INL/EXT-19-55219

Light Water Reactor Sustainability Program

An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants

Han Bao, Hongbin Zhang, Kenneth Thomas

August 2019

U.S. Department of Energy–Office of Nuclear Energy

INL/EXT-19-55219

An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants

Han Bao, Hongbin Zhang, Kenneth Thomas

August 2019

Idaho National Laboratory
Idaho Falls, Idaho 83415

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

SUMMARY

Most of the existing nuclear power plants (NPPs) in the world rely on traditional analog instrumentation and control (I&C) systems for monitoring, control, and protection functions. With the industrial base largely moving to digital systems, the operation and maintenance of plants involves managing issues including 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 (e.g., fault tolerance, self-testing, signal validation, process system diagnostics). Therefore, the U.S. nuclear power industry has initiated the replacement of existing, aging analog systems with digital I&C technology, and is developing new designs for advanced plants using digital systems in integrated control rooms to provide modern control and protection systems. However, the qualification of digital I&C systems remains a challenge, especially the issue of software common cause failure (CCF), which has been difficult to address.

A CCF is the malfunction of two or more plant components or functions due to a single failure source. CCFs have the potential to generate unanalyzed events or sequences that may not be bounded by previous plant accident analyses, therefore, to challenge the plant safety. Existing analyses on CCF in I&C systems are mainly focusing on hardware failures. With the application and upgrades of new digital I&C systems, software CCFs due to design flaws have become a potential threat to plant safety considering most redundancy designs are using the similar digital platforms or software in the operating and application systems. With complex multi-layer redundancy designs to meet the single failure criterion, these I&C safety systems are of a particular concern in the U.S. Nuclear Regulatory Commission (NRC) licensing procedures.

Therefore, there is a need to develop an integrated risk assessment strategy with digital CCF and plant transient responses considered to assure the long-term safety and reliability of vital digital systems and reduce uncertainties in costs, time, and support integration of digital systems in the plant. The overall goal of this project is to deliver a strong technical basis to support effective, licensable, and secure digital I&C technologies for the digital upgrades to existing NPPs. To deal with the expensive licensing justifications from regulatory insights, this technical basis is instructive for nuclear vendors and utilities to effectively lower the costs associated with digital compliance and speed-up industry advances by: (1) defining an integrated risk-informed analysis process for digital I&C upgrades including hazard analysis, reliability analysis, and consequence analysis; (2) applying systematic and risk-informed tools to address CCFs and quantify responding failure probabilities for digital I&C technologies; (3) evaluating the impact of digital failures at the individual level, system level, and plant level; and (4) providing insights and suggestions on designs to manage the risks, thus to support the development, licensing, and deployment of advanced digital I&C technologies on NPPs.

Upgrading digital I&C (safety and non-safety-related) systems in existing NPPs within a cost-effective and regulatory acceptable way offers the foremost means of performance improvements and cost-reductions for existing NPPs. One key outcome of this project is to perform plant-specific risk assessment to provide a sustainable scientific support for enabling industry to balance the digital-related risks, costs, reliability, and safety.

CONTENTS

FIGURES

TABLES

ACRONYMS

1D/2D/3D	one, two, or three-dimensional (respectively)
AC	Acceptance Criteria
AFWS	Auxiliary FeedWater System
ANS	American Nuclear Society
AOO	anticipated operational occurrence
APC-S	Auxiliary Process Cabinet–Safety
APR-1400	Advanced Power Reactor 1400 MW
ATWS	Anticipated Transient Without Scram
BBN	Bayesian Belief Network
BDBA	beyond design basis accident
BEPU	Best Estimate Plus Uncertainty
BP	bistable processor
CAFTA	Computer-Aided Fault Tree Analysis System
CASL	Consortium for the Advanced Simulation of Light Water Reactors
CCF	common cause failure
CDF	core damage frequency
CEDM	control element drive mechanism
CFR	Code of Federal Regulations
CHF	critical heat flux
CMFD	coarse mesh finite difference
COBRA	Coolant Boiling in Rod Arrays
CPCS	Core Protection Calculator System
CPU	central processing unit
CSARP	International Cooperative Severe Accident Research Program
CSAU	Code Scaling, Applicability, and Uncertainty
CSS	Containment Spray System
CTF	COBRA – Two Fluid subchannel thermal-hydraulics analysis code
DBA	design basis accident
DiD	defense-in-depth
DNB	departure from nuclear boiling
DNBR	departure from nuclear boiling ratio
DOE	U.S. Department of Energy
DOE–NE	U.S. Department of Energy–Office of Nuclear Energy

ECCS	Emergency Core Cooling System
ECRR	Equivalent Cladding Reacted Ratio
EMDAP	Evaluation Model Development and Application
ENFMS	Ex-core Neutron Flux Monitoring System
EPRI	Electric Power Research Institute
EPR	evolutionary power reactor
ESF	engineered safety features
ESF-CCS	Engineered Safety Features-Component Control System
ESFAS	Engineered Safety Features Actuation System
ET	Event Tree
ETA	Event Tree Analysis
FMEA	Failure Mode Effect Analysis
FPGA	Field Programmable Gate Array
FRAPTRAN	Fuel Rod Analysis Program Transient
FT	Fault Tree
FTA	Fault Tree Analysis
F-V	Fussel-Vesely
FY	Fiscal Year
GDC	General Design Criteria
HAZCADS	HAZards and Consequence Analysis for Digital Systems
HFE	human failure event
HRA	Human Reliability Analysis
HVAC	heating, ventilation, and air-conditioning
I&C	instrumentation and control
IAP	Integrated Action Plan
INL	Idaho National Laboratory
ISO	International Organization for Standardization
LCL	local coincidence logic
LERF	large early release frequency
LOCA	loss of coolant accident
LOTUS	LOCA analysis toolkit for the U.S.
LWR	light water reactor
LWRS	Light Water Reactor Sustainability
MAAP	Modular Accident Analysis Program

MELCOR	Methods for Estimation of Leakages and Consequences of Releases
MIT	Massachusetts Institute of Technology
MOC	method of characteristics
MOOSE	Multi-Physics Object-Oriented Simulation Environment
MP-BEPU	Multi-Physics Best Estimate Plus Uncertainty
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
PCTR	Peak Cladding Temperature Ratio
PIRT	Phenomenon Identification and Ranking Table
PNNL	Pacific Northwest National Laboratory
PPS	Plant Protection System
PRA	Probabilistic Risk Assessment
PSA	probabilistic safety assessment
PW	Prevention Worth
R&D	research and development
RADIC	Risk Assessment for Digital I&C
RAW	Risk Achievement Worth
RCS	Reactor Coolant System
RD&D	research, development, and deployment
RELAP5-3D	Reactor Excursion and Leak Analysis Program 5 with 3D capability
RES	NRC–Office of Nuclear Regulatory Research
RG	Regulatory Guide
RI-MP-BEPU	Risk-Informed Multi-Physics Best Estimate Plus Uncertainty
RISA	Risk-Informed Systems Analysis
RISMC	Risk-Informed Safety Margin Characterization
RMS	Radiation Monitoring System
RPS	Reactor Protection System
RTS	Reactor Trip System
RTSS	Reactor Trip Switchgear System
SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations
SIS	Safety Injection System
SNL	Sandia National Laboratories
SPOF	single point of failure

SRP	Standard Review Plan
SSC	system, structure, and component
STPA	Systems-Theoretic Process Analysis
TEPA	Top Event Prevention Analysis
U.S.	United States
UCA	unsafe control action
VERA-CS	Virtual Environment for Reactor Applications-Core Simulator

An Integrated Risk Assessment Process for Digital Instrumentation and Control Upgrades of Nuclear Power Plants

1. INTRODUCTION

1.1 Background

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 some certain environmental conditions, the primary concern with the extended analog systems comes from the effects of aging (e.g., mechanical failures, environmental degradation, and obsolescence) [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 some 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 (e.g., fault tolerance, self-testing, signal validation, process system diagnostics) [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]: (1) the application of new digital technology also introduces new potential software-based hazards in critical safety and control functions; (2) underlying technical infrastructure and regulatory framework require some changes since much of the experience from analog technology may not be suitable for the applications of digital I&C; (3) some technical problems have been identified from the applications of digital I&C in NPPs, such as common-mode failure and common cause failure (CCF) in software, commercial dedication of hardware and software, possible lack of on-site plant experience with the new technology and systems, configuration management, increased complexity leading to possible programming errors and incorrect outputs, environmental sensitivity, reliability of standard software tools, and the effects of plant margin of safety; (4) 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; and (5) the industry and regulators have less experience with this new technology and a lack of consensus on issues underlying the evaluation and adoption of digital I&C technology. As a result, the definition of licensing criteria must follow systematic study and risk assessment of different technical viewpoints.

For these reasons, the nuclear industry and regulators have made considerable efforts on addressing the technical and regulatory aspects of digital qualifications, especially digital CCFs. A CCF is the malfunction of two or more plant components or functions due to a single failure source. CCFs have the potential to generate an unanalyzed event or sequence that may not be bounded by previous plant accident analyses, therefore, to challenge plant safety [3]. A general conclusion from Probabilistic Risk Assessments (PRAs) of commercial NPPs is that CCFs are significant contributors to the unavailability of safety systems [4]. Existing analyses on CCF in I&C systems are mainly focusing on hardware failures. With the application and upgrades of new digital I&C systems, software CCFs due to design flaws in software, have become a potential threat to plant safety considering most redundancy designs are using the similar digital platforms or software in the operating and application systems.

Redundancy is an important design principle for achieving high reliability in systems important to

safety, and for meeting the single failure criterion for safety systems. I&C systems in NPPs normally have different functions as monitoring, control, and protection. According to their being consistent with defense-in-depth (DiD) principles, these I&C systems are divided to two categories: non-safety systems and safety systems. Non-safety I&C systems are used by operators to monitor and control the normal operation of the plant, and to mitigate and prevent plant operational transients. As a backup of non-safety systems, 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 Reactor Trip Systems (RTSs) and engineered safety features (ESF) systems, are of a particular concern in U.S. Nuclear Regulatory Commission (NRC) licensing procedures, especially considering potential software CCFs may generate unanalyzed plant conditions because the transient and accident analyses for existing U.S. plants was only considering the failures applicable to analog I&C technology [1].

To deal with these challenges, the NRC has started to update its regulatory infrastructure and processes since late 1990s. 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 (GDC) in Title 10 of the Code of Federal Regulations (CFR) 50, Appendix A [5]. In 2016, the NRC revised the Standard Review Plan (SRP) to fully adapt it and the associated Regulatory Guides (RGs) to digital I&C systems [6]. 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. The NRC PRA policy statement encourages the use of risk information in all regulatory activities supported by the state-of-the-art and data [7]. Activities on developing digital system models have been in process for some time; however, there are still no generally accepted approaches 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 [8]. Currently, the NRC continues to perform research that supports the development of licensing criteria to evaluate new digital I&C systems. To address the principles of the NRC's direction in the Staff Requirements Memorandum SECY-15-0106 [9], the NRC staff developed the Integrated Action Plan (IAP) and updates the plan as a living document. The IAP considers the broad context of digital I&C regulatory challenges and focuses on improving the regulatory infrastructure so that it integrates performance-based and technology neutral engineering concepts for safety assurance [10].

Digital I&C systems for NPPs have similar technological characteristics to those for other safety-critical applications in chemical plants and aircraft: equipment, response time, input and output range, and accuracy [1]. However, digital I&C systems for NPPs have higher levels of requirements on reliability, safety, and security under a wide range of conditions, because of the potentially greater consequences of accidents in NPPs. The application of digital-based systems and components raises certain technical issues, which particularly focus on the new hazards and failure modes caused by software or other digital system design flaws that may defeat existing protective features. The potential for these new digital failures to cause a single component/system failure or even failures of multiple systems/components, especially in digital safety systems, may propagate new unanalyzed events or sequences. Therefore, appropriate risk assessment strategies are needed to identify the digital-induced failures, implement reliability analysis on related digital safety I&C systems and evaluate the unanalyzed sequences introduced by these failures at the plant level. It is beneficial to perform risk assessment at early design phases to provide feedbacks back for different design phases, considering a CCF of redundant digital I&C systems could result in the complete loss of safety function or auxiliary systems that support safety systems. Therefore, the need clearly exists to develop a risk assessment strategy to assure the long-term safety and reliability of vital digital systems and reduce uncertainties in costs, time, and support integration of digital systems in the plant.

1.2 Goals & Scope

The overall goal of this project is to deliver a strong technical basis to support effective, licensable, and secure digital I&C technologies by developing a risk assessment strategy for digital upgrades/designs. To deal with the expensive licensing justifications from regulatory insights, this technical basis is instructive for nuclear vendors and utilities to effectively lower the costs associated with digital compliance and speed industry advances by:

(1). Defining an integrated risk-informed analysis process for digital I&C upgrade, including hazard analysis, reliability analysis, and consequence analysis.

(2). Applying systematic and risk-informed tools to address CCFs and quantify responding failure probabilities for digital I&C technologies.

(3). Evaluating the impact of digital failures at the individual level, system level, and plant level.

(4). Providing insights and suggestions on designs to manage the risks; thus, to support the development, licensing, and deployment of advanced digital I&C technologies on NPPs.

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

The integrated Risk Assessment for Digital I&C (RADIC) process developed for this strategy requires the cooperation of system engineers, I&C design and software engineers, PRA and risk analysts, data analysts, and multi-physics analysts. The RADIC process targets to both digital non-safety and safety systems. Considering there are some efforts focusing on hazard and reliability analysis on non-safety systems, the RADIC process will be demonstrated on the risk assessment of digital safety systems, such as RTSs and Engineered Safety Features Actuation Systems (ESFASs), which have more redundancy designs and therefore more potential CCFs than non-safety systems. The applicability of this integrated process ranges from small replacements of individual analog components to complete upgrades or new designs of the entire digital systems. Each change on the systems, no matter small-scale or large-scale, should go through the risk assessment process, especially for safety systems.

Both hardware and software failures are considered in the RADIC process. In previous PRAs for traditional analog systems of NPPs, hardware failures are the focus compared to sensor failures and human errors. There are several mutual approaches in the identification of hardware failures that use hardware component failure data together with operational profile forecasts to estimate the probability of failure for hardware systems, structures, and components (SSCs). Even for digital-based systems, hardware SSCs still provide physical boundaries, bases, and carriers for software or digital platforms. Considering a random hardware failure may trigger a software CCF, hardware failures will still be analyzed in the RADIC process. In addition, the Systems-Theoretic Process Analysis (STPA) method will be used to identify systematic software failures, which have a large potential to be CCFs if identified in a redundancy design.

The risk assessment strategy proposed in this project includes two phases: risk analysis and risk evaluation. Risk analysis aims to identify hazards of digital-based SSCs, estimate their failure probabilities, and analyze relevant consequences by performing hazard analysis, reliability analysis, and consequence analysis. The results from the risk analysis phase are compared with the specific risk acceptance criteria in the risk evaluation phase. The schematic of the risk assessment strategy for digital I&C systems is displayed in Figure 1. Hazard analysis focuses on identifying both software and hardware failures by respectively using the Fault Tree Analysis (FTA) and STPA methods, and building integrated Fault Trees (FTs) for the failure top events of the system of interest. The acceptance criterion for hazard analysis is whether the individual digital failure leads to the loss of function of the digital system. Hazard

analysis is supposed to provide integrated FTs for the failure top events, which includes both software and hardware failures. Reliability analysis aims to quantify the basic events of these integrated FTs, perform importance measures on the basic component combinations, and build event trees (ETs) for the consequence analysis of digital system failures. The acceptance criterion for reliability analysis is whether the digital system of interest is still reliable with the identified digital failures. Consequence analysis conducts uncertainty and sensitivity analysis within a multi-scale and multi-physics environment to fully evaluate the impact of the consequences of digital system failures identified in the reliability analysis. The acceptance criterion for consequence analysis is whether the consequences of digital failures are acceptable at the plant level. If all of the acceptance criteria are satisfied, the digital I&C systems of interest are safe enough for application. Otherwise, redesign is required to improve the safety of these systems. In this project, the RADIC process is developed based on the schematic of this risk assessment strategy, which integrates the risk analysis phase and the risk evaluation phase, and provides technical support for hazard analysis, reliability analysis, and consequence analysis.

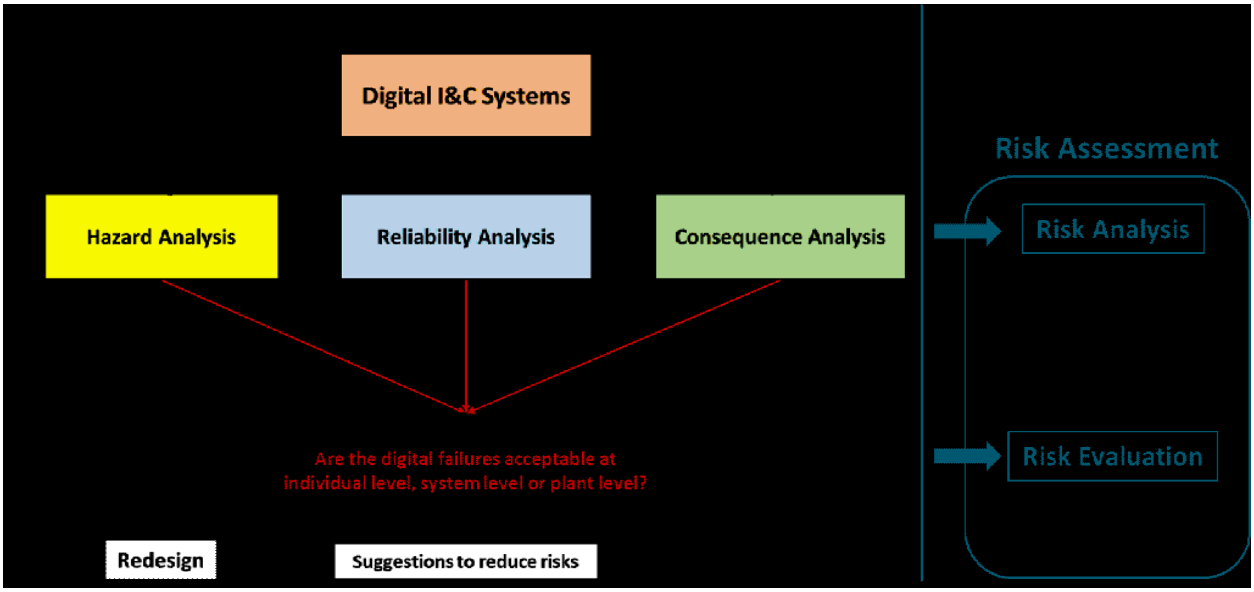


Figure 1. Schematic of proposed risk assessment strategy for digital I&C systems.

The outputs of this research effort will be part of the Risk-Informed Systems Analysis (RISA) Research and Development (R&D) Plan, which is integrated with industry efforts to recover operating/safety margins, and reduce operating/safety costs by supporting the development and employment of digital (non-)safety I&C technologies, with the ultimate goal of risk-informing NPP activities while maintaining plant safety.

