INL/CON-22-66974-Revision-0

Common Cause Failure Evaluation of High Safety-significant Safety-related Digital Instrumentation and Control Systems

June 2022

Han Bao, Hongbin Zhang , Tate Shorthill , Edward Chen , Svetlana Lawrence

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-22-66974-Revision-0

Common Cause Failure Evaluation of High Safety-significant Safety-related Digital Instrumentation and Control Systems

Han Bao, Hongbin Zhang , Tate Shorthill , Edward Chen , Svetlana Lawrence

June 2022

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

Common Cause Failure Evaluation of High Safety-significant Safety-related Digital Instrumentation and Control Systems

Han Bao[a], Hongbin Zhang[b], Tate Shorthill[c], Edward Chen[d], Svetlana Lawrence[e]
[a] Idaho National Laboratory, P.O. Box 1625, MS 3860, Idaho Falls, ID, 83415, han.bao@inl.gov
[b] Terrapower, 15800 Northup Way, Bellevue, WA, 98008, hzhang@terrapower.com
[c] University of Pittsburgh, 3700 O'Hara Street, Pittsburgh, PA, 15261, tate.shorthill@inl.gov
[d] North Carolina State University, 2500 Stinson Dr., Raleigh, NC, 27607, echen2@ncsu.edu
[e] Idaho National Laboratory, P.O. Box 1625, MS 3855, Idaho Falls, ID, 83415,
svetlana.lawrence@inl.gov

Abstract: Digital instrumentation and control (DI&C) systems in nuclear power plants (NPPs) have many advantages over analog systems, but also pose different engineering and technical challenges, such as potential threats due to common cause failures (CCFs). This paper proposes a framework for risk assessment of DI&C developed by Idaho National Laboratory (INL) for dealing with potential software CCFs in DI&C systems of NPPs. The methodology development on the quantitative evaluation of software CCFs in high safety-significant safety-related DI&C systems in NPPs is illustrated in this paper as well. In the proposed framework, qualitative hazard analysis and quantitative reliability and consequence analysis are successively implemented to obtain quantitative risk information, compare with respective risk evaluation acceptance criteria, and provide suggestions for risk reduction and design optimization. A comprehensive case study was also performed at INL and documented in this paper. Results show that proposed framework can effectively identify potential digital-based CCFs, estimate their failure probabilities, and evaluate their impacts to system and plant safety.

1 INTRODUCTION

Although the current fleet of United States (U.S.) nuclear power plants (NPPs) was originally designed and constructed with analog systems, the U.S. nuclear industry has been working on transitioning from analog to digital instrumentation and control (DI&C) technologies. DI&C systems have many advantages over analog systems. They are proven to be more reliable, cheaper, and easier to maintain given obsolescence of analog components. However, they also pose new engineering and technical challenges. The U.S. Nuclear Regulatory Commission (NRC) continues supporting the research work in developing and improving licensing criteria for the evaluation of new DI&C systems. In 2018, SECY-18-0090 [1] was published to clarify guidance associated with evaluating potential common cause failures (CCFs) of DI&C systems. SECY-18-0090 identifies the following guiding principles: (1) applicants and licensees for production and utilization facilities should continue to assess and address CCFs due to software for DI&C systems and components; (2) a defense-in-depth and diversity (D3) analysis for reactor trip systems (RTSs) should be paramount; (3) and engineered safety features should continue to be performed to demonstrate that vulnerabilities to a CCF have been identified and adequately addressed. The D3 analysis can be performed using either a design-basis deterministic approach or best-estimate approach [1]. In 2019, the NRC staff developed the integrated action plan (IAP) [2]. Four detailed modernization plans were proposed to resolve regulatory challenges, provide confidence to licensees, and modernize the I&C regulatory infrastructure. One of them—protection against CCF—addresses "developing guidance for using effective qualitative assessments of the likelihood of failures, along with coping and/or bounding analysis for addressing CCFs, use of defensive design measures for eliminating CCF from further consideration, and staff evaluation of the NRC's existing positions on defense against CCF." The current guidance, however, is unclear regarding the applicability of criteria for using coping analysis and other design features (e.g., defensive measures) for eliminating CCFs from further consideration [2]. Meanwhile, the industry stakeholders are seeking clearer NRC staff guidance on methods for the analysis of the potential for CCFs in DI&C systems and a more risk-informed, consequence-based regulatory infrastructure that removes uncertainty in requirements and enables technical consistency [2].

Many efforts from regulatory, industrial, and academic communities have been made for qualitatively addressing CCFs in DI&C systems, especially software CCFs, given the increased pace of design and deployment of high safety-significant safety-related (HSSSR) DI&C systems in NPPs. To successfully model DI&C systems, the need exists to model both the hardware and software interactions of the system. Traditional methods, such as failure modes and effects analysis (FMEA) and fault tree analysis (FTA), have been used to extensively model analog systems. However, these traditional methods are not fully suitable to identify failures in interactions between digital systems and controlled processes (i.e., Type 1 interactions), as well as interactions between digital systems and their own components or other systems (i.e., Type 2 interactions) [3]. Lessons learned from the NRC's investigation of multiple analysis methods indicate there "may not be one preferable method for modeling all digital systems" [3]. Combining methods may prove beneficial. A recent advancement in hazards analysis, developed jointly by Electric Power Research Institute (EPRI) and Sandia National Laboratory (SNL), combines FTA and the systems-theoretic process analysis (STPA) as a portion of their methodology for Hazard and Consequence Analysis for Digital Systems (HAZCADS) [4]. Though STPA may be applied at any stage of system design and review, it is ideally suited for early applications in the design process before the safety features have been incorporated into the design [5]. Then, as more details are incorporated, the STPA method is applied iteratively to further improve the design. However, even when fine details about a system are known, the analysis may remain at a high level, relying on causal factor investigations to provide details of subcomponent failures and interactions. In other words, details, such as redundant subsystems or components, are often ignored in all but the final part of STPA.

