally, a digital I&C system has a three-level hierarchical architecture[22]: (1) divisions that process the signal path from sensor to actuator level (2) units that perform a specific task by using several modules (e.g., an acquisition and processing unit or a voter unit), and (3) modules that realize a specific part of the function processing (e.g., input/output modules, processors). The representation should contain information on hardware structure and be created to a detailed level that captures sufficient design information affecting system function and reliability. In this work, most efforts on hazard identification and reliability modeling reach to the level of modules, which is the smallest hardware component to implement a specific part of the entire function processing independently. Besides, based on the requirements and purposes of risk-analysis phase, practical assumptions and reasonable simplifications of the hardware representation should be stated and explained. The representation figure should clearly display the information flow between different divisions, units, and modules. For the analysis on digital systems with redundancy designs, the complexity of redundancy should be illustrated. It builds the basis for the construction of hardware FTs and redundancy-guided multilayer control structure.

Step 2: Develop an FT of hardware failures for a top event of interest of the digital system.

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. the structure of a hardware FT should follow the levels of redundancy from the division to the unit and to module level. The probability quantification of each basic event is not required in hazard analysis.

Step 3: Determine Unsafe Control Actions (UCAs) based on a redundancy-guided application of STPA.

In this step, part of the STPA process is applied to identify the UCAs as potential software failures. First, based on the requirements and purposes specified in Step 1, key losses and system-level hazards are identified. In STPA, a loss impacts something of value to stakeholders or the public (e.g., a loss of human life or a human injury, property damage, environmental pollution, or any other loss that is unacceptable). A hazard is defined as, "a system state or state or setoff conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss." The identification of hazards is tightly connected to the function and operating requirements of the system of interest.

Second, according to the redundancy information in the hardware FT, a redundancy-guided multilayer control structure is modeled. A control structure is defined as, "a system model composed of feedback control loops," which illustrates the interactions between controllers and a controlled process, including sensors and actuators. A generic control loop is shown in Figure 2. Generally, controllers provide control actions to conduct certain processes. A controller includes control algorithms representing a controller's decision-making process while a process models that represents the controller's internal criteria used for its decision-making. The actions provided by a controller can be influenced by the controller's process models, control algorithms, and feedbacks.

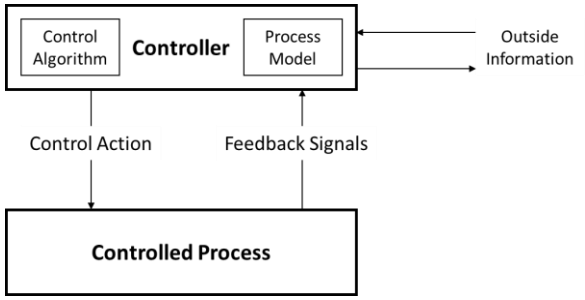

Figure 2. A generic control structure in the STPA application

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 a 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.

Third, the UCAs are identified according to the multilayer control structure and specified hazards. A UCA is defined as, "a control action that, in a particular context and worst-case environment, will lead to a hazard." There are four types of UCAs in an STPA:

UCA-a: Control action is not provided when it is needed.
UCA-b: Control action is provided when it is not needed.
UCA-c: Control action is provided when it is needed, but too early, too late, or in a wrong order.
UCA-d: Control action lasts too long or stops too soon (only applicable to continuous control actions).

The specification of the context for UCAs is important, usually words like "when," "while," or "during" are used to define the context. The UCA context should represent an actual

or true condition that would make the control action unsafe, not a controller process model that may or may not be true.

Step 4: Construct an integrated FT by adding applicable UCAs as basic events.

In this step, applicable UCAs are added into the hardware FT as the software failures. For a specific top event, 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, and 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 FT in parallel with the respective hardware failures.

Step 5: Identify software CCFs from duplicate UCAs for redundant designs within the integrated FT.

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. Additionally, 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. As one of the guidelines for the DiD analysis, software diversity should be considered. Software diversity is defined as, "the use of different programs designed and implemented by different development groups with different key personnel to accomplish the same safety goals-for example, using two separately designed programs to compute when a reactor should be tripped."[3] Therefore, before the identification of software CCFs, the level of software diversity should be one of the key assumptions to guide the classification of software CCFs.

Step 6: Determine the minimal cut sets to discover the potential SPOFs.