1.3 Report Structure

This report consists of ten chapters. Chapter 2 defines the key concepts involved in the risk assessment process of digital I&C systems. Relevant technical approaches and methods are reviewed in Chapter 3. Chapter 4 describes the proposed RADIC process at the individual, system, and plant levels. Chapter 5 and 6 respectively introduce the industry collaboration and R&D activities for the development and deployment of the RADIC process. Chapter 7 presents the computer codes that might be applied in the RADIC process. Chapter 8 and 9 provides the project schedule and anticipated outcomes of the project. References are listed in Chapter 10.

2. KEY CONCEPTS

2.1 Definitions of Analysis Approaches

Risk Analysis: Systematic use of available information to identify hazards and estimate the risk to individuals, property, and the environment [11]. As a proactive approach to deal with potential accidents, risk analysis normally includes four main steps: (1) identify hazards/define potential accident scenarios; (2) estimate the potential accident frequency; (3) evaluate the event consequences; and (4) estimate the risk [12].

Risk Evaluation: A process in which judgements are made on the tolerability of the risk on the basis of a risk analysis and taking into account factors such as socioeconomic and environmental aspects [11]. Risk evaluation includes a comparison of risk analysis results with specific risk acceptance criteria [13].

Risk Assessment: An overall process of risk analysis and risk evaluation. Risk assessment provides a structured process that identifies how objectives may be affected, and analyzes the risk in terms of consequences and their probabilities before deciding on whether further treatment is required [11]. A risk assessment analyzes what can go wrong, how likely it is to happen, what the potential consequences are, and how tolerable the identified risk is [13]. Risk assessment is necessary for both individual digital failures, and the impact of their consequences at the system and plant levels.

Hazard Analysis: In this work, hazard analysis is defined as an integrated process to identify individual software and hardware hazards by using FTA and STPA, and to build an integrated FT for the failure top events of the system of interest. According to appropriate requirements and constraints, the risks associated with these hazards are evaluated in the individual-level risk assessment. The acceptance criterion is whether the digital failures are acceptable for the function of a digital I&C safety/non-safety system.

Reliability Analysis: In this work, reliability analysis is defined as a process to: (1) quantify probabilities of basic events for software failures, hardware failures and human factors; (2) perform importance measures on the basic component combinations; and (3) construct ETs and quantify the probabilities of consequences of digital system failures. Based on reliability analysis, system-level risk assessment is performed to evaluate the reliability of digital I&C systems. The acceptance criterion is whether the digital I&C system is still reliable considering the identified digital failures.

Consequence Analysis: Assessment of the radiological consequences (e.g., doses, activity concentrations) of normal operation and possible accidents associated with an authorized facility or part thereof [14]. In this work, consequence analysis is defined as a process to conduct uncertainty and sensitivity analysis within a multi-scale and multi-physics environment to fully evaluate the impact of the consequences of digital system failures, which are identified in the reliability analysis. Based on the uncertainty studies and limit surfaces for different scenarios, a plant-level risk assessment is performed to investigate whether the consequences of digital failures are acceptable at the plant level.

Systems-Theoretic Process Analysis (STPA): A hazard analysis method that is part of a relatively new set of system safety methods being developed at the Massachusetts Institute of Technology (MIT), the STPA describes how undesired outcomes (e.g., losses) can result from inadequate enforcement of constraints (e.g., control) on the design, development, and operation of systems to achieve desired objectives. The STPA asserts that system losses result from flawed interactions between physical components, engineering activities, operational mission, organizational structures, and social factors [15].

Fault Tree Analysis (FTA): A deductive failure analysis that focuses on one undesired event and provides a method for determining the causes of the event. The undesired event constitutes the top event in a FT diagram constructed for the system, and generally consists of a complete or catastrophic failure, as mentioned above [16].

HAZards and Consequence Analysis for Digital Systems (HAZCADS): A logic and qualitative methodology for assessing hazardous states and consequences that can be initiated and/or propagated by digital systems. HAZCADS, jointly developed by Sandia National Laboratories (SNL) and Electric Power Research Institute (EPRI), integrates elements of the STPA and FTA processes, respectively [17].

Probabilistic Risk Assessment (PRA): A system scenario-based process that uses a combination of FTs, ETs, event sequence diagrams, and probability and statistical data to analyze the risk of a system, a process, or an activity. The NRC uses PRA to estimate risk by computing real numbers to determine what can go wrong, how likely it is, and what its consequences are. Thus, PRA provides insights into the strengths and weaknesses of the design and operation of NPPs [18].

Event Tree Analysis (ETA): A forward, bottom-up, logical modeling technique for both success and failure that explores responses through a single initiating event and lays a path for assessing probabilities of the outcomes and overall system analysis [18]. This analysis technique is used to analyze the effects of functioning or failed systems given that an event has occurred.

Human Reliability Analysis (HRA): A comprehensive and structured methodology that applies qualitative and quantitative methods to assess the human contribution to risk [19].

Top Event Prevention Analysis (TEPA): TEPA is a technique for choosing a collection of elements of a risk model having the property that credit for these elements alone is sufficient to satisfy a "prevention criterion." A collection of elements satisfying a prevention criterion is a "prevention set." Given a model with more than enough elements to satisfy a prevention criterion, TEPA shows how to choose subsets of model elements that satisfy the prevention criterion and optimize figures of merit, such as cost. Given a conceptual model taking credit for design features under consideration, TEPA can show which combinations of design features are capable of satisfying the criterion, and thereby support not only classification, but the design itself [20].

Redundancy: Provision of alternative (identical or diverse) structures, systems and components, so that anyone can perform the required function regardless of the state of operation or failure of any other. Redundancy is an important design principle for achieving high reliability in systems important to safety, and for meeting the single failure criterion for safety systems. Redundancy enables failure or unavailability of at least one set of equipment to be tolerated without loss of the function [14].

Event: In the context of the reporting and analysis of events, an event is any occurrence unintended by the operator—including operating error, equipment failure, or other mishap—and deliberate action on the part of others, the consequences or potential consequences of which are not negligible from the point of view of protection or safety [14].

Safety: The achievement of proper operating conditions, the prevention of accidents, or the mitigation of accident consequences, resulting in the protection of workers, the public, and the environment from undue radiation hazards.

Security: The prevention and detection of and response to, theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving nuclear material, other radioactive substances, or their associated facilities [14].

2.2 Faults and Failures

Fault: The abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function [21].

Failure: The inability of an SSC to function within acceptance criteria [14]. 'Failure' is an event, as distinguished from a 'fault,' which is a state. Failure can be activated from a fault by specific triggers. In this report, a failure of a digital I&C system results from hardware and software failures. Some of these failure sources divides into independent failures and CCFs.

Single Failure: A failure that results in the loss of the capability of a system or component to perform its intended safety function(s), and any consequential failure(s) resulting from it [14]. Multiple failures resulting from a single occurrence are considered as a single failure.

Single Failure Criterion: In [22], this is defined as "a requirement that a system which is designed to carry out a defined safety function must be capable of carrying out its mission in spite of the failure of any single component within the system or in an associated system which supports its operation."

Common Cause Failure (CCF): Failure of two or more SSCs due to a single specific event or cause [14]. The event or cause may be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human-induced event, or an unintended cascading effect from any other operation or failure within the plant. CCFs may also occur when a number of the same type of components fail at the same time. This may be due to reasons such as a change in ambient conditions, a saturation of signals, repeated maintenance error, or design deficiency.

Random Failure: Failures that can occur unpredictably during the lifetime of a hardware element, and that follow a probability distribution [21]. Hardware failures mainly belong to random failure due to manufacturing defects and aging and environmental effects.

Systematic Failure: Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors [21]. Systematic failures are considered as a direct result of some design or procedure problem. They occur when a set of circumstances happen to reveal the fault. Such failures cannot be prevented with simple redundancy.

Software is defined by the International Organization for Standardization (ISO) as "all or part of the programs, procedures, rules, and associated documentation of an information processing system" [23]. This definition includes executable software, as well as related software, firmware, documentation (e.g., requirements, design, user manuals, etc.), and data. In [24], software is defined as being composed mainly of a sequence of instructions executed on a central processing unit (CPU), the logical structure of massive parallel logic devices such as Field Programmable Gate Arrays (FPGAs) or programmable logic devices, as well as all combinations that may be implemented in an I&C system. The software also comprises all data determining the execution of calculations in the I&C system.

Software Failure: Generally, software failures are systematic; however, a software fault can be activated into a software failure by a random hardware failure. In addition, there are several reasons for software failures as classified in [24]:

(1) Software was designed incorrectly due to latent design errors, which were not detected by verification and validation or confidence-building measures performed before operational service. These errors lead to failures during the operational life of the software.

(2) The operational environment has changed, which is beyond the previously set requirements even software still works as designed (e.g., modifications in plant equipment or operator procedures).

(3) Software works as required and designed, but in specific conditions it does not function as expected due to incorrect analysis during the requirements definition/capture phase. Based on experience, software is not subject to manufacturing defects or aging and environmental effects.

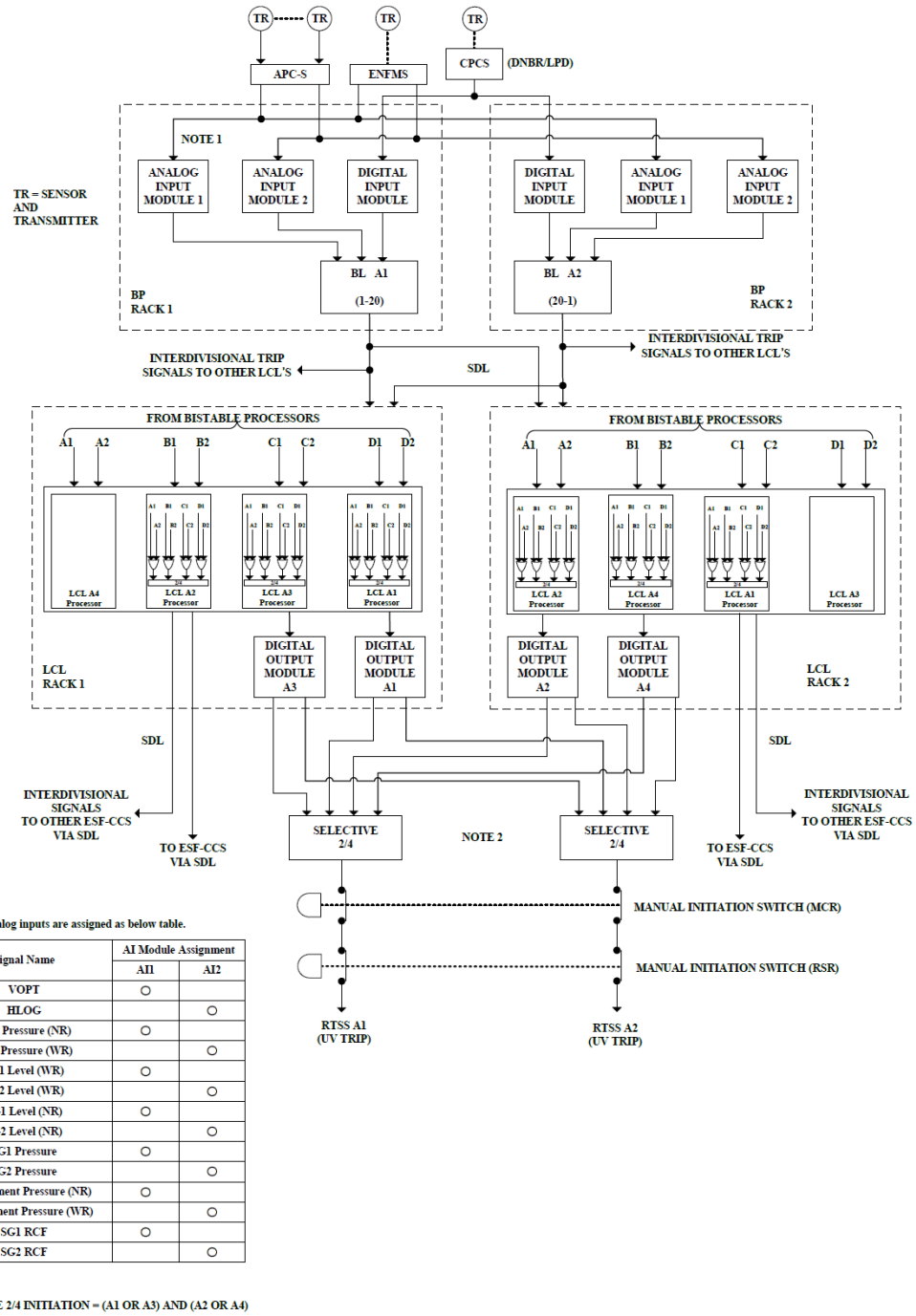
2.3 Identification of Digital Safety I&C Systems

The definitions discussed below were compiled from the NRC Advanced Power Reactor 1400 MW (APR–1400) Design Control Document, Chapter 7: Instrumentation and Controls, Rev. 3 [25].

Plant Protection System (PPS) is a safety system that includes electrical systems; electric, network, and mechanical devices; and circuits that perform the following protective functions:

(a). Reactor Protection System (RPS): The portion of the PPS that acts to trip the reactor when required. RPS functions protect the core fuel design limits and Reactor Coolant System (RCS) pressure boundary following anticipated operational occurrences (AOOs) and provide assistance in mitigating the consequences of postulated accidents. The RPS portion of the PPS includes the following functions: bistable trip logic, local coincidence logic (LCL), reactor trip initiation, and testing.

(b). Engineered Safety Features Actuation System (ESFAS): The portion of the PPS that activates the engineered safety features (ESF) systems. Figure 2 shows a sample PPS trip path diagram.



NOTE 1 Analog inputs are assigned as below table.

Signal Name	AI Module Assignment	
	AI1	AI2
VOPT	○	
HLOG		○
PZR Pressure (NR)	○	
PZR Pressure (WR)		○
SG1 Level (WR)	○	
SG2 Level (WR)		○
SG1 Level (NR)	○	
SG2 Level (NR)		○
SG1 Pressure	○	
SG2 Pressure		○
Containment Pressure (NR)	○	
Containment Pressure (WR)		○
SG1 RCF	○	
SG2 RCF		○

NOTE 2
SELECTIVE 2/4 INITIATION = (A1 OR A3) AND (A2 OR A4)

Figure 2. PPS Channel A trip path diagram [25].

Reactor Trip System (RTS) is a safety system that initiates reactor trips. The RTS consists of sensors, Auxiliary Process Cabinet–Safety (APC-S) cabinets, Ex-core Neutron Flux Monitoring System (ENFMS) cabinets, Core Protection Calculator System (CPCS) cabinets, the RPS portion of the PPS cabinets and Reactor Trip Switchgear System (RTSS). The RTS initiates a reactor trip based on the signals from the sensors that monitor various Nuclear Steam Supply System (NSSS) parameters and the containment pressure. When a safety limit is approached, the RTS initiates a signal that opens the reactor trip breakers. This action removes power from the control element drive mechanism (CEDM) coils, permitting the rods to fall by gravity into the core. The rapid negative reactivity insertion causes the reactor to shut down.

Engineered Safety Features (ESF) Systems: An ESF system is a safety system that includes the actuation systems of ESF and the components that perform protective actions after receiving a signal from the ESFAS or the operator. In the APR–1400 design, the ESF system consist of the following systems: the containment isolation system; the main steam isolation system; the Safety Injection System (SIS); the Auxiliary FeedWater System (AFWS); the Containment Spray System (CSS); the fuel handling area heating, ventilation, and air-conditioning (HVAC) system; the containment purge system, the control room HVAC system containment combustible gas control system (manual), and other supporting systems. The ESF system also includes sensors, APC-S cabinets, the ESFAS portion of the PPS, the safety portion of the Radiation Monitoring System (RMS), and the ESF-Component Control System (ESF-CCS). The ESFAS portion of the PPS includes the following functions: bistable trip logic, LCL, ESFAS initiation, and testing function. The ESF-CCS receives ESFAS initiation signals from the PPS and RMS, the electrical panel, or from the operators. The ESF-CCS generates ESF actuation signals to actuate the ESF system equipment. The ESF-CCS also generates emergency diesel generator-loading sequencer signals following the loss of offsite power. The control circuitry for the components provides the proper sequencing and operation of ESF systems.

3. TASKS AND TECHNICAL APPROACHES

Based on the schematic of the proposed risk assessment strategy for digital I&C systems, this chapter provides a list of the tasks that should be implemented in the integrated RADIC process. Relevant technical approaches and methods were reviewed for hazard analysis, reliability analysis, and consequence analysis. The goal of this chapter is to clarify the tasks and provide technical basis for the development and application of the RADIC process.

3.1 Tasks of the Risk Assessment for Digital I&C Systems

Considering the upgrades and new designs of digital (non-)safety I&C SCCs ranging from a small scale like a digital processor up to a large scale like the entire PPSs, and that digital systems can be vulnerable to random hardware failures and systematic software CCFs, this proposed RADIC process should be implemented in a DiD and diversity way, and have the flexibility, applicability, and capability to identify, quantify, and evaluate the risks at the individual, system, and plant levels.

Therefore, the tasks of the RADIC process are to evaluate whether the risk from digital failures can be accepted at the individual, system, and plant levels. The acceptance criteria should be determined in these three levels to ensure that the risk assessment is implemented in a DiD and diverse way. To meet the different acceptance criteria in the three levels, corresponding risk analysis stages are required for the hazard analysis, reliability analysis, and consequence analysis, as listed in Table 1.

Table 1. Tasks for the digital I&C systems risk assessment.

	Tasks	**Approach**	**Acceptance Criteria**
Hazard Analysis	Identify potential hardware failures	FTA	Does the individual digital failure lead to the loss of function of digital system?
	Identify potential software failures, especially CCFs	STPA	
	Build FTs that integrate software, hardware failures	HAZCADS	
Reliability Analysis	Quantify probabilities of basic events for software failures, hardware failures and human errors	Reliability Modeling Approach (RMA); HRA	Is the digital system still reliable with the individual digital failures?
	Determine the optimal basic component combinations for prevention and mitigation	TEPA	
	Estimate the probabilities of consequences of digital system failures	ETA	
Consequence Analysis	Evaluate the impact of consequences of digital failures on the plant responses	Multi-Physics Best Estimate Plus Uncertainty (MP-BEPU)	Are the consequences of individual digital failures acceptable at the plant level?

As the first stage in the risk analysis phase, the hazard analysis needs to identify all potential software failures and hardware failures for the Acceptance Criteria (AC)-1 in the risk evaluation phase. Several approaches have been applied to identify these potential failures relevant to digital-based systems. AC-1 is defined as, “Does the individual digital failure lead to the loss of function of digital system?”. The key outcome of hazard analysis is the integrated FT that includes both hardware failures and software failures, and its cut sets for the top event. The top event is normally set as the loss of function of the target digital system. The “individual digital failure” in AC-1 refers to every basic event in this integrated FT for this

specific top event, which can be a hardware failure, software failure, or human error. If the occurrence of this individual failure can result in the top event regardless of the occurrences of other basic events, its risk is not acceptable for AC-1.

The second stage in the risk analysis phase is reliability analysis, with the tasks of: (1) quantifying the probabilities of basic events of the integrated FT from the hazard analysis; (2) determining the optimal basic component combinations for prevention and mitigation; and (3) estimating the probabilities of the consequences of digital system failures. The respective AC-2 is defined as, "Is the digital system still reliable with the individual digital failures?". Quantification of failure probabilities is the main outcome in this stage, for both single failure events and consequences. Reliability modeling approaches for software, hardware, and human factors will be reviewed in this chapter. For different designs and requirements from licensing regulators, the set point for reliability probability should integrate the efforts and experiences from industry, regulators, and researchers. At the same time, TEPA will be applied to choose a combination of design features that can satisfy the prevention criterion, and thereby support the digital designs.