In July 2021, Nuclear Energy Institute (NEI) published NEI 20-07, "Guidance for Addressing Software Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems" [6], where a two-step process was proposed to address HSSSR systematic CCFs based on STPA: Step 1 is to perform a systematic hazards analysis based on STPA that creates a model of the system control structure, identifies unsafe control actions (UCAs) as software failures, and establishes a risk reduction objective (RRO); Step 2 is to develop STPA loss scenarios and eliminate or mitigate them in an efficient way. A bounding assessment is proposed to calculate the risk change when entire HSSSR systems fail due to software CCFs (assuming system failure probability = 1). The risk change (e.g., Δ core damage frequency [CDF]) is then mapped to the regions described in RG 1.174 [7] and used to determine the RRO. This process qualitatively addresses potential failures in DI&C based on a bounding assessment; consequently, the real safety margin gained by plant digitalization on HSSSR DI&C systems could be underestimated in this intentionally conservative approach.

The efforts described above provide a technical basis for dealing with potential software CCFs in the HSSSR DI&C systems of NPPs; however, some technical challenges remain: (1) Is qualitative evaluation sufficient for addressing software CCFs in HSSSR DI&C systems? (2) How can CCF-related impacts to HSSSR DI&C systems be quantitatively evaluated on an entire plant response basis? (3) How can the most significant CCFs—especially software CCFs—be efficiently identified? (4) How can a complete reliability analysis for large-scale HSSSR DI&C systems with small-scale software/digital units be performed? (5) How can different system architectures be evaluated from perspectives of both risk and cost?

To address these challenges, an integrated risk-assessment strategy is needed to include qualitative hazard analysis, quantitative reliability, and consequence analysis for addressing software CCFs in HSSSR DI&C systems. To fulfil this need and deal with the technical barriers in identifying potential software CCF issues in HSSSR DI&C systems of NPPs, Idaho National Laboratory (INL) and the Risk-Informed Systems Analysis (RISA) Pathway sponsored by the U.S. Department of Energy (DOE) Light Water Reactor Sustainability (LWRS) Program initiated a project to develop a risk assessment strategy [8] to:

1. Provide a best-estimate, risk-informed capability to quantitatively and accurately estimate the NPP safety margin gained from the modernization of HSSSR DI&C systems.

2. Develop an advanced risk assessment technology to support the transition from analog to DI&C technologies for nuclear industry.
3. Assure the long-term safety and reliability of HSSSR DI&C systems.
4. Reduce uncertainty in costs and support integration of DI&C systems at NPPs.

A framework for risk assessment of DI&C was proposed to address the project objectives. As shown in Figure 1, the proposed framework provides a systematic, verifiable, and reproducible approach based on technically sound methodologies. The framework successively implements qualitative hazard analysis, quantitative reliability analysis, and consequence analysis to obtain quantitative risk metrics. The quantified risks are then compared with respective acceptance criteria that allows for the identification of vulnerabilities, as well as providing suggestions for risk reduction and design optimization.

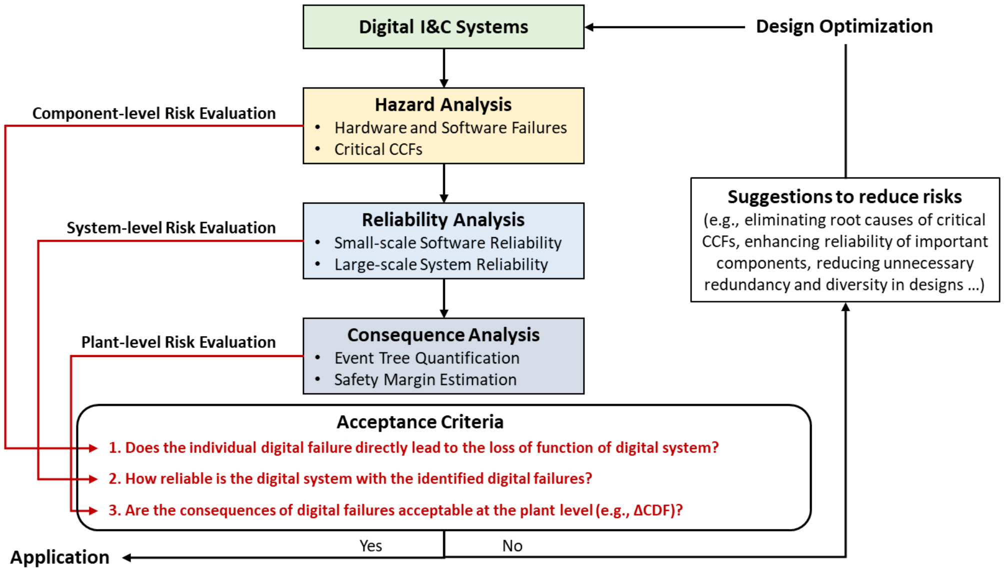
Digital I&C Systems
Design Optimization
Component-level Risk Evaluation
Hazard Analysis
• Hardware and Software Failures
• Critical CCFs
System-level Risk Evaluation
Reliability Analysis
• Small-scale Software Reliability
• Large-scale System Reliability
Suggestions to reduce risks
(e.g., eliminating root causes of critical CCFs, enhancing reliability of important components, reducing unnecessary redundancy and diversity in designs …)
Plant-level Risk Evaluation
Consequence Analysis
• Event Tree Quantification
• Safety Margin Estimation
Acceptance Criteria
1. Does the individual digital failure directly lead to the loss of function of digital system?
2. How reliable is the digital system with the identified digital failures?
3. Are the consequences of digital failures acceptable at the plant level (e.g., ΔCDF)?
Yes
No
Application

Figure 1. Schematic of the proposed framework for safety evaluation and design optimization of HSSSR DI&C systems (derived from [9] [10]).

