Guidance for Addressing Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems

Prepared by the Nuclear Energy Institute
July 2023

Revision Table

Revision	Description of Changes	Date Modified	Responsible Person
Rev E	Updated to account for SRM-SECY-22-0076. Restructured to support safety case development.	7/21/23	Campbell, Alan

Acknowledgements

This document was developed by the Nuclear Energy Institute. NEI acknowledges and appreciates the contributions of NEI members and other organizations in providing input, reviewing, and commenting on the document including:

NEI Project Lead: Alan Campbell, NEI

NEI Project Team: Warren Odess-Gillett, Westinghouse
Neil Archambo, Archambo EC
Ray Herb, Southern Nuclear Company
Jeremy Chenkovich, Dominion Energy
Mark Samselski, Constellation Energy

Notice

Executive Summary

Common Cause Failure (CCF) in High Safety-Significant, Safety-Related (HSSSR) Digital Instrumentation and Control (DI&C) Systems is a significant technical and regulatory issue that must be overcome to modernize the existing operating nuclear power plants and enable new reactor technology to be deployed. Historically, CCF has been addressed through the implementation of independent and diverse Instrumentation and Control (I&C) systems. The use of independent and diverse I&C systems may address some sources of CCF, but these systems do not sufficiently address other sources of CCF. Additionally, diverse I&C systems add complexity to the facility, divert resources from safety-significant activities, and increase Operations and Maintenance (O&M) costs. Independence and diversity are indeed useful design techniques; however, these design techniques should be used when supported by an engineering analysis. The Commission provided direction to NRC staff in SRM-SECY-22-0076 documenting an expanded policy that allows for new approaches to addressing CCF using risk insights. NEI 20-04, "The Nexus Between Safety and Operational Performance in the U.S. Nuclear Industry," provides data that displays the impact of risk-informed initiatives on the U.S. nuclear industry. Between 1992 and 2020, the U.S. nuclear industry reduced Core Damage Frequency (CDF) on average by a factor of 10. Focusing on safety significant issues allows the allocation of resources in the manner that most effectively improves safety.

This document provides a process for developing a new type of Diversity and Defense-in-Depth (D3) analysis. This document establishes a safety case using claims, arguments, and evidence to demonstrate that vulnerabilities to digital CCF have been adequately addressed.

This document provides the safety case which provides the details that demonstrate the output of the EPRI Digital Engineering Guideline (DEG), Hazards and Consequence Analysis in Digital Systems (HAZCADS), and Digital Reliability Analysis Methodology (DRAM) processes (References 13, 14, and 15) provide a D3 analysis addressing the SRM-SECY-22-0076 policy.

[redacted]

Table of Contents

Table of Figures

[redacted]

Table of Tables

1 INTRODUCTION

Common Cause Failure (CCF) in High Safety-Significant, Safety-Related (HSSSR) Digital Instrumentation and Control (DI&C) Systems is a significant technical and regulatory issue that must be overcome to modernize the existing operating nuclear power plants and enable new reactor technology to be deployed. Historically, CCF has been addressed through the implementation of independent and diverse Instrumentation and Control (I&C) systems. The use of independent and diverse I&C systems may address some sources of CCF, but these systems do not sufficiently address other sources of CCF. Additionally, diverse I&C systems add complexity to the facility as well as increase Operations and Maintenance (O&M) costs. Independence and diversity are indeed useful design techniques; however, these design techniques should be used when supported by an engineering analysis. The Commission provided direction to NRC staff in SRM-SECY-22-0076 documenting an expanded policy that allows for new approaches to addressing CCF using risk insights. NEI 20-04, "The Nexus Between Safety and Operational Performance in the U.S. Nuclear Industry," provides data that displays the impact of risk-informed initiatives on the U.S. nuclear industry. Between 1992 and 2020, the U.S. nuclear industry reduced Core Damage Frequency (CDF) on average by a factor of 10. Focusing on safety significant issues allows the allocation of resources in the manner that most effectively improves safety.