For the third and final stage, consequence analysis should be implemented to evaluate the impact of consequences of digital failures on plant responses. AC-3 for this stage is defined as, "Are the consequences of individual digital failures acceptable at the plant level?" The main concern in this stage is that CCFs, especially software CCFs, have the potential to initiate an unanalyzed event or sequence that may not be bounded by previous plant accident analyses, and therefore, to challenge plant safety, such as core damage or a large early release. The PRA results from reliability analysis are supposed to provide different (non-)LOCA scenarios for the MP-BEPU in the consequence analysis. Limit surfaces for plant failures are the main outcomes in this stage and need to satisfy the limits in AC-3.

3.2 Hazard Analysis Approaches

For a digital-based I&C system, the failure of the I&C function results from either a hardware failure or a software failure, as shown in Figure 3. 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 FTA have 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/or other digital systems often result in new systematic failure modes that are difficult to discover using FMEA or FTA [8]. 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 the digital safety system, which have multi-layer redundant divisions, units, and modules compared to non-safety systems. In NRC staff reviews of failure modes provided in [26], "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)."

There are several factors leading to many successful methods for the analysis of failure modes in traditional analog systems not applicable to identify the software hazards in digital systems. First, software does not fail randomly like hardware. Software can be purely 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. Considering all the redundant designs in digital systems are using the identical software or digital platform, redundant designs are not effective since they can fail due to the same pure 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 [27]. 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 new unexpected conditions in the operating environment. Considering that software failure may be

triggered by a random hardware failure, the requirements on hardware reliability should also be reconsidered, which should be more rigorous than the ones in analog systems.

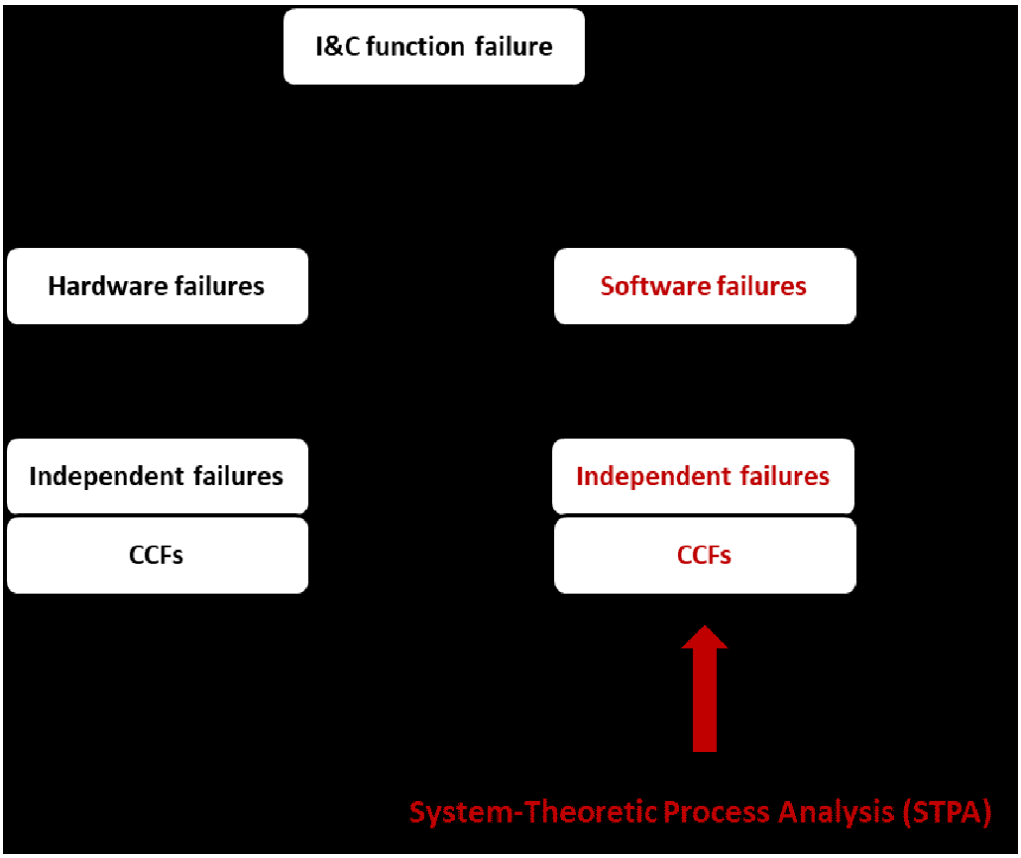


Figure 3. Fault Tree modeling for digital I&C failures.

Therefore, in this proposed risk assessment process, a relatively new hazard analysis method, STPA, is applied to identify the software failures for digital I&C systems. In 2012, STPA was applied to evaluate the safety of digital main steam isolation valve in an evolutionary power reactor (EPR) [28]. STPA describes how undesired outcomes (e.g., losses) can result from inadequate enforcement of constraints (e.g., control) on the design, development, and operation of systems to achieve desired objectives. After the identification of software failures, especially software CCFs, another method called HAZCADS is applied to construct an integrated FT by adding applicable software failures as basic events into the existing hardware FT.

Both STPA and HAZCADS are general guidelines for the identification of software failures and the construction of an integrated FT, which 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 RPS and ESFAS. Therefore, to deal with the complexity problem of redundancy and identify software CCFs effectively, STPA and HAZCADS processes are reframed in a redundancy-guided way, which are represented in: (1) framing the complexity of redundancy problem in a detailed representation; (2) clarifying the redundancy layers using FTA before applying STPA; (3) building a redundancy-guided multi-layer control structure; and (4) locating software CCFs for different layers of redundancy. More details are described in Chapter 4.

3.3 Reliability Analysis Approaches

This section gives an overview of the state-of-the-practice in reliability analysis. As shown in

Figure 3, both hardware failure and software failure contain independent failures and CCFs. There have been a couple of efforts on hardware reliability analysis for both independent failures and CCFs.

3.3.1 Hardware Reliability Modeling

Normally, a digital I&C system has a three-level hierarchical architecture [29]:

(1) Divisions (or channel), which process the signal path from the sensor to the actuator. Safety I&C systems generally have redundancy designs for this division level (e.g., the four-division design in Common-Q of APR-1400 RPS).

(2) I&C units, which perform a specific task by using several I&C modules (e.g., an acquisition and processing unit, voter unit).

(3) I&C modules, which realize a specific part of the function processing (e.g., input/output modules, processors).

Reliability analysis of a digital system should be conducted to a detailed level that captures sufficient design information affecting system reliability. It should keep the same level as hazard analysis and the availability of probabilistic data. Currently, most efforts on the reliability modeling of hardware failures reach to the level of modules, which is the smallest hardware component to implement a specific part of the entire function processing independently. Failures of hardware modules are identified in an integrated FT for the specific top event, which is one of the outcomes of hazard analysis; therefore, a reliability modeling should be assigned to each basic event for the quantification of failure probability. There are two types of failures of hardware modules: detected failures and undetected failures [29]. Different reliability measures are reviewed below.

Detected failures can be modeled using the reliability model called the “repairable component,” which means the module can return to work after repair. The failure and repair processes are assumed to

be exponentially distributed. Key model parameters are constant failure rate, , and repair rate, . The failure

probability, , at time, t, is expressed as [30]:

(1)

Given that the component is available at t=0, and . The mean failure probability in this model is:

(2)

For the undetected failures that are identified during periodic testing or in case of demand, the reliability model called “periodically tested component” can be applied. Model parameters are constant

failure rate, , and the constant test interval, TI. The failure probability at time, t, can be expressed as [30]:

(3)

The mean failure probability is:

(4)

Other reliability models exist for these components that must work during a predetermined time period, such as “components with fixed mission time,” or ones that only have one constant failure probability, such as the “constant failure model,” which is suitable for components that experience failure per demand.

These methods have been widely used to quantify the probability of single failure of hardware modules. The CCFs of hardware modules should also be considered in the hardware reliability analysis. Normally, hardware faults are uncorrelated, but can be activated by a same trigger that manifest the accumulated faults as a CCF of these faulty modules [29]. The CCFs in detected failures are not considered in reliability analysis because they can be identified and repaired in a very short time, which has a very low probability to initiate a CCF of multiple components. The CCFs in undetected failures, by contrast, has a higher probability considering that the undetected faults can accumulate over a much longer period between two tests or demands. Some traditional CCF models, such as alpha factor model [31] and beta factor model [31], have been applied for the CCFs of hardware modules. However, these traditional methods are using some generic and conservative CCF parameters for I&C hardware modules, which leads to some greatly conservative reliability results. The CCF modeling of hardware modules in I&C reliability analysis is still a very big challenge and the R&D of I&C-specific models are needed.

3.3.2 Software Reliability Modeling

In this section, several available quantitative software reliability methods are reviewed with the objective of classifying potential methods that can be used to quantify software failure rates and demand failure probabilities of digital systems at NPPs. Generally, there are two types of digital systems at an NPP: a non-safety I&C system, such as the feedwater control system, and a safety system, such as the RPS. Compared to non-safety systems, safety systems may have different failure modes. For example, the RPS may fail to provide a trip signal when needed or generate a spurious signal when not needed. Given

the occurrence of an initiating event that leads to the need for a reactor trip, the first failure mode should be modeled in the PRA model in terms of a demand failure probability. And the latter failure mode should be identified as one of the initiating events just like the way to model the failure of the feedwater system. This example shows that, even for a single digital system, a different reliability method may need to be applied for different failure modes of interest, which could be a failure-rate-based method and a failure-on-demand-based method [2].

Currently, there is no consensus method for the software reliability modeling of digital systems in an NPP. Only a few publicly available studies have attempted to quantify software failure rates and demand failure probabilities performed in nuclear fields. Generally, four types of these methods have been reviewed [2]:

(1) Reliability growth methods [32]. These are time-based methods that estimate software failure rates using test data. They can also predict the time to next failure and the required time to remove all faults. Reliability growth models are based on the sequence of times between observed and repaired failures.

(2) Bayesian Belief Network (BBN) methods [33]. These are methods that use a probabilistic graphic model to describe a set of random variables and their conditional independencies via a directed acyclic graph. One of their drawbacks is that a new BBN must be built for each specific software development environment [34], but it might be solved by using some generalized BBN templates, which are not limited to a specific environment [35]. Currently, BBN methods have been applied to software safety assessment and can be considered promising.

(3) Test-based methods [36]. Standard statistical methods are employed to run several tests and get the number of failures measured.

(4) Other methods [2] including: (a) a context-based software risk model that combines traditional PRA approaches and advanced modeling approaches to integrate the contributions of digital hardware and software into a model of overall system risk; (b) metrics-based methods that estimate software failure rates and probabilities by correlating software engineering measures and software reliability; and (c) approaches that estimate software failure rate at the end of software testing stage by making use of existing software engineering practices.

However, none of these is universally accepted, particularly for highly reliable systems [37]. All have been explored in the academic field, but not applied in real industrial PRAs for NPPs. Although there is yet no agreement on which method to use, it has been agreed that software failure could and should be analyzed probabilistically. A similar conclusion was made in the Workshop on Philosophical Basis for Incorporating Software Failures in a PRA [38]. The panelists universally agreed that: (1) software fails; (2) the occurrence of software failures can be treated probabilistically; (3) it is meaningful to use software failure rates and probabilities; and (4) software failure rates and probabilities can be included in reliability models of digital systems. Therefore, in industrial PRA applications for NPPs, the engineering judgement approaches have been applied and can be divided as the following types according to the argumentation and evidence they use [34]:

(1) Screening out approach: This means that software failures are screened out from the model and assessed through sensitivity approaches. It is suitable for the software where the contributions of software failures are insignificant or there is no practical method to estimate the failure probability (e.g., systematic failures).

(2) Screening value approach: In this approach, some conservative values are assigned for the reliabilities. For example, is chosen for a software CCF, which is taken from IEC 61226 [39]. In [40],

is claimed to represent that the single software -based system is important to safety and should be

treated with extreme caution.

(3) Expert judgement approach: This approach evaluates the features of software-based systems and assumes they have a correlation with reliability. Two important questions are: (a) Which features should be considered? and (b) What is the correlation between the features and the reliability? In [41], it was assumed that software failure has only 10% of the contribution of hardware failure to the total failure probability, because the contribution of software failure is smaller than exclusive hardware failure and there is a threat of software CCFs for the redundant components. The beta-factor CCF model was applied for both hardware failure and software failure with [41].

(4) Operating experience approach: In this approach, operational data is used to estimate the reliability. In [42], the contribution of software CCF to the unavailability of a safety system was estimated based on the operational experience in the PRA study of the Swedish NPP Ringhals 1. The

contribution of platform CCF was estimated as , since the operational experience showed that no

CCFs were caused by platform properties for over 60 years. In [43], both operational experience and engineering judgement were applied to develop reasonable estimated for the relative contributions of software to the CCF probabilities. Based on the data of more than 10 years, the CCF probability of an

operating system was estimated as . *Meanwhile, the application* software CCF probability was

estimated as *for each function group.* Besides, [43] suggested that the dependency between two

application software CCFs should be assessed if they appeared in the same cut set.

Therefore, according to the reviews in [34], currently only hardware CCFs are modeled in NPP PRA because there is no appropriate method to integrate software failures into a FT. Software CCFs can be added into FTs because they lead to the top event directly. Software CCF is generally modeled between processors with redundant designs and functions with the same application software and platform. This is similar to the module level of hardware failure depending on how many details are required to describe the features affecting the reliability of the software-based system. In [44], four different software failures were considered in the design phase probabilistic safety assessment (PSA) conducted for the automation renewal of the Loviisa NPP: (1) independent failure; (2) CCF of a single automation system; (3) CCF of programmed systems with same platforms and/or software; and (4) CCF of programmed systems with different platforms and/or software.

3.3.3 Human Reliability Analysis

The HRA should be performed to identify and estimate the probabilities of hardware/software failures due to human errors, or the basic events directly related to human errors. In PRA applications in the

nuclear industry, human failure events (HFEs) are defined as a subset of hardware failures where the hardware faults can be triggered by human errors [45]. Based on the experience of STPA applications, human errors are determined as one of the crucial causal factors resulting in systematic software failures. Therefore, the probability of human errors affecting hardware failures, software failures, or straightly leading to the top event in the FT should be quantified by HRA methods.

3.4 Consequence Analysis Approaches

As mentioned in Section 3.2, even for a single digital system (e.g., RPS), different failure modes could be identified that have different roles in different scenarios. A spurious trip signal given by an RPS when not needed may lead to an unanalyzed initiating event; meanwhile, failing to give a trip signal may lead to an Anticipated Transient Without Scram (ATWS) scenario. Therefore, consequence analysis should be performed to evaluate the impact of consequences of different failure modes of digital systems, especially safety systems, on the safety margins of NPPs.

It is noted that the term "safety margin" is used to ensure that the SSCs in an NPP can perform their intended functions under both normal and abnormal operating conditions [46]. The application of safety margins compensates for uncertainties in the phenomena and model data, as well as variability in the initial and boundary conditions associated with the analysis of events that can impact plant safety. Safety margins can also compensate (at least to some extent) for phenomena that may not have been foreseen during the design process. Simply put, safety margins provide allowances for insufficient knowledge or uncertainties associated with the design and operation of NPPs. Safety margins provide a buffer between the expected plant response during anticipated events and the point at which conditions will likely threaten plant safety (i.e., core damage or the release of fission products to the environment). Since it takes time for operating parameters in transients to overcome these buffers, the existence of safety margins allow plant safety systems and operating personnel to react to these events and mitigate their consequences.

Over the past several decades, the nuclear industry has been able to recover safety margins through multiple approaches, such as plant equipment upgrades and modernization and the application of more sophisticated analytical capabilities. With improved understanding of plant transients and accident phenomena, efforts have been made to mitigate the conservative biases and assumptions in the evaluation model methodology, allowing a licensee to move toward Best Estimate Plus Uncertainty (BEPU) methodologies. The regulatory expectations for use of BEPU methodologies for NPP transient and accident analyses are specified in RG 1.203 [47], which provides a comprehensive description of the Evaluation Model Development and Application (EMDAP) that provides an integrated approach to conduct NPP safety analyses. The key aspect of the BEPU methodology is to quantify and propagate uncertainties in the calculations across all constituent phenomena that are modeled (i.e., reactor physics, thermal hydraulics, material properties, etc.). However, the computational constraints that arise due to the complex systems and interdependencies of variables historically have prevented the nuclear power industry from executing such multi-physics schemes. Because of these limitations, the existing BEPU methodology primarily focuses on the uncertainties in thermal hydraulics.

Moving forward, as more automation is adopted into plant processes, it is anticipated that the nuclear industry will develop better standardized databases and improved interfaces that function across various engineering disciplines. Such standardization and increased automation will be capable of enabling new paradigms to evaluate and manage uncertainties across various disciplines and support a more integrated multi-physics approach that can be applied to the safety analysis problem. Fortunately, because of the advancements in computing power over the past several decades, multi-physics simulations are now practical within the context of uncertainty quantification and sensitivity analysis (i.e., Multi-Physics Best Estimate Plus Uncertainty [MP-BEPU] methodologies). Currently, the BEPU approach is predominantly applied to the analyses of predefined design basis accidents (DBAs) that are limited to single failures in active safety systems. Moving forward, a comprehensive listing of postulated initiating events for all

plant states should be prepared to ensure that the analysis is complete. Hence, combining PRA and MP-BEPU analysis would provide a comprehensive assessment of plant risks and permit a comprehensive quantification of margins. In addition, by providing a probabilistic evaluation, the results can be used to prioritize analyses to concentrate on those that have the highest likelihood of resulting in undesired consequences; thus, ensuring efficient use of resources. Therefore, in [46], a Risk-Informed Multi-Physics Best Estimate Plus Uncertainty (RI-MP-BEPU) framework was proposed to conduct comprehensive investigations of design basis requirements and their implementation through plant processes and systems (i.e., SSCs, maintenance, surveillance, testing, qualification and quality requirements of encompassed systems, technical specifications, limiting conditions of operations, etc.) to identify and recover margins associated with uncertainties and conservatisms of legacy licensing, design, and analysis. The RI-MP-BEPU framework is an extension of the loss of coolant accident (LOCA) analysis toolkit for the U.S. (LOTUS) framework [48] being developed for LOCA applications in response to the proposed new rulemaking in 10 CFR 50.46c [8]. This approach is shown schematically in Figure 4. The consequence analysis in the proposed RADIC process will be performed by following the RI-MP-BEPU framework.