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 CCF types 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. As a part of risk analysis, hazard analysis directly provides evidence to evaluate the question, "Does the individual digital failure lead to the loss of function of the digital system?" If the individual digital failure is one of the SPOFs, a redesign request will be made for system designers and engineers based on the risk evaluation results.

Step 7: Identify and provide guidance to eliminate latent faults or triggers of CCFs.

A dormant fault does not affect safety before a triggering condition or event activates it to a failure. Triggers include plant transients, initiating events, external conditions, interactions among systems, human interactions, and internal states. Two main software faults identified by the NRC and EPRI were inconsistent with the system-requirements specification,[23] as well as the faults introduced during the detailed logic-design phases of software development because the interactions between some process logic inhibits and the test logic was not recognized by the designers or verifiers.[24] The NRC proposed two design attributes to eliminate CCFs: diversity and 100% testability. [25] Diversity is applied to mitigate the potential for common faults and ensure safety using different or dissimilar means in technology, function, and implementation. With respect to 100% testability, the NRC stated, "If a portion or component of a system can be fully tested, then it can be considered not to have a potential for software-based CCF. Fully tested or 100% testing means that every possible combination of inputs and every possible sequence of device states are tested, and that all outputs are verified for every case."[25] However, both design strategies have limitations. Diversity normally leads to higher costs, while potential CCF vulnerabilities will be more complicated and difficult to identify as system complexity increases. Applying 100% testing may reveal the presence of a fault, but not its absence, which means 100% testing does not fully eliminate software CCF concerns.

Therefore, this step focuses on identifying and providing guidance to eliminate the potential latent faults or triggers of CCFs and other independent failures based on the redundancy-guided STPA application in previous steps. The faults and triggers for hardware CCFs or independent failures can be identified straightforwardly. For software CCFs and independent failures, once the respective UCAs are obtained, their causal factors or latent faults can be place into one of two categories: (1) unsafe controller behaviors (i.e., operator errors, power failure of digital controllers, or a pressurizer setpoint that is not correctly programmed in bistable processors) or (2) inadequate feedback or outside information (i.e., wrong or absent signals from pressurizer to ESFAS). The triggers for software failures are defined as the contexts of the identified UCAs. The identification of causal factors should be interpreted by expert teams in system and software engineering, human reliability analyses, etc., and would be helpful to provide guidance for risk reduction and redesign of the digital systems.

4. CASE STUDY

In this section, the proposed RESHA approach was applied in the hazard analysis of a four-division digital ESFAS, which was modeled based on the a digital ESFAS design for an advanced pressurized water reactor.[26]

Step 1: Create a detailed hardware representation of the digital system of interest.

This four-division digital ESFAS includes the portion of plant-protection system (PPS) that activates the engineered safety features and their component-control system (CCS). The safety instrumentation and controls of the ESF systems consist of the electrical and mechanical devices and circuitry from sensors to actuation-device input terminals that are involved in generating signals that actuate the required ESF systems. The ESFAS portion of the PPS includes the following functions: bistable logic, local coincidence logic (LCL), ESFAS initiation, and testing function. After receiving ESFAS initiation signals from PPS, or main control room (MCR) operator console, or remote shutdown room (RSR) shutdown console, ESF-CCS generates ESF actuation signals to ESF component interface modules (CIMs) which transmit signals to the final actuated device. ESF-CIMs also receive actuation signals from the diverse protection system (DPS).

In each division, the ESFAS portion of PPS consists of four divisions. Each PPS division is located in an I&C equipment room and contains both an input and an output module, two bistable processors (BPs), two racks for the function of LCL, and other hardware for the interface with other PPS divisions, as shown in Figure 3. The redundant BPs could generate ESF actuation signals to the LCL processors in the four redundant divisions if the process values exceed their respective setpoints. Each LCL rack contains two logic processors (LPs); the initiation signals are provided to the ESF-CCS. The ESF-CCS consists of four divisions of group-controller (GC) and loop-controller (LC) cabinets. Each GC supports component control and provides ESF actuation signals to the LC. Each LC has component control logic and multiplexing function. Each ESF-CCS GC performs selective 2-out-of-4 coincidence logic, the output of the selective 2-out-of-4 logic is transmitted to the component control logic in the LC. The logic produces digital output (DO) signals to control the component through the component interface module (CIM), which performs signal prioritization.[26]

Step 2: Develop a FT of hardware failures for a top event of interest of the digital system.