2 VALUE PROPOSITION

To deal with the technical issues in addressing potential software CCF issues in HSSSR DI&C systems of NPPs, the proposed framework is expected to provide:

1. **An integrated and best-estimate, risk-informed capability to address new technical digital issues quantitatively, accurately, and efficiently in plant modernization progress, such as software CCFs in HSSSR DI&C systems of NPPs.**

   An existing qualitative approach for addressing CCFs in HSSSR DI&C systems may significantly underestimate the real safety margin introduced by plant digitalization. This framework is developed and demonstrated in an integrated way including qualitative hazard analysis, quantitative reliability, and consequence analyses. The proposed framework aims to provide a best-estimate, risk-informed capability to accurately estimate the safety margin increase obtained from plant modernization, especially for digital HSSSR I&C systems. In the proposed framework, a redundancy-guided systems-theoretic method for hazard analysis (RESHA) was developed on HSSSR DI&C systems for supporting I&C designers and engineers to address both hardware and software CCFs and qualitatively analyze their effects on system availability [11] [12]. It also provides a technical basis for implementing following reliability and consequence analyses of unexpected software failures, and supporting the optimization of D3 applications in a cost-efficient way. Targeting the complexity of redundant designs in HSSSR DI&C systems integrates STPA [5], FTA, and HAZCAD [4] to effectively identify software CCFs by reframing STPA in a redundancy-guided way, such as (1) depicting a redundant and diverse system via a detailed representation; (2) refining different redundancy levels based on the structure of DI&C systems; (3) constructing a redundancy-guided multilayer control structure; and (4) identifying potential CCFs in different redundancy levels. This approach has been demonstrated and applied for the hazard analysis of a four-division digital RTS [11] and a four-division, digital, engineered safety features actuation system (ESFAS) [12]. These efforts have been included in the LWRS-RISA milestone report for fiscal year (FY)-2020 [13]. 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; and (2) estimating the probabilities of the consequences of digital system failures. In the proposed framework, two methods have been developed for different application conditions: the Bayesian and Human-reliability-analysis-aided Method for the reliability Analysis of Software (BAHAMAS) [14] for limited data conditions and Orthogonal-defect Classification for Assessing Software reliability (ORCAS) for data-rich analysis. More details can be found in Section 4. Finally, consequence analysis is conducted to quantitatively evaluate the consequence impact of digital failures on plant behaviors and responses. Some digital-based failures may initiate an event or scenario that may not be analyzed before, which brings in a big challenge to plant safety. In this paper, a couple of accident scenarios have been selected for the consequence analysis, as described in Section 5.

In February 2022, the NRC organized a public meeting to inform the industry and solicit external stakeholders' feedback on the NRC's plan to potentially expand the current policy for addressing CCFs for DI&C systems to allow the consideration of risk-informed alternatives. The LWRS Program's RISA team presented on providing capabilities to address and fulfil the risk-informed alternatives for the evaluation of CCFs in DI&C systems. The NRC staff found the framework interesting from a regulatory point of view since it may be useful to evaluate the impacts of various DI&C design architectures to overall plant safety.

2. **A common and a modularized platform to digital I&C designers, software developers, cybersecurity analysts, and plant engineers to efficiently predict and prevent risk in the early design stage of digital I&C systems.**

Many programs/projects were and are being created with various methods/approaches/frameworks generated either for single software reliability analysis or for quantifying the system-level interactions between digital systems and other systems. However, these efforts are rarely targeted on software CCFs in HSSSR DI&C systems. As shown in Figure 2, the proposed framework, as a modularized platform, aims to have good communication with various small-scale unit-level software reliability analysis methods (e.g., quantitative software reliability methods) and large-scale system-level reliability analysis frameworks (e.g., probabilistic risk assessment [PRA]). RESHA, as a top-down approach, can identify the digital or software failures in the unit-level interactions inside of a digital system, then BAHAMAS and ORCAS can be used to quantify the probability of the STPA-identified software failures based on suitable existing quantitative software reliability methods, such as Bayesian networks, test-based methods, or metric-based methods.

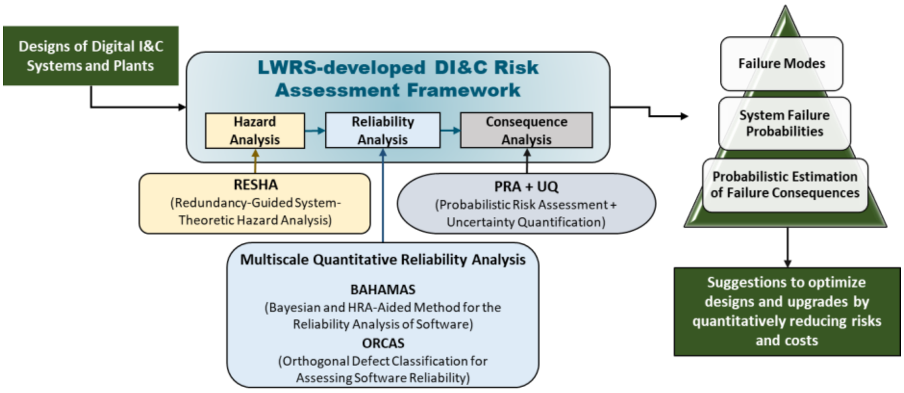
Designs of Digital I&C Systems and Plants
LWRS-developed DI&C Risk Assessment Framework
Hazard Analysis
Reliability Analysis
Consequence Analysis
RESHA
(Redundancy-Guided System-Theoretic Hazard Analysis)
PRA + UQ
(Probabilistic Risk Assessment + Uncertainty Quantification)
Multiscale Quantitative Reliability Analysis
BAHAMAS
(Bayesian and HRA-Aided Method for the Reliability Analysis of Software)
ORCAS
(Orthogonal Defect Classification for Assessing Software Reliability)
Failure Modes
System Failure Probabilities
Probabilistic Estimation of Failure Consequences
Suggestions to optimize designs and upgrades by quantitatively reducing risks and costs

Figure 2. The modularized structure of LWRS-developed framework. (derived from [15]).

3. **Technical bases and risk-informed insights to assist NRC and industry in formalizing relevant licensing processes for addressing CCF considerations in HSSSR DI&C systems.**

   Figure 3 illustrates how the proposed framework can support licensing of a HSSSR DI&C design or upgrade. NRC Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems Review Responsibilities," [16] clarifies the requirement for acceptable methods for addressing CCFs, including identifying CCFs, reducing CCF likelihood, and evaluating CCF impacts in design-basis events. The capabilities of the LWRS-developed framework in hazard, reliability, and consequence analysis matches well with these requirements.