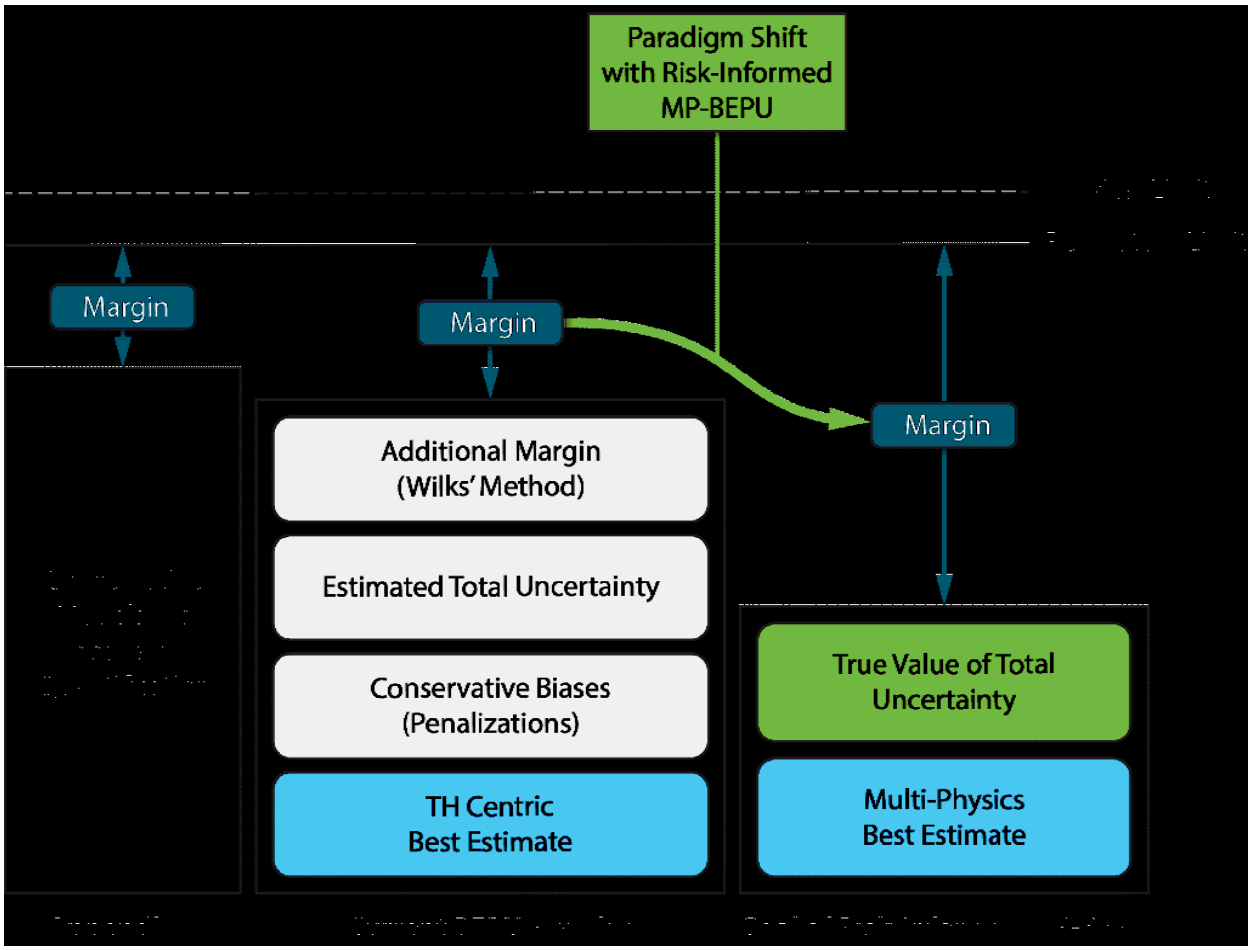


Figure 4. Schematic illustration of the objective of the RI-MP-BEPU Framework.

3.5 Risk Assessment on Cybersecurity of Digital I&C Systems

In 2009, the NRC published the cybersecurity rule in 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Network" [49]. The cybersecurity rule is a performance-based programmatic requirement that ensures that the functions of digital computers, communication systems, and networks associated with safety, important-to-safety, security, and emergency preparedness are

protected from cyber-attacks. The NRC engages with other Federal agencies, including the U.S. Department of Homeland Security, the Federal Energy Regulatory Commission, and the North American Electric Reliability Corporation on cybersecurity efforts. In 2010, cybersecurity of digital I&C systems was included in the digital I&C system research plan as a research program area. In support of 10 CFR 73.54, the NRC published RG 5.71, "Cybersecurity Programs for Nuclear Facilities," [50] in 2010, which "provides an approach that the NRC staff deems acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber-attack as defined by 10 CFR 73.1."

The NRC–Office of Nuclear Regulatory Research (RES) completed research to explore cyber-vulnerabilities in digital systems and networks, including wireless networks that were expected to be deployed in NPPs. This research validated the need for new regulatory guidance and cybersecurity programs required under 10 CFR 73.54. The NRC I&C research staff participates in government-wide, academic, and industry working groups that provide the latest information and tools to address cyber-threats. Continuous evaluation is required to maintain expertise that can address concerns that arise in this rapidly changing environment.

In implementing 10 CFR 73.54, the NRC has issued Reg Guide 5.71 [50] which addresses the requirements for nuclear instrumentation systems to address all phases of the NRC lifecycle. Specific guidance on vendor responsibilities in the software lifecycle are included in Reg Guide 1.152 [51]. In response to the NRC guidance, the industry issued and has implemented NEI 08-09 Rev 6 [52] which has a complimentary set of guidance on implementing the cyber security rule. The NRC has also conducted over 20 inspections of the nuclear plant response to the rule in the U.S. in the past two years.

As part of the digital I&C research plan, the risk assessment of cybersecurity in digital I&C systems are also required. The proposed RADIC process is applicable to identify and evaluate the impact of potential cyber-attacks at the individual, system, and plant levels.

In 2019, a U.S. Department of Energy (DOE) Office of Nuclear Energy (NE) cybersecurity program has been initiated, the mission of which is to "*enable science-based methods and technologies necessary for cost-effective, cyber-secure digital instrumentation, control and communication in collaboration with nuclear energy stakeholders.*" Integrated cross-cutting pathways were organized to incorporate efforts in risk management, secure architecture, modeling and simulation, and supply chain. The results of the DOE–NE cybersecurity program have the potential to be leveraged by the Light Water Reactor Sustainability (LWRS) Program in the following perspectives: (1) cybersecurity research in risk management, secure architecture, and supply chain; and (2) improved understanding of the cybersecurity risk posture. Specifically, potential software failures, especially CCFs, caused by cyber-attacks could be identified and eliminated.

4. DESCRIPTION OF INTEGRATED RISK ASSESSMENT PROCESS FOR DIGITAL INSTRUMENTATION AND CONTROL

To support transition from analog to digital I&C technologies for nuclear industry, this project aims to develop an integrated risk assessment process for digital I&C systems. According to the tasks of risk assessment discussed in the previous chapter, this chapter develops the framework of the proposed RADIC process in detail. The RADIC process consists of two phases: risk analysis and risk evaluation. Risk analysis aims to identify hazards of digital-based SSCs, estimate their failure probabilities, and analyze relevant consequences by performing hazard analysis, reliability analysis, and consequence analysis. The framework of the RADIC process is illustrated in Figure 5. The results of the risk analysis phase need to be evaluated based on the acceptance criteria at the individual, system, and plant levels. The three-stage risk analysis phase are described in the following sections as system-theoretic hazard analysis, integrated reliability analysis, and risk-informed consequence analysis. The relevant approaches appropriate for each stage are also listed in Figure 5.

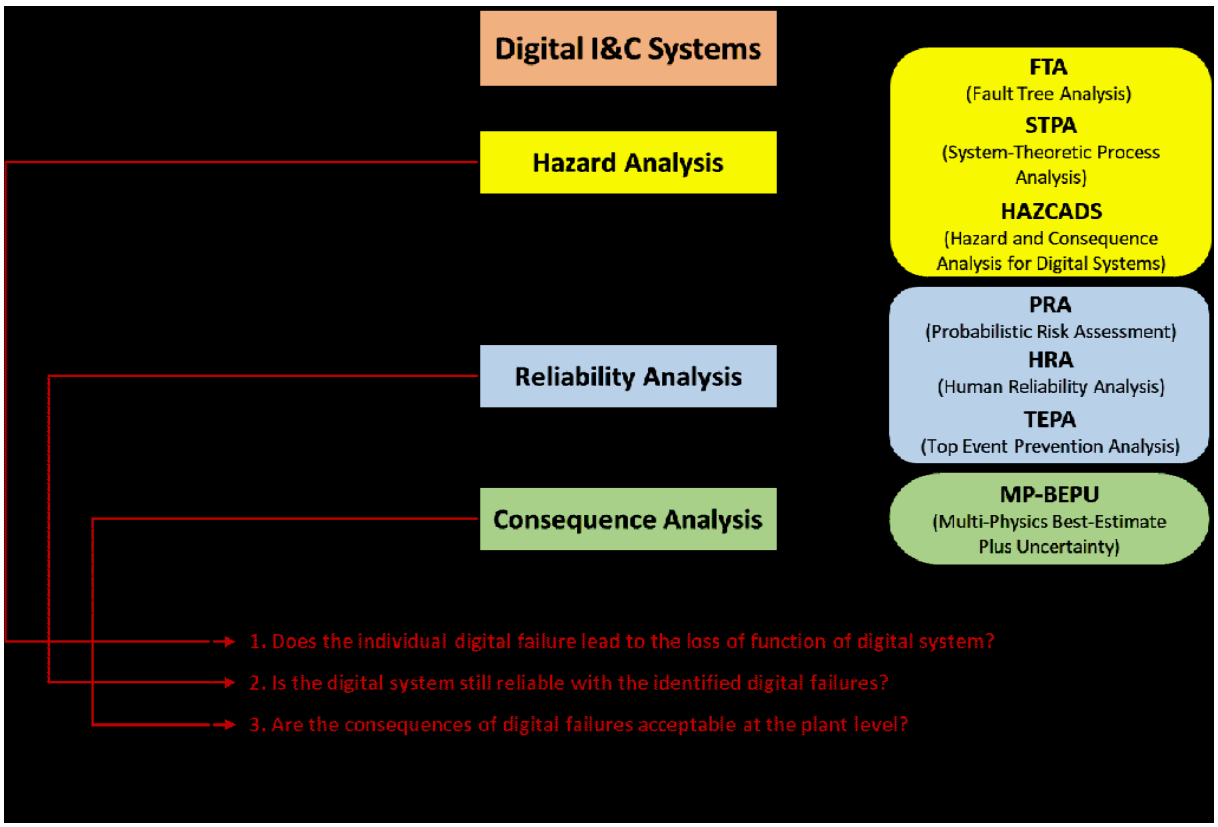


Figure 5. Illustration of the integrated RADIC process.

4.1 System-theoretic Hazard Analysis

As discussed in the previous chapters, the main challenge of performing hazard analysis on digital safety systems is the identification of software CCFs. As an important design principle for achieving high reliability in systems important to safety and for meeting the single failure criterion for safety systems, redundancy designs are widely applied in digital safety systems to initiate automatic actions to prevent and mitigate accident conditions if non-safety systems fail to maintain the plant within normal operating conditions. The I&C safety systems, such as the RTS and ESF systems, are of a particular concern in NRC licensing procedures, especially considering potential software CCFs may generate unanalyzed

plant conditions because the transient and accident analyses for existing U.S. plants was only considering the failures applicable to analog I&C technology [1]. Therefore, STPA and subsequent HAZCADS have been developed as general guidelines for the identification of software failures and the construction of the integrated FT, which have been applied for safety and security analyses. 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 RPS and ESFAS.

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 and HAZCADS processes 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 software failures, 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 that if a single part of a system fails, the entire system will lose the function. The proposed approach for system-theoretic hazard analysis is illustrated in Figure 6.

Figure 6. Proposed approach for system-theoretic hazard analysis in the RADIC process.

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 [29]: (1) divisions that process the signal path from sensor to actuator; (2) units that perform a specific task by using several modules; and (3) modules that realize a specific part of the function processing. The representation should contain the information of hardware structure and be created to a detailed level that captures sufficient design information affecting the system function and reliability. In this work, most efforts on the 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 the risk analysis phase, practical assumptions, and reasonable simplifications of the hardware representation should be stated and explained in this step. The representation figure should clearly display the information flow between different divisions, units, and modules.

For the analysis on digital system with redundancy designs, the complexity of redundancy should be illustrated in the hardware representation. It builds the basis for the construction of hardware FTs and

redundancy-guided multi-layer control structure.

Step 2: Develop a 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. For the analysis on digital system with redundancy designs, the structure of hardware FT should follow the layers of redundancy from a high level to a low level. For example, the top-level layer of redundancy in a RTS is the several independent divisions to trip the reactor. The functioning of each reactor trip breaker is affected by a specific division. Signals from plant sensors are sent to all of the divisions to compare with the engineered set points. In each division, signals are received by several independent bistable processors (BPs), the second layer of redundancy, where decisions are made whether or not to trip the reactor. Then, the trip signals from each BP are sent to the logic cabinets in all divisions, where the BP outputs are transmitted to coincidence trip signals by redundant LCL processors, considered as the third level of redundancy. This kind of redundancy-guided structure makes it convenient to add in the software failure identified in next step. Probability quantification of each basic event is not required in this step and will be performed in the integrated reliability 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, the key losses and system-level hazards are identified. In STPA, a loss includes something of value to stakeholders or the public (e.g., a loss of human life or human injury, property damage, environmental pollution, or any other loss that is unacceptable) [15]. 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" [15]. 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 multi-layer control structure is modeled. A control structure is defined as, "a system model composed of feedback control loops" [15], which illustrates the interactions between controllers and a controlled process, including sensors and actuators. A generic control loop is shown in Figure 7. 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 representing controller's internal criteria used for its decision-making. The control actions provided by a controller can be influenced by the controller's process models, control algorithms, and feedbacks.

In a digital system, all of the 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 resulting from 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 identify software CCFs effectively, control structure is built in a redundancy-guided way. The redundancy-guided multi-layer control structure zooms in the systematic information exchanges on each redundancy layer because CCFs are tightly connected with redundancy designs. Most of the redundancy layers are located in the controlled process.

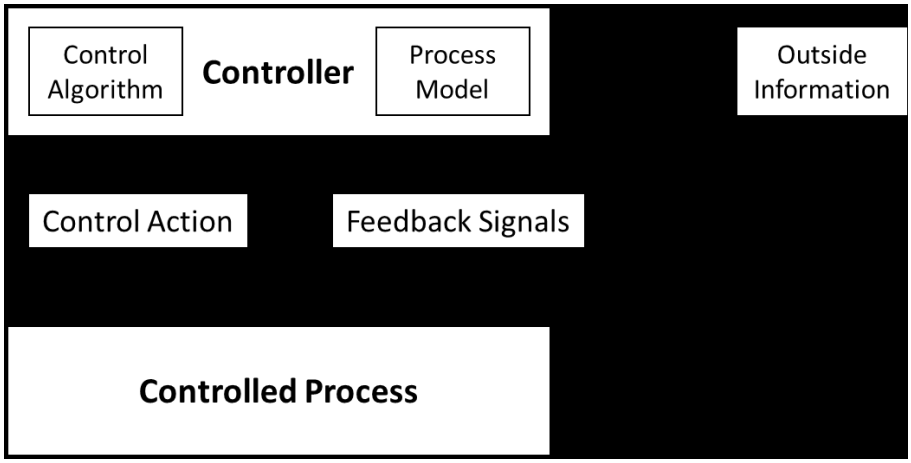


Figure 7. A generic control structure in the STPA application.

Third, the UCAs are identified according to the multi-layer 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" [15]. There are four types of UCAs in an STPA:

(1). Control action is not provided when it is needed.

(2). Control action is provided when it is not needed.

(3). Control action is provided when it is needed, but too early, too late, or in a wrong order.

(4). Control action lasts too long or stops too soon (only applicable to continuous control actions).

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 [15].

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 the software failures. For a specific top event in the FT, some UCAs may be inapplicable. For example, if the top event of hardware FT is "RTS fail to trip reactor," Type 2 and 4 of UCAs are inapplicable since the control action of "sending trip command" is needed and not a continuous action. If the top event is "Unexpected Trip by RTS," only Type 2 is applicable. Considering the hardware FT and redundancy-guided multi-layer control structure are tightly connected and consistent with each other, these applicable UCAs (software failures) can be incorporated into the hardware FT in parallel with the respective hardware failures.

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 layer can be separated into independent failures and CCFs. Additionally, software CCFs can be classified as different types depending on the redundancy layers: (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*" [51]. 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 determined to evaluate how many potential SPOFs have been added by considering the software failures. If the digital system has a low level of software diversity, the software CCFs type 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. The AC-1 is defined as, "does the individual digital failure lead to the loss of function of digital system?" If the "individual digital failure" is one of the SPOFs, AC-1 will not be satisfied and a redesign request will be developed based on the risk evaluation result.

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 [52], as well as the faults introduced during the detailed logic design phases of the software development because the interactions between some process logic inhibits and the test logic were not recognized by the designers or verifiers [53]. The NRC proposed two design attributes used to eliminate consideration of CCFs: diversity and 100% testability [54]. 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*" [54]. However, both of the design attributes have limitations. Diversity normally leads to high cost, while potential CCF vulnerabilities will be more complicated and difficult to identify as system complexity increases. Applying 100% testing may be able to reveal the presence of a fault, but not its absence, which means 100% testing does not fully eliminate software CCF concerns.

Therefore, this step is focusing 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 obtaining the respective UCAs, their causal factors or latent faults can be identified in three types: (1) unsafe controller behaviors (i.e., operator errors or power failure of digital controllers); (2) inadequate feedback or outside information (i.e., wrong or absent signals from pressurizer to RTS); and (3) inadequate design requirements (i.e., pressurizer setpoint is not correctly programmed in RTS BPs). The triggers of software failures are defined as the contexts of the identified UCAs. The identification of causal factors should be cooperated with the expert teams in system engineering, software engineering, HRA or PRA, etc., and will be helpful to provide guidance for the risk reduction and redesign of the digital systems.

4.2 Integrated Reliability Analysis

Hazard analysis identifies the potential SPOFs introduced by considering software failures, which have high probabilities to result to the loss of function of the target digital system. In this section, an integrated reliability analysis approach is proposed to evaluate how the individual software/hardware failures or human errors affect the reliability of the entire digital system of interest. Therefore, one of the tasks in this integrated reliability analysis is to quantify the probabilities of basic events and the probability of the top event of interest. Different reliability modeling methods will be applied for software failure, hardware failure, and human error. Another task is to measure and rank the importance of these individual failures (as basic events in FTs) based on their risk safety significance to the reliability of the

digital system. Importance ranking of basic events relies on the results of different metrics for importance measure, such as Fussel-Vesely (F-V), Risk Achievement Worth (RAW) or Prevention Worth (PW). Then, the number of basic events could be reduced based on importance ranking and other criteria. Last, but the most important, several ETs are to be built considering different failure modes of digital systems, especially for some unanalyzed top events resulting from some new digital failures. Some of these top events themselves can be treated as the initiating events of some scenarios, while others are modeled in the ET model given an occurrence of an initiating event leading to the need of function of the digital system. The probabilities of consequences of digital system failures should be calculated for the following consequence analysis. The proposed approach for integrated reliability analysis in the RADIC process is illustrated in Figure 8.