This document provides a process for developing a new type of Diversity and Defense-in-Depth (D3) analysis. This document establishes a safety case using claims, arguments, and evidence to demonstrate that vulnerabilities to digital CCF have been adequately addressed. This document provides the safety case which provides the details that demonstrate the output of the EPRI Digital Engineering Guideline (DEG), Hazards and Consequence Analysis in Digital Systems (HAZCADS), and Digital Reliability Analysis Methodology (DRAM) processes (References 13, 14, and 15) provide a D3 analysis addressing the SRM-SECY-22-0076 policy.

This process may be applied to operating reactor licensees or new plant applicants. Licensees and applicants should ensure the DI&C system design meets all other applicable regulatory requirements and applicable guidance. Applicants using this guidance for operating reactor license amendments and new plant applications using NUREG-0800 Standard Review Plan guidance can use this guidance to develop a D3 assessment to demonstrate that CCF has been adequately addressed. Applicants using this guidance for new plant applications using Regulatory Guide 1.233 can use this guidance to develop a D3 assessment to demonstrate the adequacy of special treatments applied to address CCF.

2 DEFINITIONS

Core Damage Frequency (CDF) – An expression of the likelihood that, given the way a reactor is designed and operated, an accident could cause the fuel in the reactor to be damaged.

Digital Common Cause Failure (CCF) – A latent design defect in active hardware components, software, or software-based logic resulting in a loss of function to multiple structures, systems, or components.

High Safety Significant Safety-Related (HSSSR) – Safety-related systems, structures, or components (SSCs) that perform safety-significant functions (e.g., Reactor Protection Systems and Engineered Safety Features Actuation Systems). These SSCs have one or more of the following: 1. Credited in FSAR to perform design functions that significantly contribute to plant safety; 2. Relied upon to initiate and complete control actions essential to maintaining plant parameters within acceptable limits for a Design Basis Event or maintain the plant in safe state after safe shutdown; and 3. Failure could directly lead to

accident conditions that have unacceptable consequences. Systems categorized as Risk Informed Safety Category 1 (RISC-1) in accordance with Regulatory Guide 1.201 are HSSSR.

Large Early Release Frequency (LERF) – An expression of the likelihood that an event involving a rapid, unmitigated release of airborne fission products from the containment to the environment that occurs before effective implementation of offsite emergency response, and protective actions, such that there is a potential for early health effects.

Software – The programs used to direct operations of a programmable digital device. Examples include computer programs and logic for programmable hardware devices, and data pertaining to its operation.

System Theoretic Process Analysis (STPA) – a hazard analysis technique developed by MIT that is based on systems engineering principles. It is a hazard analysis method that is part of a set of safety engineering methods developed by MIT under the umbrella heading of Systems-Theoretic Accident Model and Processes (STAMP).

The following definitions are from EPRI HAZCADS, EPRI DRAM and the STPA Handbook:

Control Method: The ad hoc, policy-based, plant procedure based, or technical features, functions, and capabilities that can be implemented to mitigate risk by protecting a system from a random or systematic failure, or detecting, responding, and recovering from a random or systematic failure.

Control Structure: A hierarchical control structure is a system model that is composed of feedback control loops. An effective control structure will enforce constraints on the behavior of the overall system.

Hazard: A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss). This definition is broader than the scope of what constitutes a “hazard” in the PRA.

Loss: A loss involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders.

Loss Scenario – A loss scenario describes the causal factors that can lead to unsafe control actions and to hazards.

Random Loss Scenario – A loss scenario caused by a random hardware failure. When a random loss scenario is not mitigated, the related unsafe control action (UCA) is a Single Point Vulnerability.

Risk Reduction Target (RRT) – Risk reduction to be achieved by the […] safety-related systems and/or other risk reduction measures in order to ensure that the tolerable risk is not exceeded.

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.