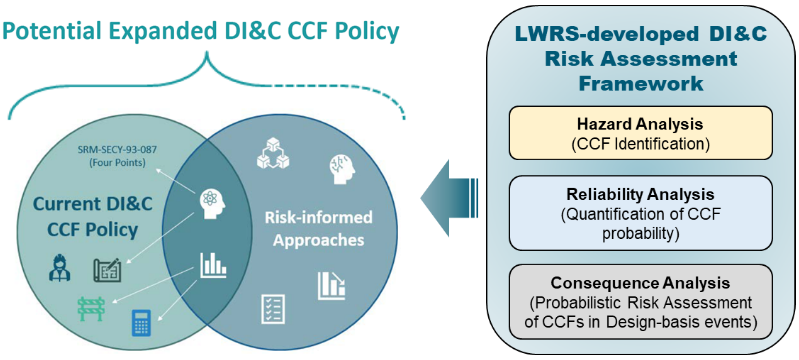
Potential Expanded DI&C CCF Policy
SRM-SECY-93-087 (Four Points)
Current DI&C CCF Policy
Risk-informed Approaches
LWRS-developed DI&C Risk Assessment Framework
Hazard Analysis (CCF Identification)
Reliability Analysis (Quantification of CCF probability)
Consequence Analysis (Probabilistic Risk Assessment of CCFs in Design-basis events)

Figure 3. NRC expanded DI&C CCF policy vs. LWRS-developed framework in CCF analysis.

4. **An integrated risk-informed tool to support the nuclear industry in addressing regulatory requirements in DI&C system implementation.**

   The LWRS-developed framework can be beneficial for the design of digital HSSSR systems in the plant modernization process, but the estimated safety margin using the LWRS-developed framework should be much higher and more accurate than other conservative bounding assessment approach. The safety improvements of these new digital designs are expected to be significant and can be presented more clearly. Currently, it is thought after qualitatively addressing CCFs, all will need to be fixed by adding diversity, which costs a lot. In fact, some CCFs do not have significant impacts on CDF change or large release frequency. The framework can evaluate and compare the design alternatives of HSSSR DI&C systems in the early design stage, by quantifying the impacts of single software CCFs to the HSSSR DI&C systems and if necessary, plant safety. For instance, it can support the determination of the level of redundancy (e.g., a four-division ESFAS vs. a two-division ESFAS) or the level of diversity (e.g., deployment of software/design/equipment diversity in division-level vs. in unit-level). By comparing the risk and cost of different redundant and diverse designs, costs can be saved if some CCFs are proved to be insignificant to plant safety and no defence actions are needed. Based on current analysis results, failure probability of HSSSR DI&C systems due to software CCFs is quite low, and the CDF is also significantly reduced compared with the one with traditional analog systems. Also, the framework is also promising to be applied to the software risk analysis for machine-learning-based digital twins in nearly autonomous management and control systems [17].

3 METHODOLOGY

3.1 Redundancy-Guided System-Theoretic Hazard Analysis

The hazard analysis method developed in the LWRS-developed framework is RESHA, which is an FTA-based method incorporating STPA to identify inner software failures and digital-based failures in Type II interactions. RESHA incorporates the concept of combining FTA and STPA from HAZCADS. STPA is reframed in a redundancy-guided way to address CCF concerns in highly redundant DI&C systems. A seven-step process, as shown in Figure 4, illustrates the workflow of RESHA for the hazard analysis of DI&C systems, especially for CCF analysis of highly redundant HSSSR DI&C systems. The main outcomes of RESHA are: (1) the identification of CCFs and potential single points of failure

(SPOFs) in the DI&C design; (2) an integrated FT including both hardware and software failures, individual failures, and CCFs; and (3) hazard preventive strategies. The acceptance criterion of risk evaluation for the hazard analysis is "does the individual digital-based failure lead to the loss of function of the DI&C system?" In another words, is there any SPOF existing in the system that may lead to the failure of a DI&C system?

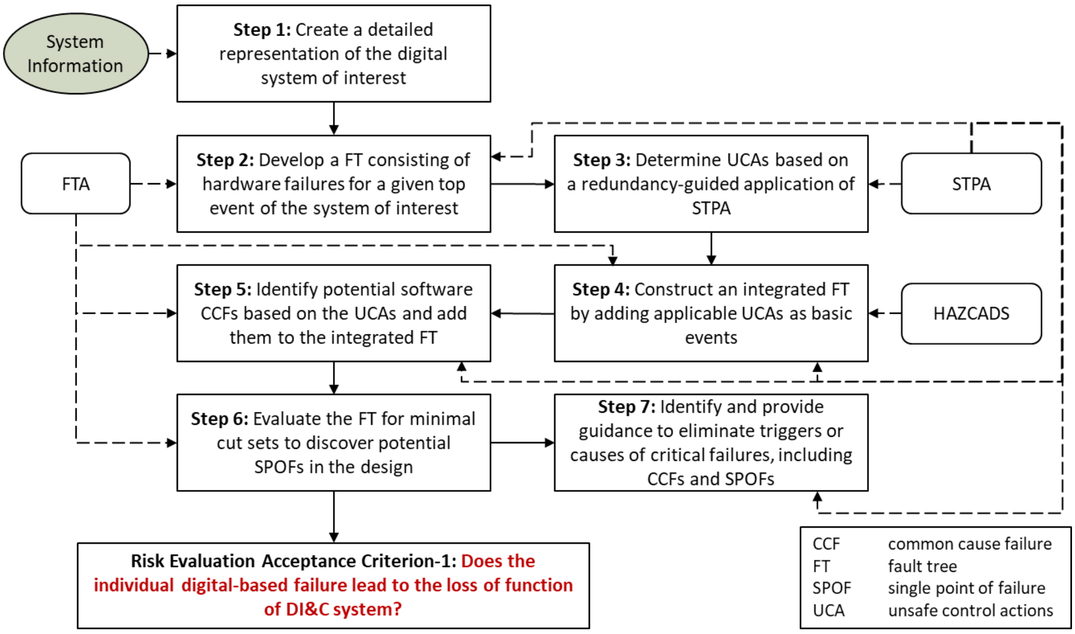
System Information
Step 1: Create a detailed representation of the digital system of interest
FTA
Step 2: Develop a FT consisting of hardware failures for a given top event of the system of interest
Step 3: Determine UCAs based on a redundancy-guided application of STPA
STPA
Step 5: Identify potential software CCFs based on the UCAs and add them to the integrated FT
Step 4: Construct an integrated FT by adding applicable UCAs as basic events
HAZCADS
Step 6: Evaluate the FT for minimal cut sets to discover potential SPOFs in the design
Step 7: Identify and provide guidance to eliminate triggers or causes of critical failures, including CCFs and SPOFs
Risk Evaluation Acceptance Criterion-1: Does the individual digital-based failure lead to the loss of function of DI&C system?
CCF common cause failure
FT fault tree
SPOF single point of failure
UCA unsafe control actions

Figure 4. RESHA workflow for DI&C system hazard analysis (derived from [9] [10]).