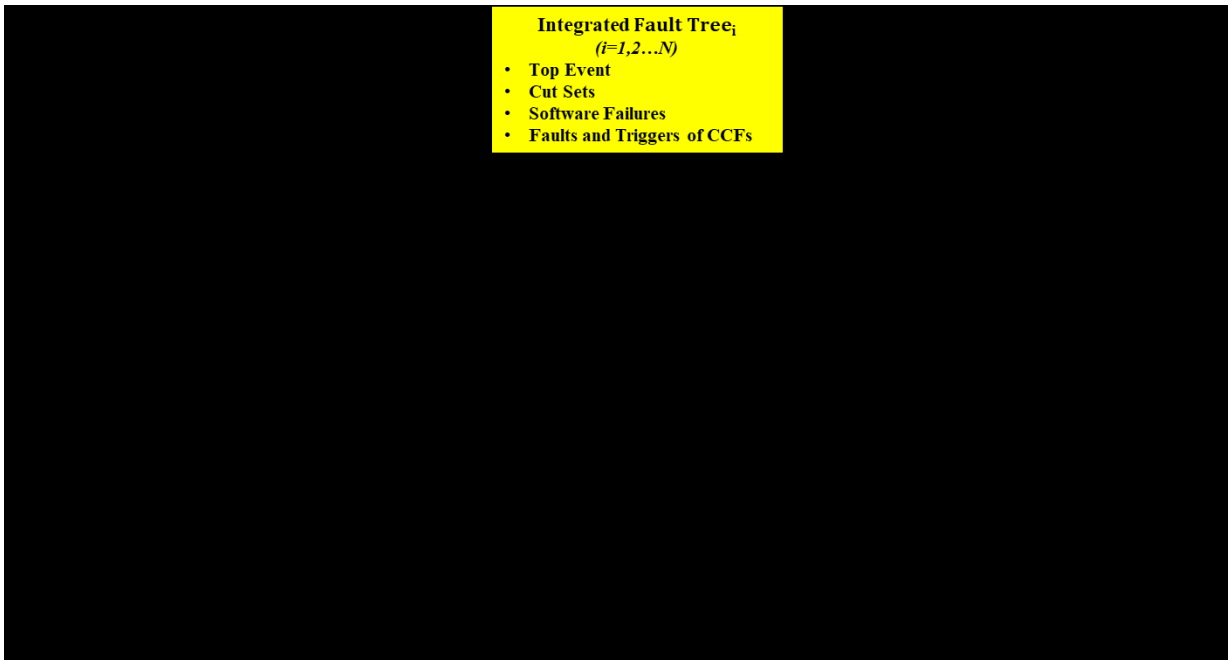


Figure 8. Proposed approach for integrated reliability analysis in the RADIC Process.

Step 1: Build ETs considering different failure modes of the digital system.

Based on different FTs with different failure modes of digital systems, respective ETs are to be built in this step. Compared to non-safety systems, safety systems may have different failure modes. For example, an RPS may fail to provide a trip signal when needed or generate a spurious signal when not needed. Given the occurrence of an initiating event leading to a necessary reactor trip, the first failure mode should be modeled in the PRA model in terms of a demand failure probability. And the latter failure mode should be identified as one of the initiating events. For these digital system failure modes existing in the top events of current ET models, only the FTs under the top events need to be updated. For some new unanalyzed failure modes of the digital system, the ET itself also needs related modifications.

An NPP could either be in an operational or accident state. Since 1970, the American Nuclear Society (ANS) classification of plant conditions has been widely used to divide plant conditions into four categories in accordance with the anticipated frequency of occurrence and potential radiological consequences to the public [55]. The four categories are: (I) normal operation and operational transients; (II) faults of moderate frequency (i.e., events that are expected to occur several times during the lifetime of the plant); (III) infrequent faults (i.e., events that may occur during the lifetime of the plant); and (IV) limiting faults (i.e., postulated accidents that are not anticipated to occur during the lifetime of the plant). Conditions 2 and 3 are typically referred as AOOs. Condition IV faults are postulated DBAs that

are not expected to occur during the operational lifetime of a NPP. In addition to Conditions I through IV described above, a NPP could also undergo an event that is beyond the design basis accident conditions. A beyond design basis accident (BDBA) involves accident conditions that are more severe than a DBA, which have the potential to result in core degradation. The research, development, and deployment (RD&D) plan described in this report will focus resources on the analyses of the anticipated performance of proposed advanced nuclear technologies across the full spectrum of plant transients and accidents, including AOOs, DBAs, and BDBAs. AOOs span the full range of conditions for which light water reactors (LWRs) must be evaluated for advanced new nuclear technologies to be licensed and deployed in the existing fleet. AOOs and DBAs constitute the spectrum of design basis events required for analysis in the licensing of a NPP in the U.S. Because the set of DBAs required for licensing represent some of the most extreme conditions a NPP could reasonably be expected to experience during the course of its operating life, these events can be used in initial evaluations as a valuable representation of the potential benefits that can be provided by advanced nuclear technologies. Therefore, ETs should be built in two categories: (1) non-LOCA for AOOs; and (2) LOCA for DBAs with different specific acceptance criteria.

Step 2: Estimate probability of all the basic events.

In this report, a failure of a digital I&C system results from hardware or software failures. Some of these failure sources divide into independent failures and CCFs. There are two types of hardware module failures: (1) detected failures; and (2) undetected failures. Different reliability measures were reviewed in the previous chapter. These straightforward methods for hardware failure probability calculation have been widely used in practical applications. However, none of the methods for software failure probability calculations is universally accepted, particularly for highly reliable systems. All of them are explored in the academic field, not applied in real industrial PRAs for NPPs. This work attempts to deal with this difficulty via the application of STPA. In Step 7 of the system-theoretic hazard analysis approach, causal factors of all these software failures (or UCAs) are identified with the cooperation with different expert teams. Once determining the probability of relevant causal factors, the software failure probability can be estimated by integrating the probability of all these causal factors. It should be noted that the quantification of software failure probability is still challenging due to the lack of testing/ operating data and a generally recognized estimation method. The probabilities of causal factors about human errors and basic events directly related to human errors can be estimated using some HRA methods.

Step 3: Perform prevention analysis to determine the optimal combinations of events.

In this step, TEPA is performed to identify a collection of design elements that is necessary and sufficient to achieve the desired level of protection of the public, the worker, and the environment. TEPA has advantages in that: (1) it identifies collections of components that are effective in managing safety; (2) risk can be shown to be insensitive to the reliability of components not found in the selected prevention set in combination with each other; (3) tests can be easily preformed to demonstrate that the selected prevention set is effective in assuring the prevention of all cut sets including those that were truncated from the original results; and (4) multiple prevention sets are generated and if ranked in some way such as any cost, the most economic optimal solution can be selected for implementation [56]. Traditional importance measures, such as F-V and RAW, do not address an essential collective property of a safety case—that its elements must work together. They are sensitivity coefficients calculated with all other components behaving nominally [20]. After determining the optimal combination of events, recommendations on the design can be provided as increasing the reliability of relevant components, which are the significant contributors to the prevention of top events. Generally, prevention analysis comprises four steps according to [56]: "*(1) build and solve a model to obtain the top event expression; (2) choose a prevention level L, and specify the events that are to be credited toward prevention or, conversely, those that are to be excluded; (3) generate an expression for each top event minimal cut set that represents prevention of the cut set by L credited events; and (4) form the Boolean product of the minimal cut set expressions, and expand and simplify this product to obtain all minimal prevention sets of*

level L. A prevention set of level L contains at least L basic events from each top event minimal cut set and it is minimal if it cases to be a prevention set of level L when any of its events are removed."

Step 4: Measure and rank the importance of basic events.

In this step, different metrics are used to measure and rank the importance of basic events based on their risk and safety significance to the reliability of digital system. Risk significance refers to the significance of a contribution to system failure probability, while safety significance refers to the significance of a contribution to system success probability. Some metrics to identify the risk significance of events are mainly from two perspectives: (1) those events that currently contribute most to the failure of the system (e.g., F-V); and (2) those events that could potentially contribute significantly if they were to degrade in reliability (e.g., RAW). Based on the properties of path sets containing the prevention of basic events, a measure of safety significance was proposed in [20] as PW. A high value of F-V means that cut sets containing the events contribute significantly to the top event frequency, while a high value of PW means the path sets containing the prevention of these events contribute significantly to the top event prevention. RAW strongly depends on what is in parallel with this event, while PW of an event depends on what is series with the prevention of this event in a success path. Different from RAW, PW is really a property of the collection of path sets containing the element, not the rest of the path sets. Only in extremely simple cases, PW is essentially equivalent to RAW.

According to the reviews in [20], F-V and PW are complementary both in the mathematical sense and in the common-language sense. PW focuses on the functionality supported by preventing the events rather than the vulnerability reflected by F-V values. Therefore, in this work, F-V and PW are used as the metrics to measure and rank the importance of basic events from their risk and safety significance to the reliability of digital system.

Step 5: Reduce the number of basic events.

Considering that every applicable UCA added into the FT may include both independent failure and CCF at a different redundancy layer, the number of basic events in the integrated FT is explosively increasing. There are some associated system analysis requirements that could exclude some basic events from the PRA model, which mainly depend on their contributions to system unavailability and unreliability (i.e., risk significance). Typically, PRA is applied to quantify the dominant contributors of risk, which does not require that every event be included in the PRA model. Most of the basic events are included because they have considerable contributions to risk, for example, with a high F-V value, which is not negligible. But this does not mean that those events not included are not important to successful operation, they may have a high PW value even their F-V values are not high. A low F-V value of the event does not imply the respective component is misplaced; it may only mean that this component is successfully set with a high reliability. However, if the prevention of this event exists in a couple of path sets, it may have a high PW value, which means its prevention significantly affects the success of the prevention of the top event.

Therefore, in this work, the basic events are classified in four different types based on their risk significance (i.e., F-V) and safety significance (i.e., PW) as shown in Figure 9: high F-V and high PW, low F-V and low PW, high F-V but low PW, and low F-V but high PW. F-V indicates relative vulnerability, while PW implies its inclusion in probabilistically significant path sets. An event with high F-V and high PW is a relatively weak link with a low reliability in a strong collection of success paths, which needs considerations with the highest priority. An event with either high F-V but low PW means the respective component has a relatively low reliability but only exists in a few path sets, some efforts should be made to increase its reliability. An event with either low F-V but a high PW means that the respective component has a relatively high reliability, but exists in several path sets, some efforts should be made on its maintenance and testing to keep its reliability at a high level. An event with either low F-V and low PW means the respective component has a relatively high reliability and only exists in few path

sets, considerations on which could be decreased to reduce the costs from maintenance and testing or use of diversity. The last type of events with low F-V and low PW may be excluded from the PRA models.

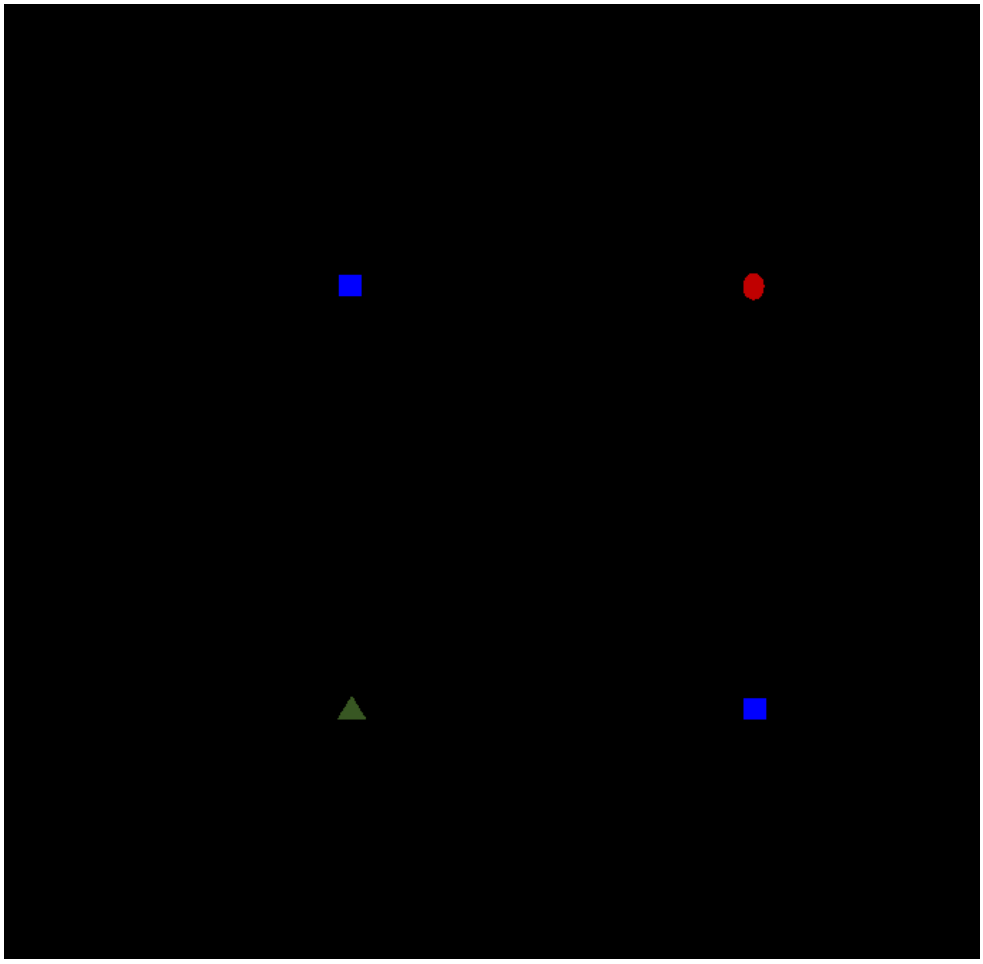


Figure 9. Classification of events based on their risk significance and safety significance.

Step 6: Calculate probability of the top event with reduced basic events.

Once the basic events have been reduced based on their risk and safety significance, the integrated FTs about digital system failures should be reconstructed and only include the events with a high F-V or a high PW. Then, the probability of a top event can be calculated based on the probabilities of existing basic events and gate symbols. It should be noted that some other top events in the ET may be correlated to the basic events analyzed in Step 5. The F-V and PW values of these basic events should be different since the cut sets or path sets of these FTs are also totally different. For those non-digital top events existing in the ET, one can choose to perform Step 4 and Step 5 to reduce the number of their basic events or keep their original FT structure built based on previous experience.

Step 7: Quantify the probability of consequences of digital system failures.

After obtaining the probability of the top event related to digital system failures, the probability of consequences of these digital failures can be quantified based on the ETs built in Step 1. The postulated initiating event, which normally results in reactor shutdown, is the starting point of a tree consisting of safety functions or safety systems. A safety function or safety system, needed to mitigate the initiating event in order to avoid core damage, may be available (success) or unavailable (failure), thus creating branching points in the tree. Each branch of the tree is an accident sequence and leads to the end state (the

reactor core is cooled or it is damaged), which is a consequence of postulated initiating event given the combination of performance of safety functions or safety systems.

4.3 Risk-Informed Consequence Analysis

Resulting from some digital failures including independent failures and CCFs, a failure of a digital I&C system can affect plant responses in either or both of two ways [57]: (1) influence the characteristics of transient and accident initiators (e.g., increase or decrease the magnitude or effects of a given initiator, or impact the initial conditions assumed in analyzing events); and (2) affect the response of mitigating systems (e.g., disable, delay, change performance, etc.). Therefore, consequence analysis should be performed to evaluate the impact of consequences of different failure modes of digital systems, especially safety systems, on the safety margins of NPPs. In this work, consequence analysis is defined as a process to conduct uncertainty and sensitivity analysis within a multi-scale and multi-physics environment to fully evaluate the impact of the consequences of digital system failures, which are identified in reliability analysis. Based on the uncertainty studies and limit surfaces for different scenarios, plant-level risk assessment is performed to investigate whether the consequences of digital failures are acceptable at the plant level. For utilities, consequence analysis could be used to analyze the plant responses and the performance of mitigation systems under the digital system failures and evaluate whether they are acceptable by owners/operators of the plants. For designers, consequence analysis could be performed to support the design of digital systems by checking whether the design meets specific safety, reliability, and licensing criteria. The proposed approach for risk-informed consequence analysis in the RADIC process is illustrated in Figure 10.

Figure 10. Proposed approach for risk-informed consequence analysis in the RADIC process.

After obtaining ETs from reliability analysis, it should be clarified whether these scenarios have been covered by previous analysis. If they are unanalyzed scenarios, consequence analysis should be performed to investigate the impact of digital failures on plant responses. Being informed by PRA models, consequence analysis is implemented via the LOTUS framework, which is being developed for LOCA applications in response to the proposed new rulemaking in 10 CFR 50.46c [58]. The key implications of this proposition are that the core, fuels, and cladding performance cannot be evaluated in isolation anymore. Both cladding and Emergency Core Cooling System (ECCS) performance need to be considered in a coupled manner and the safety analyses have to be carried out in a multi-physics framework. A safety analysis involves several disciplines, which are computationally loosely (externally)

coupled to facilitate the process and maintenance of legacy codes and methods. The focus of LOTUS is to establish the automation interfaces among the five disciplines including [48]: (1) core design automation, which focuses on automating the cross-section generation, core design, and power maneuvering process; (2) fuel performance, which focuses on automating the interface between core design and fuel performance calculations and the interface between fuel performance and system analysis; (3) system analysis, which focuses on automating the process required to setup large number of system analysis codes runs needed to facilitate Risk-Informed Safety Margin Characterization (RISMC) applications on LOCA; (4) uncertainty quantification, which focuses on uncertainty quantification and sensitivity analysis, as well as establishing the interfaces to enable combined deterministic and probabilistic analysis; and (5) core design optimization, which focuses on developing core design optimization tool that can perform in-core and out-of-core design optimization.

Step 1: Generate input files for different physics codes.

As an integrated multi-physics tool, LOTUS has the capability to provide a first-of-a-kind safety analysis capability that is efficient and affordable to the plant owners and operators to provide quantitative estimates of design or operational margin loss or gain associated with various combinations of changes in the plant (e.g., digital I&C upgrades). The first component of LOTUS is called LOTUS-IN, which is a common input processor that will be developed such that the input files for the different physics codes will be generated from a single common input file. The single common input file would contain the input syntax that is easily apprehended by the users. LOTUS_IN will convert the common input file into the input files readable by various computer codes such as the Virtual Environment for Reactor Applications Core Simulator (VERA-CS), the three-dimensional Reactor Excursion and Leak Analysis Program 5 (RELAP5-3D), FRAPCON/FRATRAN, etc. LOTUS_IN also prepares the scripts that would drive the execution of all the different physics codes. All of the plant information and sequence information should be considered in the input files of different codes. By incorporating a "plug-and-play" and task-oriented approach, LOTUS aims to integrate different physics codes together under one roof and each code is simply treated as a module that provides the input-output relationship for a specific analytical discipline.

Step 2: Perform MP-BEPU.