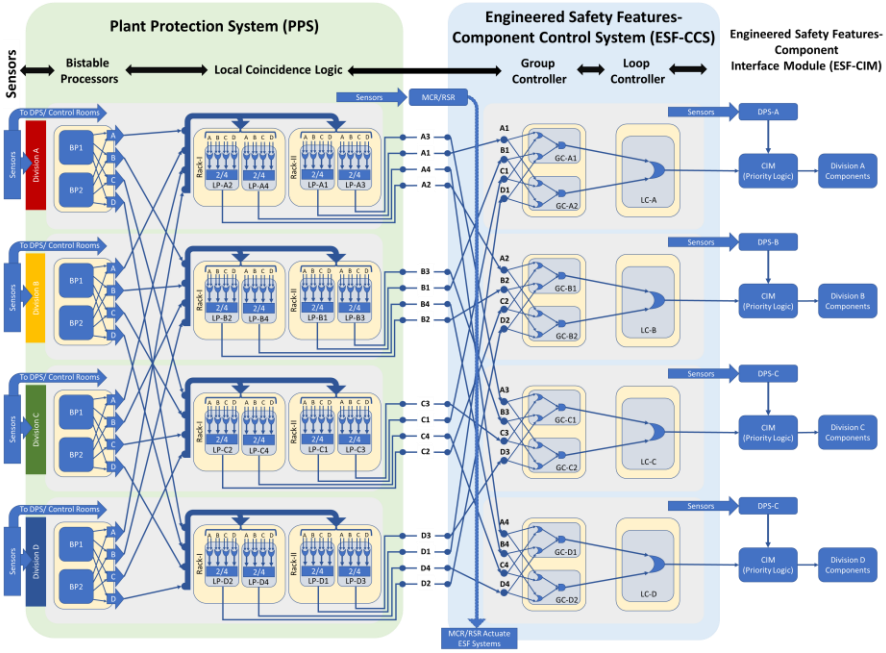

Figure 3. ESFAS functional logic

The top event for the FT was set as "ESFAS fails to actuate ESF systems." Different relevant top events can be identified for ESFAS; for example, the top event of ESFAS could also be "ESFAS sends spurious signals to actuate ESF systems" when the actuation command is not actually needed. For hardware failures of ESFAS components, units, and modules, a hardware-based FT can be built. In this work, the PRA tool SAPHIRE[27] is used to construct the FT. Part of the hardware-based FT is shown in Figure 4. The top event for this portion of the FT is "LP-A1 fails to send actuation signals to GC-A1," where two conditions should be considered if software failures are not included: LP-A1 hardware failure or LP-A1 does not receive any signals from BPs. For LP-A1 hardware failure, four basic events are included: (a) LP-A1 hardware independent failure, (b) a hardware CCF of all LPs in Rack II of division A, (c) hardware CCF of all LPs in Division A, and (d) hardware CCF of all LPs in all divisions. It is assumed that all basic units or modules that have identical function are identical. Both hardware and software diversity are ignored to simplify the process for CCF identification. It should be noted that, for a plant-specific hazard analysis, diversity of the target digital safety system should be considered. Therefore, here three

different CCFs are identified according to different levels of redundancy: division, unit, and module. In the following steps, the identification of software CCFs are also guided by the category of redundancy levels.

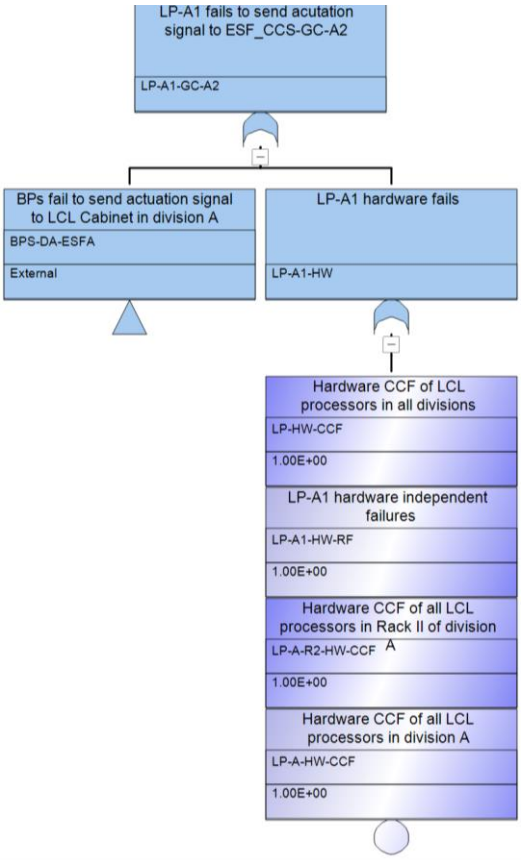

Figure 4. Portion of ESFAS FT showing hardware-type failures only (LP-A1 fails to send actuation signals to GC-A1)