Systematic Loss Scenario – A loss scenario caused by a failure that happens in a deterministic (non-random) and predictable fashion from a certain cause, which can only be eliminated by a modification of

the design, operating procedures, or other relevant factors. When a systematic loss scenario is not mitigated, and the related unsafe control action (UCA) can occur in multiple redundancies of I&C equipment, the result is a common cause failure (CCF). Systematic loss scenarios are mitigated by the allocation of systematic control methods.

Unsafe Control Action (UCA): A control action that, in a particular context and worst-case environment, will lead to a hazard.

3 REGULATORY BASIS

3.1 SRM-SECY-22-0076

SRM-SECY-22-0076 provides NRC direction regarding an expanded policy on potential CCF in HSSSR DI&C systems. The approach provided within this technical report provides a risk-informed, performance-based analysis technique that identifies hazards, determines scenarios in which those hazards may occur, and applies defensive measures.

3.1.1 SRM-SECY-22-0076 Points 1-3

1. *The applicant must assess the defense in depth and diversity of the facility incorporating the proposed digital I&C system to demonstrate that vulnerabilities to digital CCFs have been adequately identified and addressed.*

   The defense-in-depth and diversity assessment must be commensurate with the risk significance of the proposed digital I&C system.

2. *In performing the defense-in-depth and diversity assessment, the applicant must analyze each postulated CCF using either best-estimate methods or a risk-informed approach or both.*

   When using best-estimate methods, the applicant must demonstrate adequate defense in depth and diversity within the facility's design for each event evaluated in the accident analysis section of the safety analysis report.

   When using a risk-informed approach, the applicant must include an evaluation of the approach against the Commission's policy and guidance, including any applicable regulations, for risk-informed decision making. The NRC staff will review applications that use risk-informed approaches for consistency with established NRC policy and guidance on risk-informed decision making (e.g., Regulatory Guide (RG) 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decision on Plant-Specific Changes to the Licensing Basis." RG 1.233, "Guidance for a Technology-inclusive, Risk-informed, and Performance-based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors").

3. *The defense-in-depth and diversity assessment must demonstrate that a postulated CCF can be reasonably prevented or mitigated or is not risk significant. The applicant must demonstrate the adequacy of any design techniques, prevention measures, or mitigation measures, other than diversity, that are credited in the assessment. The level of technical justification demonstrating the adequacy of these techniques or measures, other than diversity, to address potential CCFs must be commensurate with the risk significance of each postulated CCF.*

> *A diverse means that performs either the same function or a different function is acceptable to address a postulated CCF, provided that the assessment includes a documented basis showing that the diverse means is unlikely to be subject to the same CCF. The diverse means may be performed by a system that is not safety-related if the system is of sufficient quality to reliably perform the necessary function under the associated event conditions. Either automatic or manual actuation within an acceptable timeframe is an acceptable means of diverse actuation.*
>
> *If a postulated CCF is risk significant and the assessment does not demonstrate the adequacy of other design techniques, prevention measures, or mitigation measures, then a diverse means must be provided.*

The approach described within this technical report leverages EPRI processes to perform a D3 analysis to demonstrate that vulnerabilities to digital CCF have been adequately and addressed commensurate with the risk significance on the proposed HSSSR DI&C system. The proposed methodology leverages the "risk-informed approach" referenced in Point 2 and provides techniques and/or measures including, but not limited to, diversity commensurate with the risk significance of each postulated CCF as described in Point 3. The safety case is described in Section 5 provides the details that demonstrate the output of the EPRI DEG, HAZCADS, and DRAM processes provide a D3 analysis addressing SRM-SECY-22-0076.