In this step, MP-BEPU is performed by the "plug-and-play" multi-physics environment of LOTUS, which is essentially a workflow engine with the capability to drive physics simulators, model complex systems, and provide risk assessment capabilities. The environment retrieves all values of interest from the output files and stores them in a more compact manner in an HDF5 format [59], which is a data model, library, and file format for storing and managing data. It supports an unlimited variety of data types and is designed for flexible and efficient input/output and for high-volume and complex data. HDF5 is portable and extensible, allowing applications to evolve in their use of HDF5. The HDF5 technology suite includes tools and applications for managing, manipulating, viewing, and analyzing data in the HDF5 format. The data are also easily accessible for use in other codes. Provided that the needed data were calculated and stored, any arbitrary codes can be added into the multi-physics integration environment in an ad-hoc manner and access previously generated data. This flexibility in storage allows for a plug-and-play environment. Some tasks implemented in this step include: (1) stochastic sampling of the Phenomenon Identification and Ranking Table (PIRT); (2) data mapping between disciplines; (3) preparation of a large number of input files with the perturbed model parameters generated from the stochastic sampling; and (4) the execution of a large number of simulations. Reactor safety analysis calculations are normally done in two sequential steps [48]:

Step 2.1 is the steady-state initialization. The parameters calculated in this step should match those of the plant conditions to ensure the accuracy of the coupled modeling and simulations. Figure 11 shows a schematic illustration of the LOTUS framework [48], with which all of the data mapping between disciplines is to be carried out through a central database in the HDF5 format.

Step 2.2 is the transient calculations to predict the plant accident behaviors. For transient calculations, the tightly coupled calculations between computer codes would be necessary. For instance, the coupling between computer codes for transient calculations (e.g., LOCA) will be carried out through tightly coupled simulations (i.e., coupled RELAP5-3D/FRAPTRAN or coupled RELAP5-3D/BISON runs) under LOCA conditions. The coupling between computer codes for steady-state initialization is done through Python, an interpreted, object-oriented, high-level programming language with dynamic semantics. Its high-level built in data structures, combined with dynamic typing and dynamic binding, make it very attractive for rapid application development, as well as for use as a scripting or glue language to connect existing components together.

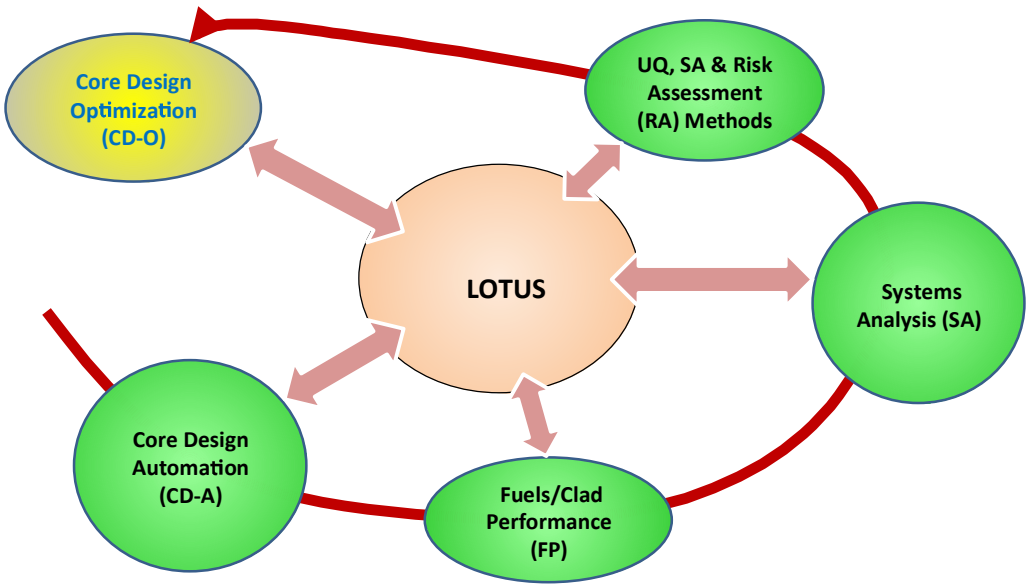


Figure 11. Schematic illustration of the LOTUS framework.

Step 3: Quantify safety margins by comparing statistical analysis results with regulatory limits.

To deal with the uncertainties existing in current simulation approaches to estimate and manage safety margins, significant research efforts are being made in exploring techniques to obtain more complete characterizations of analytical results. By providing more realistic information about the plant behaviors, BEPU approaches assists in identifying the most relevant safety parameters and allows more realistic comparison with acceptance criteria. By following the Code Scaling, Applicability, and Uncertainty (CSAU) methodology developed in NUREG/CR-5249 [60] and the EMDAP proposed in RG 1.203 [47], this MP-BEPU framework, LOTUS, propagates uncertainties directly from all of the uncertainty design and model parameters. The interactions between the various model parameters are directly solved within the MP-BEPU framework. This not only facilitates the automation of the process, but it is also more robust mathematically because of the advanced procedures considered to propagate uncertainties and/or perform global sensitivity and risk studies, which require that the inputs sampled are independent.

Margin quantification and risk assessment is performed in the post-processing of LOTUS. All of the outputs for the figures of merit will be extracted along with the perturbed parameters from PIRT. Uncertainty quantification establishes confidence intervals for outputs of interest and establish the 95/95 upper tolerance limit for the figures of merit (e.g., Peak Cladding Temperature Ratio [PCTR] or Equivalent Cladding Reacted Ratio [ECRR]) to provide the risk assessment capability. The 95/95 coverage/confidence has been recognized by the NRC as having sufficient conservatism for use in transient analyses.

Step 4: Perform sensitivity analysis to determine the contribution of parameters to system responses of interest.

In this step, sensitivity analysis is performed to quantify the amount of output variance attributable to specific input parameters. One obstacle to some uncertainty propagation techniques is the dimensionality of the uncertain input space. As the number of uncertain inputs grows, the number of samples required to represent that space accurately grows exponentially. To help alleviate this problem, global sensitivity analysis can be employed. Global sensitivity analysis methods explore the whole input parameter space by sampling chosen input parameters simultaneously, rather than performing perturbations of input parameters one-at-a-time. Global sensitivity analysis has the advantage of being able to identify nonlinear uncertainty structures over the global admissible input parameter space. The non-influential parameters in nonlinearly parameterized models can be fixed for subsequent model calibration or uncertainty propagation. In global sensitivity analysis, the effect of perturbing an input at the moment of a response is quantified. Often, a response is much more sensitive to some inputs than others. In some cases, no responses are sensitive to perturbations of a particular input. If this is discovered, the uncertainty in that parameter can be ignored without negatively impacting the BEPU analysis. Numerous sensitivity analysis methods exist, which should be carefully chosen based on the complexity and specific model to be evaluated. In this work, a sampling-based approach is used to evaluate those parameters that most profoundly affect the figures of merits.

4.4 Information Flow of Integrated Risk Assessment Process for Digital Instrumentation and Control

According to the descriptions of system-theoretic hazard analysis, integrated reliability analysis and risk-informed consequence analysis in the previous sections, this section describes the information flow of the proposed RADIC process among the different analysis stages, as shown in Figure 12.

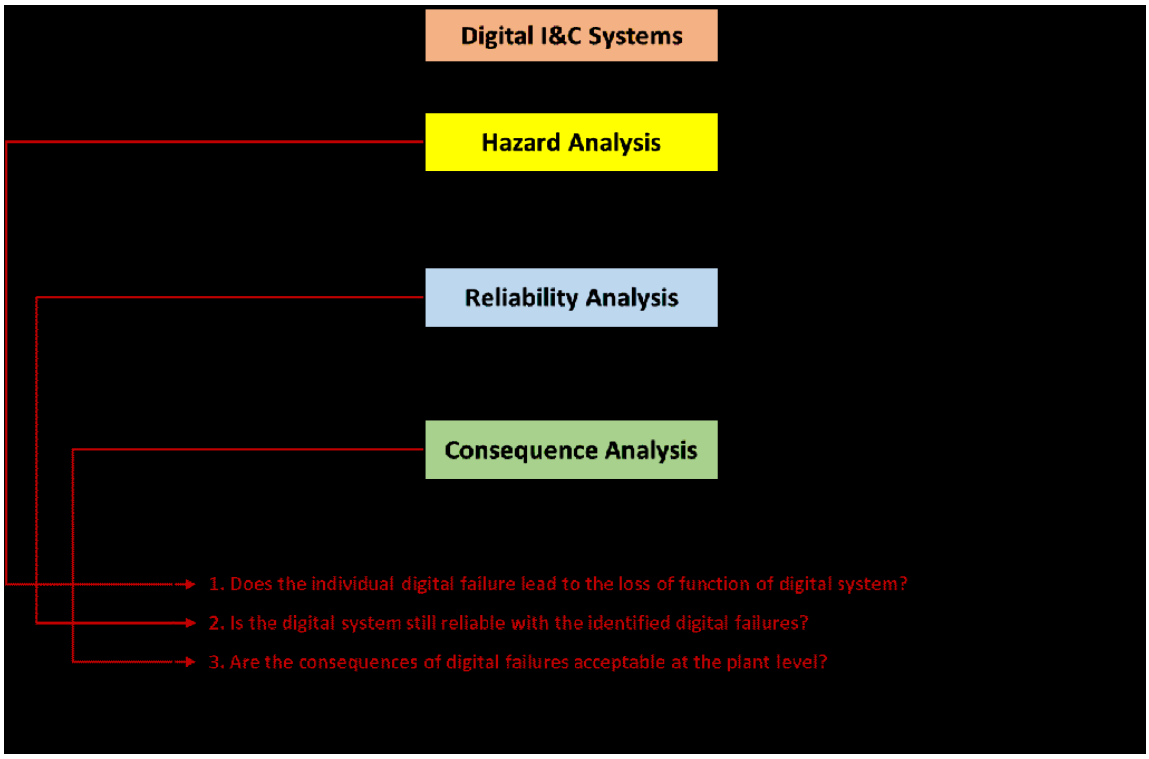


Figure 12. Illustration of the information flow of integrated risk assessment process for digital I&C.

Obtaining design information of the digital system of interest, hazard analysis is performed, which then provides minimal cut sets for individual-level assessment and integrated FTs including individual failures and CCFs to the reliability analysis stage. The main outcome from the reliability analysis stage to consequence analysis stage is the ETs containing potential unanalyzed events due to digital failures. Meanwhile results of reliability analysis (i.e., digital system failure probabilities, importance ranking of components) are also provided for system-level assessment. Finally, the consequence analysis stage provides the quantification of safety margins induced by digital upgrades or designs using the risk-informed MP-BEPU framework, LOTUS.

In a word, the proposed RADIC process contains risk analysis and risk evaluation, by which some suggestions could be provided to manage or reduce these risks induced by digital failures; some have been listed in Table 2. These suggestions on designs, maintenance, and testing are beneficial for vendors, utilities, system designers, and regulators, including some improvement within and outside of the digital systems. For instance, some recommendations can be summarized on how to eliminate software CCF triggers and latent faults based on the causal factors of software failures identified in hazard analysis. Important digital components could be identified in reliability analysis, so the failures of key digital systems may be reduced by increasing the reliability of these importance components. Based on the safety margin quantification by consequence analysis, some improvements of mitigation systems could be performed for coping.

Table 2. Digital I&C risk analysis, evaluation, and management.

	Key Analysis Results	**Acceptance Criteria**	**Suggestions to reduce risks**
Hazard Analysis	Integrated FTs including software CCFs	Does the individual digital failure lead to the loss of function of digital system?	Eliminate CCF triggers and latent faults *(within the digital systems)*
	Single points of failure in minimal cut sets		
Reliability Analysis	Probabilities of digital system failures	Is the digital system still reliable with the individual digital failures?	Increase the reliability of "important" digital components *(within the digital systems)*
	Important basic component combinations for prevention and mitigation		
	Probabilities of consequences of digital system failures		
Consequence Analysis	Safety margin quantification	Are the consequences of digital failures acceptable at the plant level?	Improvement of mitigation systems for coping *(outside the digital systems)*

5. COLLABORATION

Under the RISA Pathway of the LWRS Program, the development and application of the proposed RADIC process described in this report will be implemented with collaboration from the Plant Modernization Pathway of the LWRS Program, digital vendors (e.g., Westinghouse and Framatome), universities, utility partners, and other ongoing initiatives on data collections, methodology development, plant-specific risk analysis, and cybersecurity. This research is being coordinated via ongoing interactions between these organizations to develop integrated research plans that will maximize the effective allocation of resources and support development and deployment of digital I&C technologies. The collaboration with multiple partnerships will formulate an integrated assembly line to support the development, licensing, and deployment of advanced digital technologies to NPPs from data collection, methodology, and tool development to the applications on specific plants.

Within the multiple-partnership collaboration, each organization has its own focuses during the development and application of the proposed RADIC process. The activities and responsibilities of each organization are described below:

- Idaho National Laboratory (INL) will focus on the development and demonstration of the advanced methods and tools applied in the implementation of the RADIC process for the specific applications for the utilities and Plant Modernization Pathway. With the usage of these methods and tools, the RADIC process should be well-structured and clearly defined to provide risk analysis results, risk evaluation feedbacks, and risk management suggestions for the plant-specific applications of the digital technologies. The main efforts of INL will be made on the development and demonstration of approaches for the risk analysis stage, including systems-theoretic hazard analysis, integrated reliability analysis, and risk-informed consequence analysis. The conduct of the RADIC process requires the cooperation of system engineers, I&C design and software engineers, PRA and risk analysts, data analysts and multi-physics analysts. Targeting on the difficulties in the identification and evaluation of software CCFs existing in digital systems, the RADIC process will be demonstrated on the risk assessment of digital safety systems, such as RTS and ESFAS, which have more redundancy designs, and therefore, potential CCFs than non-safety systems.
- Collaborations with utilities and Plant Modernization Pathway of LWRS Program will be sought for the specific plant information including the designs and structures of digital I&C systems, usage of software and platforms, and respective hardware boundaries to conduct the RADIC process. Within this tight connection, the RADIC process will analyze and assess the benefits of advanced digital technologies developed in the Plant Modernization Pathway, then give feedbacks and improvement recommendations on risk management.
- Collaborations with digital I&C vendor partners will be sought for the information of digital SSCs for the reliability analysis, such as design requirements, failure modes, and rate. The methods and tools preliminarily developed for hazard analysis and reliability analysis could be tested and improved, which needs the cooperation of software engineers, designers of digital SSCs, and reliability and data analysts.
- Collaborations with university partners will be sought to support the development and demonstration of methods and tools for system-theoretic hazard analysis, integrated reliability analysis and risk-informed consequence analysis. Considering their previous research efforts, university partners have the capability to develop and apply the state-of-the-art methods and tools for the difficulties and challenges in identifying digital hazards (especially software CCFs), quantifying their effects on the reliability of digital systems and the plant responses via dynamic PRA.

- The collaboration with other initiatives on cybersecurity is ongoing to leverage their efforts to apply the risk assessment process on the cybersecurity of digital systems. Provided system information and security requirements, the RADIC process is expected to inform the identification and impact evaluation of cyber-attacks on the target digital systems of NPPs.

The collaborations for the digital I&C risk assessment project is illustrated in Figure 13. According to the demands on the software CCF study proposed by the NRC, the RADIC process aims to build the capability on the identification, reliability study, and impact evaluation of the potential software CCFs existing in the designs and upgrades of NPP digital systems.

Figure 13. Deep collaboration and contributions on the construction of the digital I&C risk assessment capability.

6. RESEARCH AND DEVELOPMENT ACTIVITIES

For the development, demonstration, deployment of the proposed RADIC process, some efforts are needed for the construction of the knowledge basis for methodology development, data collection for the testing of methods and tools, and collaboration with industry and university partners for plant-specific application. This chapter describes the main R&D activities including the identifying characteristics of CCFs in digital systems, clarifying data required for reliability analysis, and categorizing potential transient and accident scenarios to be analyzed.

6.1 Characteristics of Common Cause Failures in Digital Systems

Considering the importance of CCF effect on the safety of digital systems, the types and failure sources are discussed in this section by leveraging some concepts and definitions from previous efforts. In this report, CCFs in digital systems refer to the failure of any two or more modules, units, or divisions due to a single failure source. In an EPRI report [57], two fundamental controller architectures were presented to distinguish how a shared source can lead to a CCF of multiple digital SSCs:

- Type I design: each controller can influence or control multiple SSCs.
- Type II design: each controller can only influence or control one SSC, but two or more controllers can be affected by one shared resource.

According to these two types of designs and the location of the failure source, there are three different potential types of CCFs, as shown in Figure 14 (derived from the materials in [57]). In Type 1 CCFs, two SSCs share one controller where the failure source exists, the failure of this SSC leads to the malfunctions of both SSC 1 and SSC 2. In Type 2 CCFs, two SSCs are also affected by one controller, and the failure source locates in an external resource of this controller that results in the failure of the controller and two SSCs. In Type 3 CCFs, each SSC is influenced by one controller, and two controllers share one resource where the failure source exists. In Type 4 CCFs, two controllers have a common or similar design inside the SSC where the failure source may locate. It should be noted that the difference between the Type 1 and Type 2 (or between Type 3 and Type 4) CCF is the location of the failure source, depending on it is an internal defect or external disturbance.

According to the previous efforts [3] [57], several potential sources exist that may lead to the occurrence of a CCF:

(1) Random hardware failure. Multiple control functions through these components can be adversely affected. A Type 1 CCF can be initiated by a random hardware failure (e.g., the malfunction of a digital controller or a digital data communication interface). Type 2 and Type 3 CCFs can also be triggered by a random hardware failure, such as a power supply, network or workstation, etc.

(2) Design defect. In digital systems, a design defect or latent fault can be activated by a trigger and generate a failure (e.g., loss of function) or misbehavior (e.g., spurious actuation). An EPRI report [57] explained that, "*A design defect refers to an error in the digital equipment design that is introduced at any phase of the development life cycle (from conceptual design through implementation) and remains hidden in the system.*" Activating triggers can occur through a hardware random failure (e.g., the capability of hardware device is exceeded due to degradation), a software defect (e.g., unanticipated or untested conditions ignored in the design requirements), a rapid change of operating environment, or an operator error. Both Type 1 and Type 4 CCFs may be induced by design defects; for a Type 4 CCF, the shared resource may be similar software or digital platforms for a same function.

(3) Environmental hazards. An environmental change due to high temperature or high pressure, a seismic event, or a flooding event, may affect the performance of digital SSCs and cause a CCF in Type 2 and Type 3.

(4) Human errors. During operation, testing or maintenance, human errors have the potential to activate Type 2 and Type 3 CCFs.

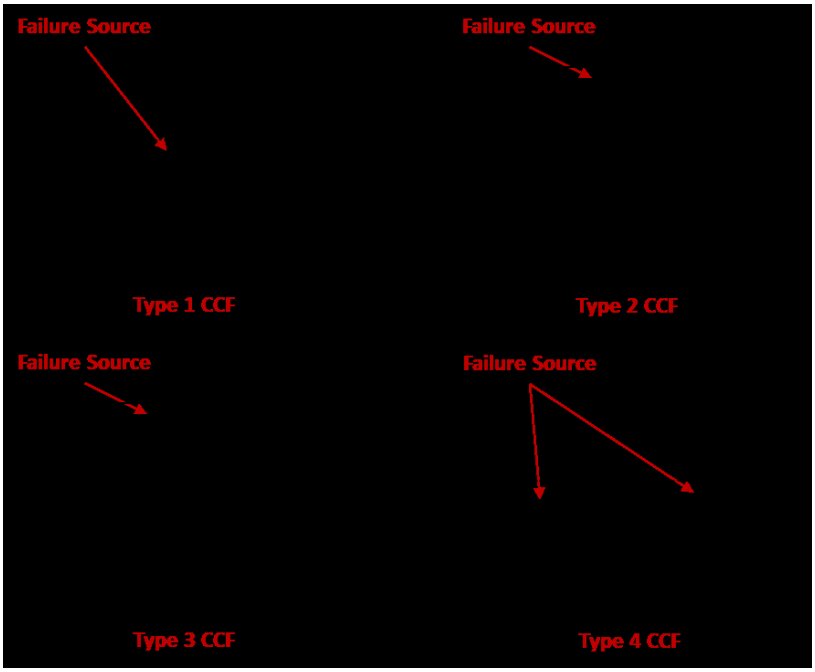


Figure 14. Three types of CCFs of digital SSCs caused by different locations of failure sources and controller designs.