The RESHA method has been demonstrated based on a representative four-division digital RTS and ESFAS, which were modeled based on the DI&C design of an Advanced Power Reactor 1400 MW (APR-1400) [18]. The final outputs from RESHA feed into following the reliability analysis and component-level risk evaluation that provides a guidance for system modifications (e.g., the elimination of SPOFs, the enhancement of reliability of specific components or diversity in designs). In other words, the RESHA provided a means to identify CCFs in digital-based Type II interactions and software of highly redundant HSSSR DI&C systems, by fully considering redundancy into the hazard analysis process.

3.2 Multiscale Quantitative Reliability Analysis

The goal of the reliability analysis is to estimate DI&C system reliability by calculating the integrated FT of DI&C systems obtained in the hazard analysis, and then provide inputs for following the consequence analysis. For the reliability analysis of large-scale DI&C systems, the quantitative small-scale reliability analysis of software and Type II interactions in DI&C systems are also included in the reliability analysis workflow. Figure 5 illustrates the framework of the multiscale reliability analysis of DI&C system.

The first step to any good reliability analysis for a DI&C system is the adequate collection and evaluation of design and requirement documentation. The next step is to estimate the failure probability of UCAs identified in the hazard analysis. In the proposed framework, two methods have been developed for different application conditions: BAHAMAS [14] for limited data conditions and ORCAS for data-rich analysis. BAHAMAS was developed for the conditions with limited testing/operational data or for reliability estimations of software in an early development stage. It can provide a rough estimation of failure probabilities to support the design of software and target DI&C systems even when data is very limited. Instead of relying on testing data, BAHAMAS assumes software failures can be traced to human errors in the software development life cycle (SDLC) and modeled with human reliability analysis (HRA). In BAHAMAS, a Bayesian belief network (BBN) is developed to provide a means of combining disparate causal factors and fault sources in the system, while HRA is applied to quantify the potential root human errors during SDLC. More technical information about the BAMAHAS method can be found in [14]. In contrast to BAHAMAS, ORCAS applies a white box software invasive testing and modeling strategy to trace and identify the software defects that can potentially lead to software failures. The approach is a root-cause analysis methodology focused on comprehensive testing and follows the orthogonal-defect classification (ODC) approach to determine testing sufficiency. ODC is also used to systematically classify the identified defects into specific software causality groups, thereby linking defects to potential software failure modes. The failure data collected from testing strategies is also combined with software reliability growth models and linear reliability models to quantify the software failure probability of specific UCAs.

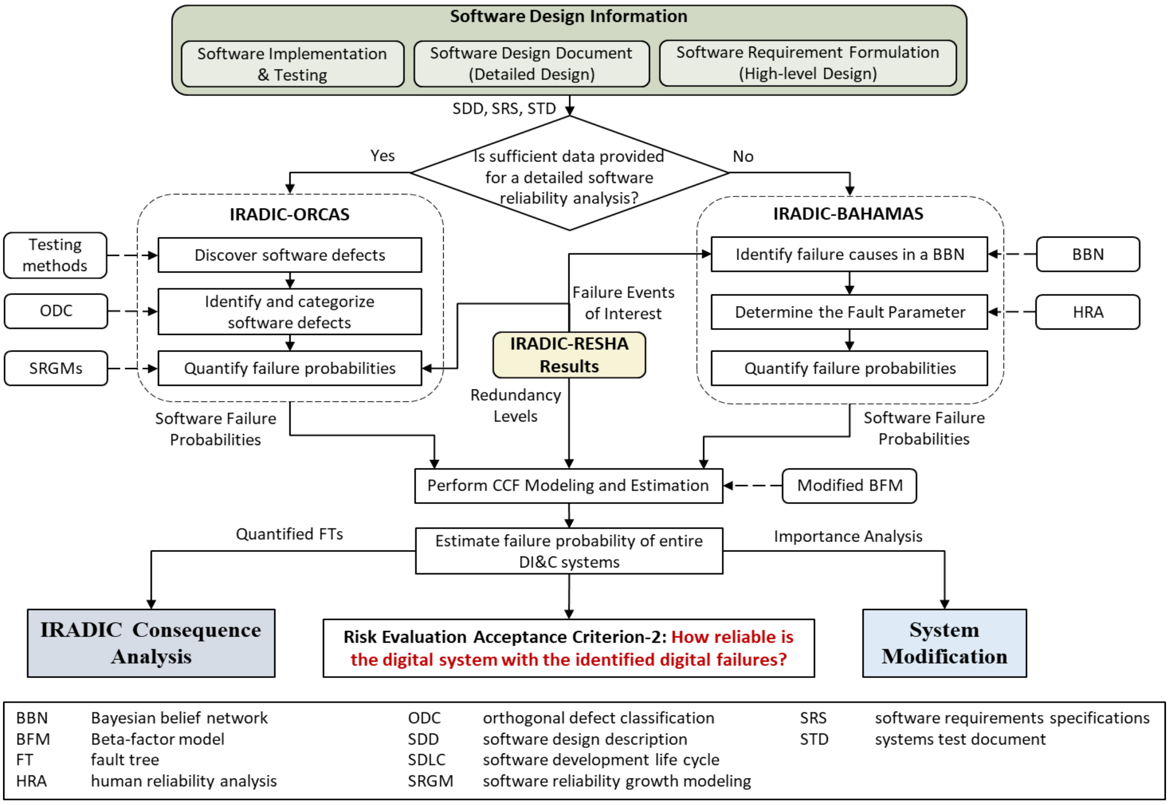
Software Design Information
Software Implementation & Testing
Software Design Document (Detailed Design)
Software Requirement Formulation (High-level Design)
SDD, SRS, STD
Is sufficient data provided for a detailed software reliability analysis?
Yes
No
IRADIC-ORCAS
Testing methods
ODC
SRGMs
Discover software defects
Identify and categorize software defects
Quantify failure probabilities
IRADIC-BAHAMAS
Identify failure causes in a BBN
Determine the Fault Parameter
Quantify failure probabilities
BBN
HRA
Failure Events of Interest
IRADIC-RESHA Results
Redundancy Levels
Software Failure Probabilities
Software Failure Probabilities
Perform CCF Modeling and Estimation
Modified BFM
Estimate failure probability of entire DI&C systems
Quantified FTs
Importance Analysis
IRADIC Consequence Analysis
Risk Evaluation Acceptance Criterion-2: How reliable is the digital system with the identified digital failures?
System Modification
BBN Bayesian belief network
BFM Beta-factor model
FT fault tree
HRA human reliability analysis
ODC orthogonal defect classification
SDD software design description
SDLC software development life cycle
SRGM software reliability growth modeling
SRS software requirements specifications
STD systems test document

Figure 5. The framework of the multiscale quantitative reliability analysis.