Step 3: Determine UCAs based on a redundancy-guided application of STPA.

The first task is to build tables for losses that will be prevented and hazards which may lead to those losses. The major losses could be identified as human injury or loss of life, environmental contamination, equipment damage, and damage to public perception while hazards could be core damage, release of radioactive materials, etc. Next, a redundancy-guided multilayer control structure is created for ESFAS, based on its functional logic and hardware structure, as shown in Figure 5. Figure 5 illustrates the different levels of redundancy in a digital ESFAS, shown in Figure 3. The top-level layer of redundancy is the four independent divisions to actuate ESF components (i.e., the division-level redundancy). The functioning of each ESF component is affected by a specific division. Signals from plant sensors are sent to all divisions to compare with the engineered set points. In each division, signals are received and sent by several independent LCL racks, where decisions are made as to whether to actuate ESF components. This is the second layer of redundancy: unit-level redundancy. Then, in each LCL rack, actuation signals are transmitted in redundant LPs, which is considered as the third level of redundancy: module-level redundancy.

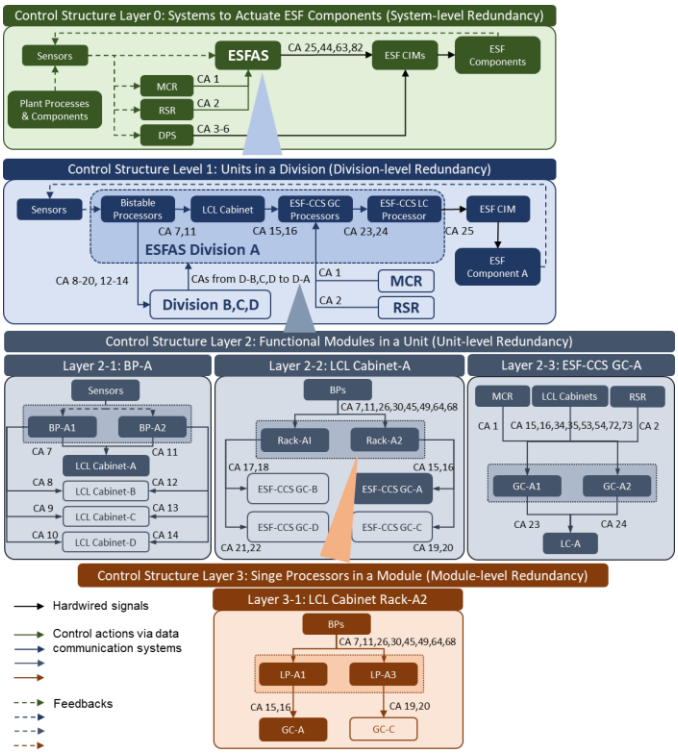

Figure 5. Redundancy-guided multilayer control structure for a digital ESFAS

Based on the information contained in ESFAS multilayer control structure, there are 82 total CAs identified: one CA from MCR, one CA from RSR, four CAs from DPS, and four groups of 19 CAs, one from each ESFAS division: A, B, C, and D. Based on these CAs and the categories of UCAs described in the STPA handbook, different UCAs can be defined. Table 1 lists the UCAs identified for LP-A1 software failures.

Table 1. UCAs identified for LP-A1 software failures

CA	UCA-a	UCA-b	UCA-c	UCA-d
CA-15: LCL-Rack-A2-LP-A1 provides an actuation signal to GC-A1	UCA-15a: LCL-Rack-A2-LP-A1 fails to provide an actuation signal to GC-A1 when it's needed	UCA-15b: LCL-Rack-A2-LP-A1 provides an actuation signal to GC-A1 but it's not needed	UCA-15c: LCL-Rack-A2-LP-A1 provides an actuation signal to GC-A1 but too late	UCA-15d: LCL-Rack-A2-LP-A1 provides an actuation signal to GC-A1 but stops too soon

Step 4: Construct an integrated FT by adding applicable UCAs as basic events.