In summary, an internal defect or hazardous state must be activated by an external activating condition (i.e., trigger) to become a failure. Especially for a CCF, a combination of internal latent fault and external input must exist and be encountered separately and concurrently for the malfunction of several digital SSCs. Therefore, internal diversity has the potential to eliminate a common internal latent fault, therefore, preventing a CCF. However, a balance should be reached between the cost on the use of diversity and the risk induced by a CCF.

6.2 Data Collection

To conduct the integrated reliability analysis, operating and testing data of target digital I&C systems should be identified, collected, and analyzed. Collaboration between INL, industry partners, and university partners have been initiated for data collection and the development of analysis methods. Considering the complex redundancy of digital safety systems (e.g., RTS and ESFAS) and tight interconnections between their divisions, this project will focus on the risk assessment of digital RTS and ESFAS. For the data collection of digital RTS, data on hardware failures and software failures should be identified and collected. The data request for the data sources (e.g., digital I&C vendors) will be generated based on the level of required information in the basic events of FTs built in the system-theoretic hazard analysis.

6.3 Unanalyzed Plant Events for Transient and Accident Analysis

New digital CCFs can cause unanalyzed plant events that may threaten plant safety without any additional analysis. According to NUREG-800 Chapter 15 [61], the evaluation of plant safety is assured by the analysis of the plant's responses to postulated equipment failures or malfunctions. CCFs have the potential to generate an unanalyzed event or sequence that may not be bounded by previous plant accident analyses; therefore, to challenge plant safety, such as core damage or a large early release [3]. A general

conclusion from PRAs of commercial NPPs is that CCFs are significant contributors to the unavailability of safety systems [4]. Existing analyses on CCF in I&C systems are mainly focusing on hardware failures. With the application and upgrades of new digital I&C systems, CCFs due to software design flaws, have become a potential threat to plant safety considering most redundancy designs are using the similar digital platforms or software in the operating and application systems. Normally, CCFs in digital I&C systems can be an initiator resulting in new unanalyzed plant transients or can affect the systems that are involved in the mitigation of accidents.

Three examples are listed in [3] to illustrate the new unanalyzed plant transients induced by CCFs:

(1) A typical overcooling event may be initiated considering the flow from one main feedwater pump whose analog controller provides full flow due to a random hardware failure. However, if two main feedwater pumps are controlled by one digital controller, a random hardware failure in this controller may cause a doubled flow mass rate from both pumps. This malfunction of the feedwater control system belongs to a Type 1 CCF, as described in Section 6.1, which leads to a new unanalyzed transient that threatens the departure from nuclear boiling ratio (DNBR) margin.

(2) A typical power distribution anomaly event may be realized considering a single control rod deviation or an erroneous withdrawal of one control rod group. But if multiple control rod groups are controlled by a digital rod controller, a single random hardware failure within this controller may cause the withdrawal of more than one control rod group. This CCF also belongs to a Type 1 CCF, which leads to a new unanalyzed transient challenging the local power density duel design limit.

(3) A typical safety system spurious actuation event may occur due to the wrong actuation of a single ESF function by ESFAS. For some digital ESF systems where multiple ESF functions are controlled by one digital controller, a single random hardware failure within this controller may spuriously actuate multiple ESF functions, which may challenge several critical safety functions. This is also a Type 1 CCF.

These examples denote that it is possible to cause a different unanalyzed plant-level event by a CCF in digital I&C systems, which is not covered by previous analysis for analog technology; therefore, it needs additional analysis to evaluate the impact of these failures at the plant level. Besides, other considerations should be taken into the effect of CCFs on the mitigation of accidents. Traditionally, a CCF due to a common design defect is not considered in the transient and accident analysis for design basis AOOs because an analog defect was considered unlikely enough to require no further studies in the design basis analysis. However, with the increase of inherent complexity of digital technology, the likelihood of a design defect also significantly increases compared to its analog equivalent. The updated likelihood considering the design defect in digital SSCs is not negligible and needs to be further analyzed to determine their effects on plant responses.

7. DESCRIPTION OF COMPUTER CODES

Both existing and advanced analysis tools will be utilized in the application of digital risk assessment. Due to the high costs associated with the qualification and regulatory acceptance of analytical tools, it is anticipated that the licensing of advanced nuclear technologies will rely predominantly on the current suite of tools used to assess AOO/DBA/BDBA events. However, because of the large uncertainties that currently exist for advanced nuclear technologies, the existing tools will need to be informed and enhanced to support the licensing and deployment of these technologies. The codes that have been identified for use in the execution of this research plan are detailed below.

7.1 Core Design and Analysis: VERA-CS

VERA-CS [62] includes coupled neutronics, thermal-hydraulics, and fuel temperature components with an isotopic depletion capability. The neutronics capability employed is based on MPACT [63], a three-dimensional (3D) whole core transport code. The thermal-hydraulics and fuel temperature models are provided by the Coolant Boiling in Rod Arrays (COBRA)-Two Fluid (TF) subchannel thermal-hydraulics analysis code (CTF) [64]. The isotopic depletion is performed using the ORIGEN [65] code system.

7.1.1 MPACT

As stated in the MPACT Theory Manual [63], MPACT is a 3D whole core transport code that can generate subpin-level power distributions. This is accomplished by solving an integral form of the Boltzmann transport equation for the heterogeneous reactor problem in which the detailed geometrical configuration of fuel components, such as the pellet and cladding, is explicitly retained. The cross-section data needed for the neutron transport calculation are obtained directly from a multi-group cross-section library, which has traditionally been used by lattice physics codes to generate few-group homogenized cross-sections for nodal core simulators. Hence, MPACT involves neither *a priori* homogenization nor group condensation to achieve the full core spatial solution.

The integral transport solution is obtained using the method of characteristics (MOC) and employs discrete ray tracing within each fuel pin. MPACT provides a 3D MOC solution; however, for practical reactor applications, the direct application of MOC to 3D core configuration requires considerable amounts of memory and computing time associated with the large number of rays. Therefore, an alternative approximate 3D solution method is implemented in MPACT for practical full core calculations, based on a “two-dimensional (2D)/one-dimensional (1D)” method in which MOC solutions are performed for each radial plane and the axial solution is performed using a lower-order 1D diffusion or SP3 approximation. The core is divided into several planes, each on the order of 5 to 10 cm thick, and the planar solution is obtained for each plane using 2D MOC. The axial solution is obtained for each pin, and the planar and axial problems are coupled through transverse leakage. The use of a lower order 1D solution, which is most often the nodal expansion method with the diffusion or P3 approximation, is justified by the fact that most heterogeneity in the core occurs in the radial direction, rather than the axial direction. Alternatively, a full 3D MOC solution can be performed, if necessary, should the computational resources be available.

The coarse mesh finite difference (CMFD) acceleration method, which was originally introduced to improve the efficiency of the nodal diffusion method, is used in MPACT for the acceleration of the whole core transport calculation. The basic mesh in the CMFD formulation is a pin cell, which is much coarser than the flat source regions defined for MOC calculations. (Typically, there are approximately 50 flat source regions in each fuel pin.) The concept of dynamic homogenization of group constants for the pin cell is the basis for the effectiveness of the CMFD formulation to accelerate whole core transport calculations. The intra-cell flux distribution determined from the MOC calculation is used to generate the homogenized cell constants, while the MOC cell surface-averaged currents are used to determine the

radial nodal coupling coefficients. The equivalence formalism makes it possible to generate the same transport solution with CMFD as the one obtained with the MOC calculation. In addition to the acceleration aspect of the CMFD formulation, it provides the framework for the 3D calculation in which the global 3D neutron balance is performed through the use of the MOC generated cell constants, radial coupling coefficients, and the nodal expansion method-generated axial coupling coefficients.

In the simulation of depletion, MPACT can call the ORIGEN code, which is included in the SCALE [66] package. However, MPACT has its own internal depletion model, which is based closely on ORIGEN, with a reduced isotope library and number of isotopes. The internal depletion model will be used for in the Use Case applications where MPACT is applied.

7.1.2 COBRA-TF

COBRA-TF [64] is a transient subchannel code based on the two-fluid formulation, in which the conservation equations of mass, energy, and momentum are solved for three fields, namely the vapor phase, continuous liquid, and entrained liquid droplets. The conservation equations for the three fields and heat transfer from within the fuel rods are solved using a semi-implicit finite-difference numerical scheme, with closure equations and physical models to account for interfacial mass transfer, interfacial drag forces, interfacial and wall heat transfer, inter-channel mixing, entrainment, and thermodynamic properties. The code is applicable to flow and heat transfer regimes beyond critical heat flux (CHF), and is capable of calculating reverse flow, counter flow, and crossflow with either 3D Cartesian or subchannel coordinates for thermal-hydraulic or heat transfer solutions. It allows for full 3D LWR core modeling and has been used extensively for LWR LOCA and non-LOCA analyses including the departure from nuclear boiling (DNB) analysis.

The COBRA-TF (CTF) code was originally developed by Pacific Northwest National Laboratory (PNNL) and has been updated over the last few decades by several organizations. CTF is being further improved as part of the VERA multi-physics software package as part of the DOE Consortium for the Advanced Simulation of Light Water Reactors (CASL) Energy Innovation Modeling and Simulation Hub. These enhancements include:

- Improvements to user-friendliness of the code through the creation of a preprocessor utility
- Code maintenance, including source version tracking, bug fixes, and the transition to modern Fortran
- The incorporation of an automated build and testing system using CMake/CTest/Tribits [67]
- The addition of new code outputs for better data accessibility and simulation visualization
- Extensive source code optimizations and full parallelization of the code, enabling fast simulation of full-core subchannel models
- Improvements to closure models, including Thom boiling heat transfer model, Yao-Hochreiter-Leech grid-heat-transfer enhancement model, and Tong factor for the W-3 CHF correlation
- The addition of a consistent set of steam tables from the IAPWS-97 standard [68]
- The application of an extensive automated code regression test suite to prevent code regression during development activities
- Code validation study with experimental data.

In a steady-state or transient CTF simulation subchannel data, such as flow rate, temperature, enthalpy, pressure, and fuel rod temperatures are projected onto a user-specified or preprocessor generated mesh and written to files in a format suitable for visualization. The freely available Paraview [69] software is used for visualizing the 3D data that results from large, full-core models and calculations.

7.2 Fuel Performance

The following codes are currently used throughout the U.S. commercial nuclear industry for fuel performance analysis.

7.2.1 FRAPCON/FRAPTRAN

FRAPCON/FRAPTRAN is a suite of codes developed by PNNL for the NRC for the purposes of performing fuel performance analyses under steady state (FRAPCON) and transient (FRAPTRAN) conditions. FRAPCON [70] is used to analyze the steady-state response of LWR fuel rods. The code calculates the temperature, pressure, and deformation of a fuel rod as functions of time-dependent fuel rod power and coolant boundary conditions. The phenomena modeled by FRAPCON include: (1) heat conduction through the fuel and cladding to the coolant; (2) cladding elastic and plastic deformation; (3) fuel-cladding mechanical interaction; (4) fission gas release from the fuel and rod internal pressure; and (5) cladding oxidation. The code contains necessary material properties, water properties, and heat-transfer correlations.

The Fuel Rod Analysis Program Transient (FRAPTRAN [71]) is a Fortran computer code that calculates the transient performance of LWR fuel rods during reactor transients and hypothetical accidents such as LOCAs, ATWS, and reactivity-initiated accidents. FRAPTRAN calculates the temperature and deformation history of a fuel rod as a function of time-dependent fuel rod power and coolant boundary conditions. Although FRAPTRAN can be used in "standalone" mode, it is often used in conjunction with, or with input from, other codes. The phenomena modeled by FRAPTRAN include: (1) heat conduction; (2) heat transfer from cladding to coolant; (3) elastic-plastic fuel and cladding deformation; (4) cladding oxidation; (5) fission gas release; and (6) fuel rod gas pressure.

7.2.2 BISON

BISON [72] is a finite element-based nuclear fuel performance code applicable to a variety of fuel forms including LWR fuel rods, tristructural isotopic (TRISO) particle fuel, and metallic rod and plate fuel. This advanced fuel performance code is being developed at INL and offers distinctive advantages over FRAPCON/FRAPTRAN such as 3D simulation capability, etc. BISON solves the fully coupled equations of thermomechanics and species diffusion, for either 1D spherical, 2D axisymmetric, or 3D geometries. Fuel models are included to describe temperature and burnup dependent thermal properties, fission product swelling, densification, thermal and irradiation creep, fracture, and fission gas production and release. Plasticity, irradiation growth, and thermal and irradiation creep models are implemented for clad materials. Models also are available to simulate gap heat transfer, mechanical contact, and the evolution of the gap/plenum pressure with plenum volume, gas temperature, and fission gas addition. BISON has been coupled to the mesoscale fuel performance code, MARMOT, demonstrating its fully coupled multi-scale fuel performance capability. BISON is based on the Multi-Physics Object-Oriented Simulation Environment (MOOSE) framework; therefore, BISON can efficiently solve problems using standard workstations or very large high-performance computers. BISON is currently being validated against a wide variety of integral LWR fuel rod experiments.

7.3 Systems Analysis Codes: RELAP5-3D

The RELAP5-3D [73] code has been developed for best-estimate transient simulation of LWR coolant systems during postulated accidents. Specific applications of the code have included simulations of transients in LWR systems, such as LOCA and ATWS, and operational transients, such as loss of

feedwater flow, loss of offsite power, station blackout, and turbine trip. RELAP5-3D, the latest in the series of RELAP5 codes, is a highly generic systems code that, in addition to calculating the behavior of the reactor coolant system during a transient, can be used to simulate a wide variety of hydraulic and thermal transients in both nuclear and nonnuclear systems involving mixtures of vapor, liquid, noncondensable gases, and nonvolatile solutes.

RELAP5-3D is suitable for the analysis of all transients and postulated accidents in LWR systems, including both large- and small-break LOCAs, as well as the full range of operational and postulated transient applications. Additional capabilities include space reactor simulations, gas-cooled reactor applications, fast breeder reactor modeling, and cardiovascular blood flow simulations.

The RELAP5-3D code is based on a nonhomogeneous and nonequilibrium model for the two-phase system that is solved by a fast, partially implicit numerical scheme to permit economical calculation of system transients. The objective of the RELAP5-3D development effort from the outset was to produce a code that included important first-order effects necessary for the accurate prediction of system transients, but that was sufficiently simple and cost-effective so that the conduct of parametric or sensitivity studies would be possible.

The code includes many generic component models from which general systems models can be developed and the progress of various postulated events can be simulated. The component models include pumps, valves, pipes, heat releasing or absorbing structures, reactor kinetics, electric heaters, jet pumps, turbines, compressors, separators, annuli, pressurizers, feedwater heaters, ECC mixers, accumulators, and control system components. In addition, special process models are included for effects such as form loss, flow at an abrupt area change, branching, choked flow, boron tracking, and noncondensable gas transport.

The system mathematical models are coupled into an efficient code structure. The code includes extensive input checking capability to help the user discover input errors and modeling and input inconsistencies. Also included are free-format input, restart, renodalization, and variable output edit features. These user conveniences were developed in recognition that the major cost associated with the use of a system transient code generally is in the engineering labor and time involved in accumulating system data and developing system models, while the computational cost associated with generation of the final result is usually small.

7.4 Containment Response: MELCOR

The Methods for Estimation of Leakages and Consequences of Releases (MELCOR) [74] is a computational code developed by SNL for the NRC, DOE, and the CSARP. The MELCOR code is primarily used by the NRC, U.S national laboratories, and university researchers for the conduct of severe accident analyses. Similar to the Modular Accident Analysis Program (MAAP) code, this code simulates the response of LWRs during severe accidents and is also used to determine success criteria and accident timing for NPP PRAs to obtain estimates of core damage frequency (CDF) and large early release frequency (LERF). Given a set of initiating events and operator actions, MELCOR predicts the plant's response as the accident progresses. The code is used for the following:

- The prediction of the timing of key events (e.g., core uncovery, core damage, core relocation to the lower plenum, vessel failure)
- The evaluation of the influence of mitigation systems and operator actions
- The prediction of the magnitude and timing of fission product releases
- The evaluation of uncertainties and sensitivities associated with severe accident phenomena.

Similar to MAAP, MELCOR results are used to determine success criteria and accident timing for NPP PRAs to obtain estimates of CDF and LERF.

7.5 Risk Assessment

The following codes represent the current suite of mature as well as advanced tools that are still being developed to perform PRAs of commercial NPPs operating in the United States.

7.5.1 SAPHIRE

The Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) [75] is a software application developed for performing a complete PRA using a personal computer running the Microsoft Windows operating system. It was developed by INL for the NRC.

SAPHIRE enables users to supply basic event data, create and solve fault and ETs, perform uncertainty analyses, and generate reports. In that way, analysts can perform PRAs for any complex system, facility, or process. For NPP PRAs, SAPHIRE can be used to model a plant's response to initiating events, quantify core damage frequencies, and identify important contributors to core damage (Level 1 PRA). The program can also be used to evaluate containment failure and release models for severe accident conditions given that core damage has occurred (Level 2 PRA). In so doing, the analyst can build the PRA model assuming that the reactor is initially at full power, low power, or shutdown. Finally, SAPHIRE can be used to analyze both internal and external events and, in a limited manner, to quantify the frequency of release consequences (Level 3 PRA).

7.5.2 CAFTA

The Computer-Aided Fault Tree Analysis (CAFTA) System [76] is a computer program developed by EPRI to create, edit, and quantify reliability models, utilizing FTs and ETs. CAFTA is used to build PRA models to assess Level 1 (core damage) and Level 2 (large early release) events. Given a set of initiating events, basic events, and operator actions, CAFTA quantifies the top gate of the FT. CAFTA is used to perform the following analyses:

- Develop, manage, and evaluate FTs and ETs
- Generate and analyze cut sets
- Evaluate the influence of modeled events
- Perform risk ranking evaluations
- Conduct sensitivity analyses.

CAFTA interfaces with multiple programs within the EPRI Risk and Reliability Workstation Suite of risk assessment tools to permit rapid and comprehensive risk assessments. Since CAFTA was developed by EPRI, it has been used by operating utilities in their conduct of plant risk assessments. The code has been developed and is maintained under a quality assurance program, which is in compliance with 10 CFR 50, Appendix B, and ISO 9001 quality assurance requirements.

7.5.3 EMRALD

EMRALD [77] is a dynamic PRA tool being developed at INL based on three-phase discrete event simulation. Traditional PRA modeling techniques are effective for many scenarios, but it is hard to capture time dependencies and any dynamic interactions using conventional techniques. EMRALD modeling methods are designed around traditional methods, yet enable an analyst to probabilistically model sequential procedures and see the progression of events through time that caused the outcome. Compiling the simulation results can show probabilities or patterns of time correlated failures.