3.1.2 SRM-SECY-22-0076 Point 4

4. *Main control room displays and controls that are independent and diverse from the proposed digital I&C system (i.e., unlikely to be subject to the same CCF) must be provided for manual, system-level actuation of risk-informed critical safety functions and monitoring of parameters that support the safety functions. These main control room displays and controls may be used to address point 3, above. The applicant may alternatively propose a different approach to this point in the policy if the plant design has a commensurate level of safety.*

SRM-SECY-22-0076 Point 4 assumes a digital CCF has already occurred and is intended to allow Reactor Operators to take manual actions. Point 4 prescribes Control Methods such as location (i.e., Main Control Room), diversity, and independence. The intended scope of Point 4 is "critical safety functions." The term "critical safety functions" is not defined within the regulatory infrastructure. The original functions proposed by the NRC staff in SECY-93-087 were not approved by the Commission in SRM-SECY-93-087 as a requirement but rather as "general guidance." BTP-7-19 provides a description of "critical safety functions" based upon the text that the Commission eliminated from SECY-93-087. SRM-SECY-93-087 states:

> *Further, the remainder of the discussion under the fourth part of the staff position is highly prescriptive and detailed (e.g., "shall be evaluated," "shall be sufficient," shall be hardwired," etc.). The Commission approves only that such prescriptiveness be considered as general guidance, the practicality of which should be determined on a case-by-case basis.*

BTP 7-19 refers to guidance in NUREG-0737, Supplement 1 for additional guidance on identifying "critical safety functions." NUREG-0737, Supplement 1 does not use the term "critical safety functions," nor does it provide criteria for determining required manual control capabilities. NUREG-0737, Supplement 1 provides minimum criteria for a Safety Parameter Display System (SPDS) including

location (“located convenient to the control room operators”), use case (“SPDS is used in addition to the basic components and serves to aid and augment these components”), and design criteria, such as:

- “Need not meet requirements of the single-failure criteria”
- “Need not be qualified to meet Class 1E requirements”
- “Shall be suitably isolate from electrical or electronic interference”
- “Shall be designed to incorporate accepted human factors principles…”

NUREG-0737, Supplement 1, Section 4.1.f provides the minimum information to be displayed to plant operators. The review guidance does not provide any requirements for establishing “critical safety functions” nor manual controls. The “critical safety function” term implies that a set of safety functions exists that are more important than other established safety functions without performing plant specific analysis to determine the validity of this conclusion. Additionally, the assumed definition of this term only includes functions pertinent to existing light water reactor designs. This is problematic for non-light water reactor technologies which may have different safety functions. Instead of focusing on “critical safety functions,” this alternate approach intends to identify design features external to the HSSSR DI&C system (and their Control Methods) required to maintain the safety of the plant.

For applicants using NUREG-0800, Post-Accident Monitoring and SPDS requirements exist to address the need for monitoring parameters that support safety functions. For applicants using Regulatory Guide 1.233, special treatment considerations and human factors engineering processes should indicate required monitoring parameters that support safety functions.

3.2 Other Regulatory Requirements

Appendix A provides further detail on relevant regulatory requirements that are considered in the development of this process OR are required to be considered by the applicant using this methodology.

4 SYSTEM DIAGNOSTIC PROCESS

The development of a safety case concluding that CCF has been adequately addressed is dependent on the analysis performed using the EPRI DEG, HAZCADS, and DRAM.

4.1 Process Overview

[redacted] These diagnostic processes provide effective means of identifying, analyzing, and addressing potential CCF. These processes are to be used within the context of the EPRI DEG which provides a systems engineering approach to the design and lifecycle management of DI&C systems. [redacted]

When using this process to support the modification of an operating plant, the applicant should refer to NISP-EN-004 for incorporation of these processes into the Standardized Design Process, IP-ENG-001.

EPRI Digital Engineering Guide (DEG) provides a systems engineering process by which engineers integrate digital technology into a nuclear power plant. It uses a graded approach based on configurability and consequence to address procurement, human factors engineering, data communications, cyber security, plant integration design, testing, configuration management and digital obsolescence management. The DEG provides an iterative design process to develop DI&C systems. The DEG provides the DI&C system scope, design, and plant interfaces for further analysis in the EPRI HAZCADS and DRAM processes. Insights (i.e., requirements and Control Methods) developed during the HAZCADS and DRAM processes are provided back into the DEG as design input. The design continues to mature as it progresses through the design phases and iterative diagnostic loops. Insights from HAZCADS and DRAM become more granular as the design reaches more granular levels of detail.