After the small-scale reliability analysis of software and Type II interactions, a modified beta-factor model (BFM) is applied for the modeling and estimation of CCFs, especially for software CCFs. Finally, when the basic events of integrated FT are calculated, the failure probability of the entire DI&C system can be estimated using FTA tools. A CCF is the result of the existence of two main factors—a failure cause and a coupling factor (or mechanism) [19] [20] [21]. The failure cause is the condition to which failure is attributed. The coupling factor (or coupling mechanism) creates the condition for a failure cause to affect multiple components, thereby producing a CCF [19]. Often, CCF models attempt to simplify an analysis by assuming symmetry for components of the common cause component group (CCCG). For example, a CCCG may be created by assuming components are similar and that any subtle differences in coupling factors might be ignored. Nearly all CCF models rely on symmetry (e.g., the most notable exception being the BBN-based approaches) [22]. However, placing components into unique, coupling-factor-based CCCGs that account for the inconsistency between the groups may result in issues when relying on traditional techniques. Allowing a component to be part of multiple groups may lead to double counting of failure events or difficulties in quantification [15] [23].

In addition, most methods are designed to incorporate some form of operational data. A major challenge is the issue of limited data, which has a direct influence on all methods and nearly guarantees the dependence on elicitation techniques. Therefore, rather than making special exceptions for conventional methods, other options were investigated. One method from 2012 was specifically developed for the multiple CCCG scenario and is based on a ratio approach like that of the BFM [24]. This method, the modified BFM, was designed specifically to allow for components to be members of multiple CCCGs. The next challenge is to define and estimate the beta factors of the modified BFM given a limited data scenario while also providing consideration of the unique qualitative attributes for each CCCG. The partial beta-factor (PBF) was developed by R. A. Humphreys and Rolls-Royce and Associates [25] and later became part of Unified Partial Method (UPM) [26]. The PBF-A method was founded on the question, "What attributes of a system reduce CCFs?" [25] A collection of attributes, called sub-factors, were selected that are known to contribute to the prevention of CCFs. Each subfactor was weighted by reliability engineers for their importance. The methodology requires the analyst to assign a score (e.g., A, B, C, etc.) for each subfactor. An "E" indicates a component is well-defended against CCFs (i.e., A= worst, E = best). Beta is then determined as a function of the assigned scores. The model was arranged such that the upper and lower limits for beta correspond with values reported in literature [25]. This is ensured by the subfactor weighting and the denominator given in Equation (1). The beta value determined by this method is intended to be used with the BFM.

$$\beta = \frac{\sum(Sub - factors)}{d} \tag{1}$$

Where d is assumed to be 5100. The subfactor names alone are not sufficient to describe the details for assessing each actual subfactor; therefore, readers are advised to visit the original source material for making assessments. The advantage of employing this method is that it is simple to apply and allows for a more structured determination of beta than simple judgments. The provided model allows for qualitative features to be considered in the quantification of CCFs. An approach for performing CCF analysis given the limited data and multiple CCCGs was developed by integrating modified BFM and PBF. The approach relies on the modified BFM to account for multiple CCCGs and PBF to define beta factors for each CCCG. The hybrid approach provides a means to overcome the limitations of conventional methods. A formalized process relying on the modified BFM and PBF is shown in Figure 6. The primary sections headings of Figure 6 come from the descriptions of the CCF modeling processes found in existing sources [19] [22]. The subsequent section will demonstrate this process as part of a case study.

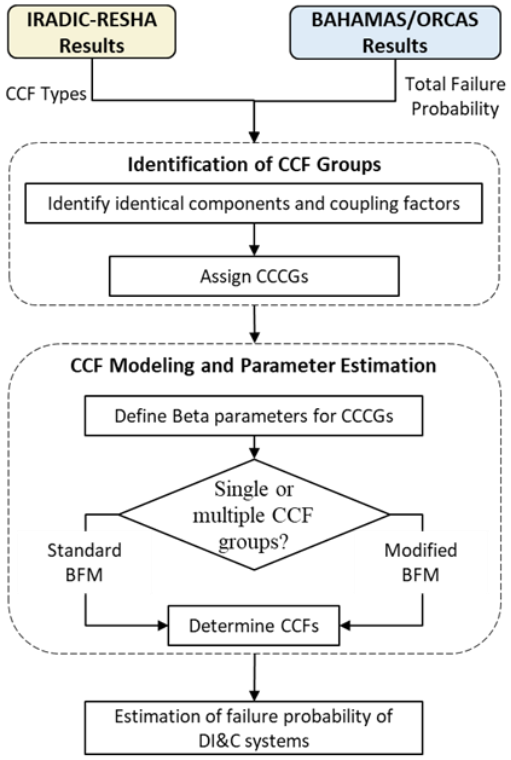
IRADIC-RESHA Results
BAHAMAS/ORCAS Results
CCF Types
Total Failure Probability
Identification of CCF Groups
Identify identical components and coupling factors
Assign CCCGs
CCF Modeling and Parameter Estimation
Define Beta parameters for CCCGs
Single or multiple CCF groups?
Standard BFM
Modified BFM
Determine CCFs
Estimation of failure probability of DI&C systems

Figure 6. A CCF modeling flowchart developed for software CCF modeling and estimation.