In this step, applicable UCAs are selected and added into the hardware FT as software failures. For a specific top event in

the FT, some UCAs may be inapplicable. Considering the top event for the portion of FT in Figure 4 is "LP-A1 fails to send actuation signals to GC-A1," UCA-15b and UCA-15d are not applicable because sending an actuation command is required and is not a continuous action. Only UCA-a and UCA-c were considered in this case.

Step 5: Identify software CCFs from duplicate UCAs for redundant designs within the integrated FT.

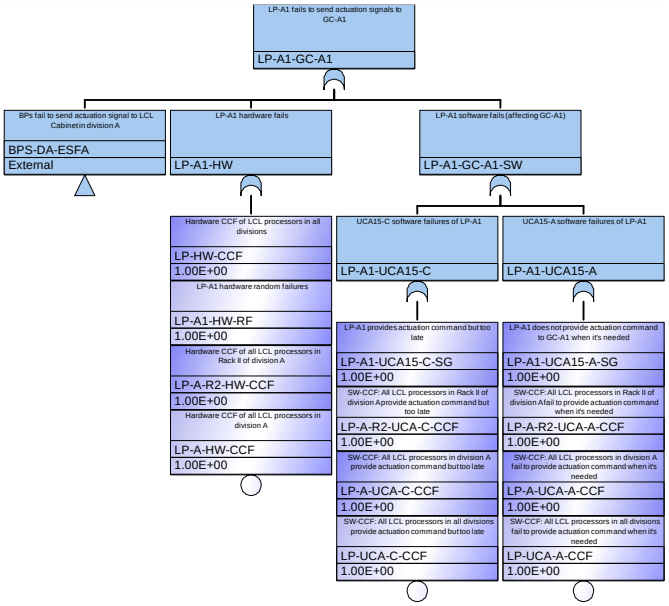

Figure 6. Integrated FT for "LP-A1 fails to send actuation signals to GC-A1" with relevant software failures added

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. According to the assumption that all basic units or modules that have identical function are identical, and software diversity is ignored to simplify the process for CCF identification, three different software CCFs, based on UCA-15a or UCA-15c, are classified depending on the redundancy levels. UCA-15a provides an example: (1) all LPs in Rack II of Division A fail to provide an actuation command when it is needed, (2) all LPs in Division A fail to provide an actuation command when it is needed, and (3) all LPs in all divisions fail to provide an actuation command when it is needed, as shown in Figure 6.

Step 6: Determine the minimal cut sets to discover the potential SPOFs.

SAPHIRE was used to calculate the cut sets of the integrated FT and to determine the potential SPOFs that might be added by considering software failures. The cut sets are truncated based on order, rather than by probability, as listed in Table 2. The values of failure probabilities are not assigned in this work. For the fully integrated ESFAS FT model, there is only one 1st-order cut set that leads to the top event, which is "CIM hardware CCF." CIMs only receive hardwired signals from ESF-CCS and transmit signals to the final actuated devices. This basic event is also the only one 1st-order cut set for the FT model with hardware failures only and for the FT model without MCR/RSR operations. The latter is considered as a model for automatic actuation only. For the ESFAS FT model without diverse actuation systems (i.e., DPS and MCR/RSR), there are 13 1st-order cut sets identified, as shown in Table 3. Four of these basic events are hardware CCFs, and others are software CCFs identified using redundancy-guided STPA. It should be noted that both hardware and software diversity are ignored to simplify the process for CCF identification in this work. Results should be different for plant-specific analysis once diverse designs are considered. Compared to other cut sets, these identified ones could be potential key hazards that fail the whole digital ESFAS system if other diverse actuation systems are not in a good working condition.