The following overview of EPRI HAZCADS and DRAM is intended to be descriptive, not instructional. Practitioners of these processes should consult EPRI HAZCADS (Reference 14) and DRAM (Reference 15) for detailed guidance.

4.1.1 EPRI HAZCADS Overview

EPRI HAZCADS is a diagnostic tool that identifies plant and system level hazards and consequences as well as their associated risk sensitivity. EPRI HAZCADS uses the DI&C and system interface design information provided by the EPRI DEG as inputs to its diagnostic process. EPRI HAZCADS uses two hazard/failure analysis methodologies: Systems Theoretic Process Analysis (STPA) and Fault Tree Analysis (FTA). The result of HAZCADS is identification of Stakeholder Losses, System Hazards, UCAs, and RRTs. The EPRI HAZCADS outputs interface with downstream processes that further analyze and apply Control Methods based upon causal factors.

Stakeholder Losses should be identified at a high level of abstraction, so they are relatively simple and bounding. Stakeholder Losses typically should not reference individual components or specific causes and may involve aspects of the environment that are not directly controlled by the system designer.

A Stakeholder Loss is related to one or more System Hazard. System Hazard identification in STPA identifies conditions that are inherently unsafe— regardless of the cause. Systems Hazards should be specified at a high-enough level that does not distinguish between causes related to technical failures, design errors, flawed requirements, or human procedures and interactions. The STPA Handbook identifies three basic criteria for defining System Hazards:

1. Hazards are states or conditions (not component-level causes or environmental states).

2. Hazards will lead to a loss in some worst-case environment.

3. Hazards must describe states or conditions to be prevented.

As the system design matures in detail, new hazards may be uncovered and the list of hazardous system states can be revisited and revised, as needed. Once Hazards are created, a control structure is developed to model the HSSSR system. A hierarchical control structure is composed of control loops consisting of process models, feedback signals, command signals, sensors, control algorithms, controllers, and human operators. A controller may provide control actions to control some process and to enforce constraints on the behavior of the controlled process. The control algorithm represents the controller's decision-making process—it determines the control actions to provide. Controllers also have process models that represent the controller's internal beliefs used to make decisions. Process models may include beliefs about the process being controlled or other relevant aspects of the system or the environment. Process models may be updated in part by feedback used to observe the controlled process.

A control structure will emphasize functional relationships and functional interactions, which is very useful for identifying problems like design flaws, requirement flaws, human errors, software errors, and even traditional physical component failures. A control structure model does not typically capture purely physical relationships like physical proximity between components or fire propagation. The physical processes being controlled are typically specified at the lowest level of the control structure while every level above specifies functional controllers that make decisions and directly or indirectly control the physical processes.

The control actions identified during the control structure modelling will be the basis for establishing UCAs. EPRI HAZCADS states that there are four ways a control action can be unsafe:

1. Control action not provided when conditions require it.

2. Control action provided when conditions do not require it.

3. Control action provided too early, provided too late, or provided in the wrong order.

4. Control action stopped too soon or provided too long.

An important attribute in determining a UCA is the timing requirements associated with a given control action. Realistic times should be considered in lieu of overly conservative estimates for improbable

licensing basis events. For example, a realistic break opening time should be used to determine the necessary response time to a Large Break Loss of Coolant Accident in lieu of an assumed double-ended guillotine break). These timing estimates are considered in the development of UCAs as well as performance of the risk sensitivity analysis.