The results of the CCF analysis are shown in Table 1 and Table 2. Note that RACK, DIVISION, and ALL correspond to the CCCG categories, while INDIVIDUAL corresponds to individual component failure. The CCCG ALL column contains all the identical components within the system of interest. The given CCCG categories are not shared by all components; hence, there are no RACK CCCGs for the reactor trip breakers (RTBs). Regarding the results, there is a difference between the software and hardware CCCGs of the local coincidence logical (LCL) processors. The hardware CCCG for LCL processor is separated by location just like the BPs. However, the potential for DIVISION and RACK level CCFs are precluded from consideration because there is nothing to distinguish them from the CCCGs representing all LCL processors; according to the case study, each LCL processor has the same software and receives the same inputs. By contrast, the BPs have the potential for input variation amongst divisions. Thus, the BPs have DIVISON level software CCCGs, but the LCL processors do not. By assigning the failure probabilities into the integrated FTs of four-division digital RTS and ESFAS, the failure probabilities of these two systems can be calculated using the INL-developed probabilistic risk assessment (PRA) tool SAPHIRE [27].

Table 1. Hardware failure probability for RTS components.

Component	**INDIVIDUAL Failure**	**RACK CCF**	**DIVISION CCF**	**ALL CCF**	**Total**
BPs	4.000E-05	N/A	5.943E-06	2.187E-06	4.813E-05
LCL Processors	6.480E-05	1.076E-05	7.647E-06	3.961E-06	8.717E-05
DOMs	1.640E-05	1.706E-06	1.015E-06	1.983E-07	1.932E-05
Selective Relay	6.200E-06	N/A	6.073E-07	7.059E-08	6.878E-06
RTB-UV device	1.700E-03	N/A	N/A	1.763E-05	1.718E-03
RTB-Shunt device	1.200E-04	N/A	N/A	1.244E-06	1.212E-04
RTB RTSS1	4.500E-05	N/A	N/A	1.944E-06	4.694E-05
RTB RTSS2	4.500E-05	N/A	N/A	1.944E-06	4.694E-05

Table 2. Software failures probability for RTS components.

Component	**INDIVIDUAL Failure**	**RACK CCF**	**DIVISION CCF**	**ALL CCF**	**Total**
BPs	5.591E-07	N/A	1.062E-04	8.030E-05	1.871E-04
LCL Processors	8.086E-05	N/A	N/A	1.062E-04	1.871E-04

The main logic of this integrated RTS-FT was quantified with SAPHIRE 8 using a truncation level of 1E-12; RTS failure probability is 1.270E-6 with 13 cut-sets. Table 3 lists part of these cut-sets with significant contributions. Mechanical CCF of rod control cluster assembly (RCCA) is the main contributor (>95% of total); the software CCFs do not significantly affect the reliability of digital RTS because of the highly redundant design and high reliability of digital components. The ESFAS-FT was also quantified with SAPHIRE 8 using a truncation level of 1E-12; ESFAS failure probability is 2.095E-5 with one cut-set. Hardware CCF of ESF-component interface modules (ESF-CIMs) is the main contributor, and the software CCFs do not significantly affect the reliability of digital ESFAS because of the high-redundant design and high reliability of digital systems.

Table 3. Cut-sets for the improved RTS-FT.

FT Name	**#**	**Probability**	**Total %**	**Cut Sets**
Integrated RTS-FT	1	1.210E-6	95.31	RPS-ROD-CF-RCCAS
	2	2.052E-8	1.62	RPS-CCP-TM-CHA, RPS-TXX-CF-4OF6, RPS-XHE-XE-NSIGNL
	3	1.944E-8	1.53	RPS-XHE-XE-SIGNL, RTB-SYS-2-HD-CCF
	4	1.944E-8	1.53	RPS-XHE-XE-SIGNL, RTB-SYS-1-HD-CCF
	Total	1.270E-6	100	-

3.3 Consequence Analysis

To compare the changes of CDF after replacing the current simplified FTs of digital RTS and ESFAS with the integrated FTs in the generic PWR ET models, consequence analysis has been performed based on INT-TRANS (initiating event - general plant transient) with ATWS (anticipated transient without scram), LOSC (loss-of-seal cooling), SBLOCA (small-break loss-of-coolant accident), and MBLOCA (medium-break LOCA). This generic PWR SAPHIRE model represents the conditions of existing U.S. NPPs with traditional analog HSSSR DI&C systems. Integrated FTs of RTS and ESFAS include both software and hardware failures, particularly CCF, that may occur in a four-division digital RTS and a four-division digital ESFAS. Results show the CDF of INT-TRANS accident scenarios are reduced significantly. The generic PWR SAPHIRE model adopts one FT to represent the failure of a two-train RTS, consisting of hardware failures, operator errors, and failures due to external hazards. ESFAS failure is modeled using a basic event as a CCF of ESF actuation signal, which is embedded in the FTs of relevant safety features including auxiliary feedwater, high pressure injection and low pressure injection. This CCF basic event is included in cut-sets that have significant contributions to CDF.

By adding the integrated FTs of four-division digital RTS and ESFAS into the PRA models, the safety margin obtained from the plant digitalization on HSSSR DI&C systems are quantitatively estimated. For example, results show RTS failure probability is greatly reduced from 4.288E-6 to 1.270E-6; LPI failure probability greatly decreases from 8.416E-4 to 2.095E-4 due to the improvement of ESFAS-FT. This explains the significant reduction of CDF in these analyzed accident scenarios, as summarized in Table 4. Plant modernization, including the improvement of HSSSR DI&C systems such as RTS and ESFAS, will benefit plant safety by providing more safety margins to accident management. The numbers of cut-sets are also reduced due to the improved design from two-train analog I&C systems to four-division DI&C systems. As the complexity of the system increases, the number of failure combinations should also increase. However, with the improved design, the cut-set probabilities are reduced and truncated below the 1E-12 threshold hence the cut sets do now show up in the final results.

Table 4. Changes of ET CDFs by adding digital RTS and ESFAS FTs into ETs.