An open communication protocol using the very common messaging platform XMPP [78] allows for easy coupling with other engineering tools. This coupling allows for direct interaction between the PRA model and physics-based simulations, so that simulated events can drive the PRA model and sampled PRA parameters can affect the simulation environment. The capabilities included in EMRALD permit PRA models to more easily and realistically account for the dynamic conditions associated with the

progression of plant transient and accident sequences including accounting for the occurrence of modeled operator actions taken to mitigate the event.

7.5.4 RAVEN

RAVEN (Risk Analysis and Virtual ENviroment) [79] is a software framework that is designed to perform parametric and stochastic analyses based on the response of complex systems codes. It is capable of communicating directly with the system codes described above that currently used to perform plant safety analyses. The provided Application Programming Interfaces (APIs) allow RAVEN to interact with any code as long as all the parameters that need to be perturbed are accessible by input files or via python interfaces. RAVEN is capable of investigating system response and exploring input spaces using various sampling schemes such as Monte Carlo, grid, or Latin hypercube. However, RAVEN's strength lies in its system feature discovery capabilities such as: constructing limit surfaces, separating regions of the input space leading to system failure, and using dynamic supervised learning techniques.

7.6 Integration Tools: LOTUS

LOTUS [48] is a risk-informed MP-BEPU analysis framework being developed at INL. It established the automation interfaces among the various disciplines depicted in Figure 7 of Section 4.1 such that uncertainties can be propagated consistently in multi-physics simulations. These disciplines include: (1) Core Design Automation, which focuses on automating the cross-section generation, core design, and power maneuvering process; (2) Fuel Performance, which focuses on automating the interface between core design and fuel performance calculations, and the interface between fuel performance and systems analysis; (3) Components Aging and Degradation, which focuses on automating the interface between core design and systems analysis with component aging and degradation; (4) System Analysis, which focuses on automating the process required to setup large numbers of system analysis code runs needed to facilitate RISA applications on LOCA and other accident scenarios; (5) Containment Response, which focuses on automating the interface between systems analysis and containment response; (6) Radioactive Material Release, which focuses automating the interface between systems analysis, containment response, and radioactive material release; (7) Uncertainty Quantification and Risk Assessment, which focuses on uncertainty quantification and sensitivity analysis in multi-physics simulations and on establishing the interfaces to enable combined deterministic and probabilistic analysis; and (8) Core Design and Plant Systems Optimization, which focuses on developing a core design and plant modifications optimization tool that can perform in-core and out-of-core design optimization.

LOTUS integrates existing computer codes, as well as advanced computer codes that are being developed under various DOE programs to provide feedback and guide the development of advanced tools. Regardless of the specific codes used to model the physics, the methodology discussed here is a paradigm shift in managing the uncertainties and assessing risks.

Conventional methods are strongly "code-oriented." The analyst has to be familiar with the details of the codes utilized, in particular with respect to their input and output structures. This represents a significant barrier for widespread use. It becomes apparent how difficult it is to make changes and accelerate progress under such a paradigm, especially in a heavily regulated environment where even a single line change in a code carries a heavy cost of bookkeeping and regulatory review.

The vision for LOTUS is to move toward to a "plug-and-play" approach where the codes are simply modules "under the hood" that provide the input-output relationships for a specific discipline. The focus shifts to managing the data stream at a system level. LOTUS is essentially a workflow engine with the capability to drive physics simulations, model complex systems, and provide risk assessments. A plug-and-play approach will enable plant owners and vendors to consider and further customize the LOTUS framework for utilizing their established codes and methods. Therefore, it could potentially become the engine for license-grade methodologies. In other words, it is possible that LOTUS technology could be

advanced in the future to a level of fidelity and maturity such that it could be used for licensing or regulatory applications.

8. PROJECT SCHEDULE

This proposed digital I&C risk strategy is to be conducted in collaboration with work being performed as part of broader industry efforts to develop, mature, license, and deploy advanced digital technologies in the industry to increase the reliability of digital systems and reduce costs in the operation, testing, and maintenance of NPPs. The project schedule is shown in Table 3. It should be noted that this schedule reflects current or short-term industry objectives and priorities for the licensing and deployment of the advanced digital technologies. This schedule is anticipated to evolve over the next several fiscal years (FYs) as additional information is obtained and interactions between industry, DOE, and the NRC occur.

Table 3. Timeline for RADIC activities.

Activities	**FY-2020**				**FY-2021**				**FY-2022**			
	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4
A. System-theoretic Hazard Analysis												
A1. Develop and Optimize an approach for system-theoretic hazard analysis.												
A2. Develop integrated FTs for hardware failures of digital RTS.												
A3. Perform system-theoretic process analysis for software failures of digital RTS.												
A4. Identify potential CCFs and triggers in the operation of digital RTS.												
A5. Apply the proposed hazard analysis approach (A2~A4) on digital ESFAS.												
B. Integrated Reliability Analysis												
B1. Develop and Optimize an approach for integrated reliability analysis.												
B2. Collect testing & operating data, and quantify the failures of digital RTS.												
B3. Perform prevention analysis to determine the optimal combinations of events and provide guidance on the component selection to reduce cost.												
B4. Measure and rank the importance of basic event, reduce the number of basic events for the integrated FTs of digital RTS.												
B5. Build ETs and quantify the probability of consequences of digital system failures.												
B6. Apply the proposed reliability analysis approach (A2~A5) on digital ESFAS.												

C. Risk-informed Consequence Analysis												
C1. Develop and Optimize an approach for risk-informed consequence analysis.												
C2. Identify unanalyzed scenarios due to digital RTS failures and generate input files for different physics codes.												
C3. Build/Extend RELAP5 model and perform analysis for unanalyzed transient scenarios with concurrent digital RTS failures.												
C4. Perform MP-BEPU for plant-specific risk analysis.												
C5. Quantify safety margins and perform sensitivity analysis.												
C6. Apply risk-informed consequence analysis on digital ESFAS.												
D. Cybersecurity of Digital Systems												
D1. Collaborate with DOE–NE cybersecurity program and leverage their efforts to apply the risk assessment process on cybersecurity of digital systems.												

9. ANTICIPATED OUTCOMES

The outcomes of this research effort will be part of the RISA R&D plan that is integrated with industry efforts to recover operating/safety margins and reduce operating costs by supporting the development, licensing, and deployment of digital (non-)safety I&C technologies.

The overall goal of this project is to deliver a strong technical basis to support effective, licensable, and secure digital I&C technologies by developing a risk assessment strategy for the digital upgrades/designs. To deal with the expensive licensing justifications from regulatory insights, this technical basis is instructive for nuclear vendors and utilities to effectively lower the costs associated with digital compliance and speed up industry advances. One of the key outcomes is the implementation of plant-specific risk assessment to provide a sustainable scientific basis for enabling industry to balance the induced risks, costs, reliability, and safety. The proposed RADIC process is expected to have the following characteristics:

(1). The workflow is well-structured, clearly defined, and will systematically integrate system-theoretic hazard analysis, integrated reliability analysis, and risk-informed consequence analysis.

(2). Advanced methods and tools are developed or applied to deal with the difficulties in risk analysis of the digital system, especially for the identification of CCFs, probability quantification of software failures and RI-MP-BEPU.

(3). The impact of digital SSC failures is quantitatively evaluated at the individual, system, and plant levels.

Although the RADIC process aims at the risk assessment of the digital upgrades of existing NPPs, it also provides insights on the new digital designs of advanced NPPs. Considering that new NPP designs are all expected to deploy digital I&C systems, the RADIC process has the capability to provide plant-specific support for risk analysis, evaluation, and management, particularly for digital safety I&C systems, which have more complex redundant designs and more potential threats from CCFs than non-safety systems. The applicability of this integrated process ranges from small replacements of individual analog components to complete upgrades or new designs of the entire digital systems. Each change on the systems, no matter whether they are small-scale or large-scale, should go through the risk assessment process, especially for safety systems.

In addition to the risk assessment process, the database for the reliability studies of digital SSCs is to be built according to the project schedule. The failure database could be used for the probability quantification of both software and hardware failures, and both independent failures and CCFs.

The RADIC process also provides recommendations on designs to manage the risks, thus, to support the development and deployment of advanced digital I&C technologies. Each part of risk analysis gives feedback on how to reduce the risks. For instance, the approach for system-theoretic hazard analysis identifies the triggers and latent faults related to the software CCFs, then the improvement on the designs can be proposed to eliminate CCF triggers and latent faults, which helps to optimize the diversity attributes in a cost-effective manner. As one step of integrated reliability analysis, prevention analysis is performed to determine the optimal basic component combinations for the prevention and mitigation of system failures. According to the ranking of component or event importance, suggestions can be given to increase the reliability of “important” digital components, thus, to increase the reliability of entire digital systems. The most economic optimal solution based on “importance ranking” can be used to support business decision-making to balance the cost and risk management.

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

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

[9] [Online]. Available: https://www.nrc.gov/docs/ML1605/ML16056A614.pdf.

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

[11] IEC, "Risk management - Risk assessment techniques," International Electrotechnical Commission, France, 2009.

[12] J. Liu, L. Martinez, H. Wang, R. M. Rodriguez and V. Nobozhilov, "Computing with Words in Risk Assessment," *International Journal of Computational Intelligence Systems,* vol. 3, no. 4, pp. 396-419, 2010.

[13] M. Rausand, Risk assessment : theory, methods, and applications, Hoboken, NJ: John Wiley & Sons Inc, 2011.

[14] IAEA, "IAEA Safety Glossary: Terminology used in Nuclear, Radiation, Radioactive Waste and Transport Safety," Department of Nuclear Safety and Security, International Atomic Energy Agency, Vienna, September 2006.

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

[16] W. E. Vesely, F. F. Goldberg, N. H. Roberts and D. F. Haasl, "Fault Tree Handbook," U.S.NRC, Washington, D.C., 1981.

[17] 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.

[18] U.S.NRC, "Probabilistic Risk Assessment (PRA)," U.S.NRC, 4 1 2018. [Online].

Available: https://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html#Definition.
[19] M. Philippart, "Chapter 12 - Human reliability analysis methods and tools," in *Space Safety and Human Performance*, Oxford, United Kingdom, Butterworth-Heinemann, 2018, pp. 501-568.
[20] R. W. Youngblood, "Risk Significance and Safety Significance," *Reliability Engineering and System Safety,* vol. 73, no. 2, pp. 121-136, 2001.
[21] IEC, "Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 2: Requirements for electrical/electronic/programmable electronic safety related systems.," International Elechtrotechnical Commission, Geneva, 2010.
[22] U.S.NRC, "Safety Failure Criterion," U.S.NRC, Washington, D.C., August 1977.
[23] "Information Technology: Vocabulary," ISO/IEC, Geneva, 2015.
[24] "Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants," IAEA, Vienna, Austria, 2018.
[25] "APR1400 Desing Control Document Tier 2. Chapter 7: Instrumentation and Controls," Korea Electric Power Corporation; , Korea Hydro & Nuclear Power Co., Ltd;, South Korea, 2018.
[26] 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..
[27] N. Leveson, "The Role of Software In Spacecraft Accidents," *AIAA Journal of Spacecraft and Rockets,* vol. 41, no. 4, July 2004.
[28] 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.
[29] 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.
[30] J. Gustafsson, "Reliability Analysis of Safety-related Digital Instrumentation and Control in a Nuclear Power Plant," Royal Institute of Technology, May 2012.
[31] U.S.NRC, "Guidelines on Modeling Common Cause Failures in Probabilistic Risk Assessment," U.S.NRC, Washington, D.C., November 1998.
[32] IEEE, "IEEE Recommended Practice on Software Reliability," IEEE, March 2008.
[33] B. A. Gran and A. Helminen, "The BBN Methodology: Progress Report," OECD Halden Reactor Project, August 2002.
[34] O. Backstrom, J.-E. Holmberg, M. Jockenhovel-Barttfeld, M. Porthin, A. Taurines and T. Tyrvainen, "Software reliability analysis for PSA: failure mode and data analysis," Nordic Nuclear Safety Research (NSK), Roskilde, Denmark, July 2015.
[35] H. Eom, G. Park, H. Kang and S. Jang, "Reliability Assessment Of A Safety-Critical Software By Using Generalized Bayesian Nets," in *Proc. of Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC&HMIT 2009*, Knoxville, Tennessee, April 2009.
[36] G. Dahll, B. Liwang and U. Pulkkinen, "Software-Based System Reliability," Working Group on Risk Assessment (WGRISK) of the Nuclear Energy Agency, January 26, 2007.
[37] EPRI, "Estimating Failure Rates in Highly Reliable Digital Systems," EPRI, Palo Alto,

CA., 2010.
[38] T.-L. Chu, G. Martinez-guridi, M. Yue, P. Samanta, G. Vinod and J. Lehner, "Workshop on Philosophical Basis for Incorporating Software Failures in a Probabilistic Risk Assessment," Brookhaven National Laboratory , November 2009.
[39] IEC, "Nuclear Power Plants - Instrumentation and Control Systems important to Safety - Classification aof Instrumentation and Control Functions," IEC, Gevena, 2005.
[40] SSM, "Licensing of safety critical software for nuclear reactors — Common position of seven European nuclear regulators and authorized technical support organisations," SSM, Stockholm, 2010.
[41] P. V. Varde, J. G. Choi, D. Y. Lee and J. B. Han, "Reliability Analysis of Protection System of Advanced Pressurized Water Reactor-APR 1400," Korea Atomic Energy Research Institute, South Korea, 2003.
[42] S. Authén, E. Wallgren and S. Eriksson, "Development of the Ringhals 1 PSA with Regard to the Implementation of a Digital Reactor Protection System," in *Proc. 10th International Probabilistic Safety Assessment & Management Conference, PSAM 10*, Seattle, Washington, June 7–11, 2010.
[43] B. Enzinna, L. Shi and S. Yang, "Software Common-Cause Failure Probability Assessment," in *Proc. of Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC&HMIT 2009*, Knoxville, Tennessee, April 5–9, 2009.
[44] K. Jänkälä, "Reliability of New Plant Automation of Loviisa NPP," in *Proceedings of the DIGREL seminar "Development of best practice guidelines on failure modes taxonomy for reliability assessment of digital I&C systems for PSA"*, Espoo, Finland, October 25, 2011.
[45] R. L. Boring, "Top-down and Bottom-up Definitions of Human Failure Events in Human Reliability Analysis," in *Proceedings of Human Factors and Ergonomics Society 58th Annual Meeting*, Chicago, IL, 2014.
[46] H. Zhang, R. Szilard, S. Hess and R. Sugrue, "A Strategic Approach to Employ Risk-Informed Methods to Enable Margin Recovery of Nuclear Power Plants Operating Margins," Idaho National Laboratory, Idaho Fall,s ID, September 2018.
[47] U.S.NRC, "Regulatory Guide 1.203: Transient and Accident Analysis Methods," U.S.NRC, Washington, D.C., 2005.
[48] H. Zhang, R. Szilard, A. Epiney, C. Parisi, R. Vaghetto, A. Vanni and K. Neptune, "Industry Application ECCS/LOCA Integrated Cladding/Emergency Core Cooling System Performance: Demonstration of LOTUS-Baseline Coupled Analysis of the South Texas Plant Model," INL, Idaho Falls, ID, June 2017.
[49] U.S.NRC, "10 CFR 73.54 Protection of digital computer and communication systems and networks," U.S.NRC, Washington, D.C., 2009.
[50] U.S.NRC, "Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities," U.S.NRC, Washington, D.C., January 2010.
[51] U.S.NRC, "Regulatory Guide 1.152. "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"," U.S.NRC, Washington, D.C., July 2011.
[52] NEI, "Cyber Security Plan for Nuclear Power Reactors," NEI, Washington, D.C., April 2010.
[53] U.S.NRC, "Method of Performing Diversity and Defense-in-Depth Analysis of Reactor

Protection Systems," U.S.NRC, Washington, D.C., 1994.
[54] U.S.NRC, "Technical Specification Required Shutdown Due to Core Protection," U.S.NRC, Washington, D.C., October 2005.
[55] U.S.NRC, "Design Defect in Safeguards Bus Sequencer Test Logic Places Both Units," U.S.NRC, Washington, D.C., July 1995.
[56] 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.
[57] ANS, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants," ANS, 1983.
[58] P. D. Blanchard and B. R. Worrell, "Top Event Prevention Analysis A Method for Identifying Combinations of Events Important to Safety," in *2002 International Topical Meeting on Probabilistic Safety Assessment and Analysis*, October 2002.
[59] EPRI, "Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems," EPRI, Palo Alto, CA, 2016.
[60] U.S.NRC, "Draft Regulatory Guide DG-1263, Establishing Analytical Limites for Zirconium-based Alloy Cladding," U.S.NRC, Washington, D.C., 2011.
[61] T. H. G. [Online]. Available: https://www.hdfgroup.org/HDF5/.
[62] U. "Quantifying Reactor Safety Margins," U.S.NRC, Washington, D.C., Octorber 1989.
[63] U.S.NRC, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition — Transient and Accident Analysis," U.S.NRC, Washington, D.C., 2007.
[64] S. Palmtag and A. Godfrey, "VERA Common Input User Manual, Version 2.0.0," CASL, February 2015.
[65] B. Collins, T. J. Downar, J. Gehin, A. Godfrey, D. Jabaay, B. Kelley, K. S. Kim, B. Kochunas, E. Larsen, Y. Liu, W. R. Marin, S. Palmtag, M. Rose, T. Saller, S. Stimpson, J. Wang, W. Wieselquist and M. Young, "MPACT User's Manual Version 2.0.0," CASL, February 2015.
[66] M. N. Avramova and R. K. Salko, "CTF – A Thermal-Hydraulic Subchannel Code for LWRs Transient Analysis," Pennsylvania State University, March 2015.
[67] "https://www.ornl.gov/division/rnsd/projects/origen," [Online].
[68] "https://www.ornl.gov/scale," [Online].
[69] "https://cmake.org/," [Online].
[70] "http://www.iapws.org/relguide/IF97-Rev.html," [Online].
[71] "https://www.paraview.org/," [Online].
[72] U.S.NRC, "FRAPCON-3.5: A Computer Code for the Calculation of Steady-State, Thermal-Mechanical Behavior of Oxide Fuel Rods for High Burnup," U.S.NRC, Washington, DC, October 2014.
[73] U.S.NRC, "FRAPTRAN 1.4: A Computer Code for the Transient Analysis of Oxide Fuel Rods," U.S.NRC, Washington, DC, March 2011.
[74] J. D. Hales, R. L. Williamson, S. R. Novascone, G. Pastore, B. W. Spencer, D. S. Stafford, K. A. Gamble, D. M. Perez, R. J. Gardner, W. Liu, J. Galloway, C. Matthews, C. Unal and N. Carlson, "BISON Theory Manual, The Equations behind Nuclear Fuel Analysis," INL, Idaho Falls, ID, September 2016.

[75] "https://relap53d.inl.gov/SitePages/Home.aspx," [Online].
[76] "https://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6119/," [Online].
[77] "https://saphire.inl.gov/," [Online].
[78] "Risk and Reliability Workstation," EPRI, Palo Alto, CA, August 2012.
[79] "https://emrald.inl.gov/SitePages/Overview.aspx," [Online].