RRTs are identified based upon risk sensitivity analyses using a PRA model. The RRT can be developed from one of five different pathways based upon the scope of the system under analysis, the stage of the design process, and whether the system(s) is modeled in the PRA. When performing the risk sensitivity analysis, it is assumed that the DI&C system has failed. The result may be a change in Core Damage Frequency (CDF) and Large Early Release Frequency (LERF). Some reactor technologies may use different risk metrics specific to the reactor design. For those reactor technologies, the RRT thresholds should align with industry accepted guidance. For reactor technologies that use CDF and LERF, the ΔCDF and ΔLERF are then mapped to the regions in RG 1.174 Figures 4 and 5 and used to determine the RRT as shown in Table 1. For instance, assume the ΔCDF of a complete failure of the HSSSR system is 1E-3, then to reach the level of non-risk-significance, the RRT would be A in Table 1. If ΔCDF and ΔLERF results provide different RRT results, then the most conservative RRT result is applied throughout the remaining process steps. If the ΔCDF result is 1E-2, then the RRT is not attainable and thus a new design needs to be created. Note that the changes in CDF and LERF as used in Table 1 are not indicative of the actual CDF or LERF expected after installation of the I&C system. The static and relative changes of CDF and LERF are used only for the purpose of providing a mechanism for risk-informing decisions about the HSSSR DI&C design.

Table 1:Establish RRT Based on ΔCDF and ΔLERF

RRT	**ΔCDF**	**ΔLERF**
Change the Design	ΔCDF > 1E-3	ΔLERF > 1E-4
A	1E-4 ≤ ΔCDF ≤ 1E-3	1E-5 ≤ ΔLERF ≤ 1E-4
B	1E-5 ≤ ΔCDF ≤ 1E-4	1E-6 ≤ ΔLERF ≤ 1E-5
C	1E-6 ≤ ΔCDF ≤ 1E-5	1E-7 ≤ ΔLERF ≤ 1E-6
D	ΔCDF ≤ 1E-6	ΔLERF ≤ 1E-7

4.1.2 EPRI DRAM Overview

EPRI DRAM is an analytical process using the results of HAZCADS (e.g., UCAs and RRTs) to identify Loss Scenarios (or causal factors) of UCAs and apply Control Methods commensurate with the RRT. EPRI DRAM provides an iterative reliability analysis that starts early in the conceptual design phase and continues through detailed design to achieve a sound design.

Loss Scenarios are developed such that specific causes of UCAs are identified that can be prevented and/or detected. EPRI DRAM defines two (2) types of Loss Scenarios:

1. Scenarios that drive the execution of UCAs.

2. Scenarios that improperly execute, or prevent execution of, control actions.

To develop a complete set of Loss Scenarios that provide the reasons why a UCA is manifested or why a control action is improperly executed, the control structure is decomposed for assessment as follows:

- Unsafe controller behaviors
- Inadequate feedback and information
- Failures in control paths
- Failures in controlled processes

Loss Scenarios consider data communications, combining functions, the sharing of resources and identical designs among redundant elements, and independence between layers of echelons of defense. Loss Scenarios consider operations of the HSSSR system and the potential for hardware failure cascading effects and error propagation.

This process is performed iteratively throughout the design lifecycle as the design matures. Design decisions (e.g., automatic function allocation, control structure changes, networking) are updated on the control structure hierarchy and drive modifications to the UCAs and Loss Scenarios. In doing so, the

applicant creates a bounding set of Loss Scenarios associated with System Hazards and Stakeholder Losses. For the purposes of this document, only Loss Scenarios associated with regulatory safety factors (e.g., core damage or radiological release) should be considered.

A Control Method is a method that can be implemented to prevent, mitigate, or respond/recover from a systematic Loss Scenario. The identification of systematic Control Methods suitable for any given Loss Scenario is highly dependent on the characteristics of the Loss Scenario itself, and since this process is a performance-based approach to development of Loss Scenarios, it also takes a performance-based approach to the identification and allocation of appropriate Control Methods. A systematic Control Method could be solely applied to one element in the HSSSR system (e.g., on a particular controller) or it can span multiple elements in the HSSSR system (e.g., multiple controllers or controller and equipment under control). Once a set of systematic Control Methods has been identified for a given Loss Scenario, each Control Method is individually scored to provide an objective comparison of the relative effectiveness of the Control Methods. A scoring method is used as a tool to perform a qualitative assessment of the Control Method effectiveness. A scoring method removes potential bias in the qualitative assessment. Each Control Method is evaluated separately for its Control Method effectiveness and in combination when more than one Control Method is applied to an I&C element or relationship set of I&C elements.