Table 2. Cut set calculations for different ESFAS models

Truncation (Order)	Cut Set #			
	Full FT	FT with hardware only	FT w/o MCR or RSR	FT w/o DPS, MCR or RSR
5	50714	570	127236	1096601
4	182	6	417	39834
3	19	3	91	139
2	19	3	37	31
1	1	1	1	13

Table 3. 1st-order cut set for the ESFAS FT model without diverse actuation systems (i.e., DPS and MCR/RSR)

#	Cut set / Basic event	Description
1	LC-BP-UCA-A-CCF	All BPs in logic cabinets fail to send actuation signals to LPs
2	LC-BP-UCA-C-CCF	All BPs in logic cabinets send actuation signals to LPs but too late
3	LC-BP-HW-CCF	BP hardware fails in all divisions
4	LP-UCA-A-CCF	All LPs in logic cabinets fail to send actuation signals to ESF-CCS
5	LP-UCA-C-CCF	All LPs in logic cabinets send actuation signals to ESF-CCS but too late
6	LP-HW-CCF	LP hardware fails in all divisions
7	ESF-CCS-GC-UCA-A-CCF	All GC processors in ESF-CCS fail to send actuation signals to ESF-CCS LC processors
8	ESF-CCS-GC-UCA-C-CCF	All GC processors in ESF-CCS send actuation signals to ESF-CCS LC processors but too late
9	ESF-CCS-GC-HW-CCF	GC processors hardware fails in all ESF-CCS divisions
10	ESF-CCS-LC-UCA-A-CCF	All LC processors in ESF-CCS fail to send actuation signals to CIMs
11	ESF-CCS-LC-UCA-C-CCF	All LC processors in ESF-CCS send actuation signals to CIMs but too late

12	ESF-CCS-LC-HW-CCF	LC processors hardware fails in all ESF-CCS divisions
13	CIM-HW-CCF	CIM hardware fails in all divisions

Step 7: Identify and provide guidance to eliminate latent faults or triggers of CCFs.

This step focuses on providing guidance to eliminate potential triggering conditions or events that activate dormant faults to the CCFs that were identified in previous steps. As mentioned in Section 4, for software CCFs or independent failures, causal factors or potential triggers can be identified in two categories: (1) unsafe controller behaviors and (2) inadequate feedback or outside information. The triggers of software failures are defined as the contexts of the identified UCAs. The step takes the CCF of UCA-15a (#4. LP-UCA-A-CCF in Table 3) as an example to illustrate how to determine these causal factors. The identification of causal factors should cooperate with the expert teams in system and software engineering, human reliability analysis, etc. According to the contexts of the UCAs, different subcausal factors can be defined for the two categories by using Bayesian networks. Figure 7 displays a simple Bayesian network; more details should be added via collaborations with different expert teams. In this way, reliability analysis can be performed based on these Bayesian networks and reliability models for quantifying the probabilities of identified CCFs in future work.

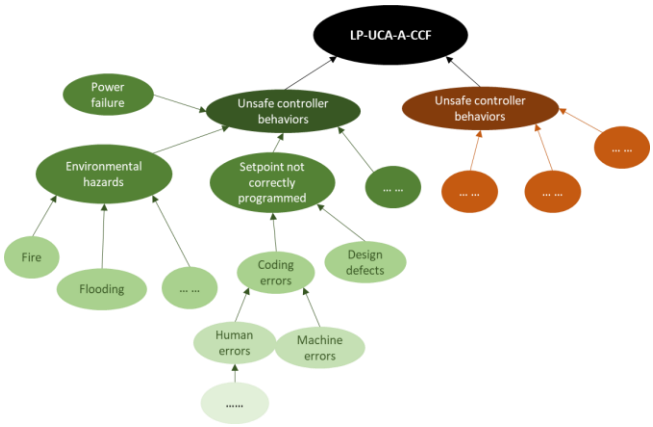

Figure 7. A simple Bayesian network for the identification of causal factors (triggers) of a CCF

5. CONCLUSIONS

This paper applies a modularized approach to conduct redundancy-guided systems-theoretic hazard analysis for an advanced digital ESFAS with multilevel redundancy designs. Systematic methods and risk-informed tools are incorporated to address both hardware and software CCFs, which provide a guidance to eliminate the triggers of potential single points of failure in the design of digital safety systems in advanced plant designs. The applied redundancy-guided systems-theoretic approach was developed for a hazard analysis that aims to help system designers and engineers address digital-based CCFs and qualitatively analyze their effects on digital system vulnerability. Failures with a high level of impact to system safety can thus be identified, especially software CCFs. Potential triggers (causal factors) of CCFs can be identified in different categories and classified using Bayesian networks. 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.

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 work was also supported by consultations and contributions from Ken Thomas and James Knudsen from INL, Andrew Clark and Adam Williams from Sandia National Laboratory, and Edward (Ted) Quinn from Technology Resources.