ETs	Original CDF	New CDF	Δ CDF	Δ CDF/ Original CDF
INT-TRANS	1.073E-6	5.769E-7	- 4.961E-7	- 46.23%
INT-SLOCA	7.784E-8	7.509E-8	- 2.720E-9	- 3.53%
INT-MLOCA	6.279E-7	4.984E-7	- 1.247E-7	- 20.62%

4 CONCLUSION

This paper documents the research activities that quantitatively evaluate CCFs (especially software CCFs) in HSSSR DI&C systems (e.g., four-division digital RTS and ESFAS) in NPPs using the LWRS-developed framework. The framework has been developed, demonstrated, and improved for the design of HSSSR DI&C systems with multilayer software CCFs, human interactions with these systems, and plant responses. This technology complements other approaches being developed for deploying DI&C technologies and emphasizes risk-informed approaches used to facilitate the adoption and licensing of HSSSR DI&C systems. Currently, only qualitative assessment is required for evaluating design attributes and quality measures of DI&C systems because there is no appropriate approach for performing quantitative assessment. To deal with the technical issues in addressing potential software CCF issues in HSSSR DI&C systems of NPPs, the LWRS-developed framework provides:

1. An integrated and best-estimate, risk-informed capability to address new technical digital issues quantitatively, accurately, and efficiently in plant modernization progress, such as software CCFs in HSSSR DI&C systems of NPPs.
2. A common and modularized platform for I&C designers, software developers, plant engineers, and risk analysts to efficiently prevent and mitigate risk by identifying crucial failure modes and system vulnerabilities, quantifying DI&C system reliability, and evaluating the consequences of digital failures on plant responses.

3. A technical basis and risk-informed insights to assist the NRC and industry in formalizing relevant licensing processes relevant to CCF issues in HSSSR DI&C systems.
4. An integrated risk-informed tool for vendors and utilities to meet the regulatory requirements and optimize the D3 applications in the early design stage of digital HSSSR systems.

Work in the near future includes the improvement of CCF modeling for software failures, the development of the reliability analysis method (i.e., ORCAS) for data-rich conditions, relevant validation and uncertainty quantification of these quantitative methods, and the adjustment of the framework on the risk assessment and design optimization of artificial intelligence (AI)-guided advanced control systems.

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.

References

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

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

[3] 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.

[4] Electric Power Research Institute, “Hazard Analysis Methods for Digital Instrumentation and Control Systems,” EPRI, Palo Alto, CA, 2013.

[5] N. G. Leveson and J. P. Thomas, STPA Handbook, March 2018.

[6] *Guidance for Addressing CCF in High Safety Significant Safety-related DI&C Systems,* NEI, July 1, 2021.

[7] U.S.NRC, “Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” U.S.NRC, Washington, D.C., 2002.

[8] 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.

[9] H. Zhang, H. Bao, T. Shorthill and E. Quinn, “An Integrated Risk Assessment Process of Safety-Related Digital I&C Systems in Nuclear Power Plants,” 17 Dec 2021. [Online]. Available: arXiv preprint arXiv:2112.09287. [Accessed 2022].

[10] H. Bao, H. Zhang, T. Shorthill and S. Lawrence, “Quantitative Evaluation of Common Cause Failures in High Safety-significant Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants,” 7 April 2022. [Online]. Available: https://arxiv.org/abs/2204.03717. [Accessed 2022].

[11] 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,” *Nuclear Technology,* 2021.

[12] H. Bao, T. Shorthill and H. Zhang, “Hazard Analysis for Identifying Common Cause Failures of Digital Safety Systems using a Redundancy-Guided Systems-Theoretic Approach,” *Annals of Nuclear Energy,* vol. 148, p. 107686, 2020.

[13] H. Bao, H. Zhang and T. Shorthhill, “Redundancy-guided System-theoretic Hazard and Reliability Analysis of Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants,” Idaho National Laboratory, Idaho Falls, ID, 2020.

[14] T. Shorthill, H. Bao, Z. Hongbin and H. Ban, “A novel approach for software reliability analysis of digital instrumentation and control systems in nuclear power plants,” *Annals of Nuclear Energy,* vol. 158, 2021.

[15] H. Bao, T. Shorthill, E. Chen and H. Zhang, “Quantitative Risk Analysis of High Safety-significant Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants using IRADIC Technology,” Idaho National Laboratory, Idaho Falls, ID, August 2021.

[16] U.S.NRC, “Guidance for Evaluation Of Diversity And Defense-In-Depth In Digital Computer-Based Instrumentation And Control Systems Review Responsibilities,” U.S.NRC, Wshington, D.C., August 2016.

[17] L. Lin, H. Bao and N. Dinh, “Uncertainty quantification and software risk analysis for digital twins in the nearly autonomous management and control systems: A review,” *Annals of Nuclear Energy,* vol. 160, p. 108362, 2021.

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

[19] A. Mosleh, D. Rasmuson and F. Marshall, “Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment,” NUREG/CR-5485, U.S. Nuclear Regulatory Commission, Washington, DC, 1998.

[20] G. W. Parry, “Common Cause Failure Analysis: A Critique and Some Suggestions,” *Reliability Engineering and System Safety,* vol. 34, no. 3, pp. 309-326, 1991.

[21] H. M. Paula, D. J. Campbell and D. M. Rasmuson, “Qualitative cause-defense matrices: Engineering tools to support the analysis and prevention of common cause failures,” *Reliability Engineering & System Safety,* vol. 34, no. 3, pp. 389-415, 1991.

[22] A. O'Connor and A. Mosleh, “A General Cause Based Methodology for Analysis of Dependent Failures in System Risk and Reliability Assessments,” University of Maryland, 2013.

[23] Z. Ma, R. F. Buell, J. K. Knudsen and S. Zhang, “Common-Cause Component Group Modeling Issues in Probabilistic Risk Assess,” Idaho National Laboratory, Idaho Falls, ID, 2020.

[24] D. Kancev and M. Cepin, “A new method for explicity modelling of single failure evetn within different common cause failure groups,” *Reliability Engineering and System Safety,* vol. 103, pp. 84-93, 2012.

[25] R. A. Humphreys, “Assigning a Numerical Value to the Beta Factor Common Cause Evaluation,” in *Reliability '87*, 1987.

[26] V. P. Brand, Ed., UPM 3.1: A pragmatic approach to dependent failures assessment for standard systems, SRDA-R13, Warrington, UK: AEA Technology, Safety and Reliability Directorate, 1996.

[27] U.S. Nuclear Regulatory Commission, “Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8.0,” U.S. Nuclear Regulatory Commission, Washington, D.C., 2011.