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.

REFERENCES

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

[2] T.-L. Chu, M. Yue, G. Martinez-Guridi and J. Lehner, “Review of Quantitative Software Reliability Methods,” Brookhaven National Laboratory, Upton, NY , September 2010.

[3] U.S.NRC, "Method of Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems," U.S.NRC, Washington, D.C., 1994.

[4] K. Thomas and K. Scarola, "Strategy for implementation of Safety-Related Digital I&C Systems," Idaho National Laboratory, Idaho Falls, ID, 2018.

[5] T. E. Wierman, D. M. Rasmuson and A. Mosleh, "Common-Cause Failure Databased and Analysis System: Event Data Collection, Classification, and Coding," Idaho National Laboratory, Idaho Falls, ID, 2007.

[6] U.S. NRC, "Title 10 CFR (Code of Federal Regulations) Part 50, Appendix A: General Design Criteria for Nuclear Power Plants," U.S. NRC, Washingyon. D.C., 1995.

[7] U.S. NRC, "Digital Systems Software Requirements Guidelines," U.S. NRC, Washington, D.C., 2001.

[8] U.S. NRC, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," U.S. NRC, Washington, D.C., 2008.

[9] U.S. NRC, "Historical Review and Observations of Defense-in-Depth," U.S. NRC, Washington, D.C., 2016.

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

[11] U.S.NRC, "Use of Probabilistic Risk Assessment Methods in Nuclear," U.S.NRC, Washington, D.C., 1995.

[12] S. A. Arndt and A. Kuritzky, "Lessons Learned from the U.S. Nuclear Regulatory Commission's Digital System Risk Research," *Nuclear Technology*, vol. 173, no. 1, pp. 2–7, 2010.

[13] U.S. NRC, "Plans for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls," U.S. NRC, Washington, D.C., 2018.

[14] U.S.NRC, "Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure," U.S.NRC, Washington, D.C., 2019.

[15] H. Bao, H. Zhang and K. Thomas, "An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants," Idaho National Laboratory, Idaho Falls, ID, 2019.

[16] T. Shorthill, H. Bao, H. Zhang and H. Ban, "Demonstration of Integrated Hazard Analysis for Digital Reactor Trip Systems," in *2019 ANS Winter Meeting and Nuclear Technology Expo*, Washington, D.C., 2019.

[17] T. Shorthill, H. Bao, H. Zhang and H. Ban, "A Redundancy-Guided Approach for the Hazard Analysis of Digital Instrumentation and Control Systems in Advanced Nuclear Power Plants (Under Review)," *Reliability Engineering and System Safety*, 2020.

[18] U.S.NRC, "Research Information Letter 1002: Identification of Failure Modes in Digital Safety Systems – Expert Clinic Findings, Part 2," U.S.NRC, Washington, D.C.

[19] N. Leveson, "The Role of Software In Spacecraft Accidents," *AIAA Journal of Spacecraft and Rockets*, vol. 41, no. 4, July 2004.

[20] J. Thomas, F. L. d. Lemos and N. Leveson, "Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants," MIT, Cambridge, Massachusetts, 2012.

[21] A. J. Clark, A. D. Williams, A. Muna and M. Gibson, "Hazard and Consequence Analysis for Digital Systems – A New Approach to Risk Analysis in the Digital Era for Nuclear Power Plants," in *Transactions of the American Nuclear Society*, Orlando, Florida, November 11-15, 2018.

[22] M. Jockenhovel-Barttfeld, S. Karg, C. Hessler and H. Bruneliere, "Reliability Analysis of Digital I&C Systems within the Verification and Validation Process," in *Probabilistic Safety Assessment and Management*, Los Angeles, CA, Septemmber 2018.

[23] U.S.NRC, "Technical Specification Required Shutdown Due to Core Protection," U.S.NRC, Washington, D.C., October 2005.

[24] U.S.NRC, "Design Defect in Safeguards Bus Sequencer Test Logic Places Both Units," U.S.NRC, Washington, D.C., July 1995.

[25] U.S.NRC, "Standard Review Plan: Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-based Instrumentation and Control Systems Review Responsibilities," U.S.NRC, Washington, D.C., August 2016.

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

[27] U.S. NRC, "Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8," U.S. NRC, Washington, D.C., March, 2011.