There are two parts to the scoring Control Method effectiveness:

1. Pre-scored systematic Control Methods for the control algorithm commensurate with the RRT.

   A set of pre-scored systematic Control Methods are established to mitigate the Loss Scenario of an inadequate control algorithm. These Control Methods are synthesized from IEC 61508 Part 3, Normative Annex A. Similar to how IEC 61508-3, Annex A is formatted in which a given technique or measure listed in the Annex is designated has Highly Recommended (HR), Recommended (R), or No Recommendation (-) for a given Safety Integrity Level, the pre-scored systematic Control Methods for the Loss Scenario of an inadequate control algorithm have the same nomenclature but for a given Risk Reduction Target.

   For each systematic Control Method synthesized from IEC 61508-3, Annex A, designated as “HR” for a given RRT, that algorithm Control Method must be used, or an alternative provided. A Control Method designated as “R” should be used, and if not, a justification for not using it is provided. A Control Method designated as “-” is used at the practitioner’s discretion, and if not, no justification for not using it is needed.

2. Score each Control Method individually to determine its effectiveness and compare the score to the benchmark set for the RRT.

   The Control Method scoring is used as a tool to perform a qualitative assessment of the Control Method Effectiveness (CME). A scoring method removes potential bias in the qualitative assessment and provides the relative effectiveness of a Control Method. Refer to EPRI DRAM for details regarding the CME scoring methodology.

   It is the combining of the Control Method attributes that assesses the CME. A set of attributes is used to objectively define critical characteristics of a Control Method. A set of baseline scores are established for each attribute to establish the effectiveness relationship. This process provides a means of “weighting” attributes based on their relative impact to effectiveness. For

example, an attribute of “Control Method type” that provides options for Ad Hoc, Policy, Plant Procedure and Technical would provide a higher baseline score to the Technical option vice the Ad Hoc option since a Technical Control Method is designed into the system. Likewise, an attribute of “Control Method strength” would provide a higher baseline score to a High strength than a Low strength. The baseline values are arbitrary values that provide a means to differentiate between the various combinations of Control Method attributes that are commensurate with an RRT.

A CME score is not probabilistic. It is a deterministic measure that qualitatively measures the CME score on a preferred scale. If all individual CME scores meet or exceed the requisite Control Method effectiveness for the RRT, then the RRT is achieved for the system. If an individual Control Method effectiveness score does not meet or exceed the requisite Control Method effectiveness for the RRT, then additional Control Methods are added and combined in attempt to achieve the requisite CME.

4.2 Process Clarifications for US Regulatory Compliance

EPRI HAZCADS and DRAM were not developed specifically for U.S. regulatory compliance. Instead, these processes were developed based on best practices from safety critical industries, international standards, and other bodies of knowledge. The following sections provide clarifications specific to compliance with U.S. NRC regulation, policy, and/or guidance.

4.2.1 EPRI HAZCADS Clarifications

The following are clarifications to the EPRI HAZCADS that shall be considered by the applicant to adequately address vulnerabilities of CCF.

4.2.2 EPRI DRAM Clarifications

The following are clarifications to the EPRI DRAM that shall be considered by the applicant to adequately address vulnerabilities of CCF.

[redacted]

5 SAFETY CASE DEVELOPMENT

The safety case structure provided in this section was adopted from ISO/IEC/IEEE 15026-2:2022. The safety case starts with a top-level claim for the system and uses a structured argument and evidence to support the claim. Through multiple levels of subordinate claims (sub-claims), the structured argument connects the top-level claim to the evidence.

The safety case is constructed by connecting key elements, which include:

- *Claims* which are assertions about a property of the system. Claims that are asserted as true without justification become assumptions and claims supporting the argument are called sub-claims.
- *Arguments* which link the evidence to the claim, which can be deterministic, probabilistic or qualitative.
- *Evidence* which supplies the basis for the justification of the claim. Some sources of evidence may include the design, the development process, testing, and inspections.

A simplified diagram of an assurance case is shown in Figure 1.

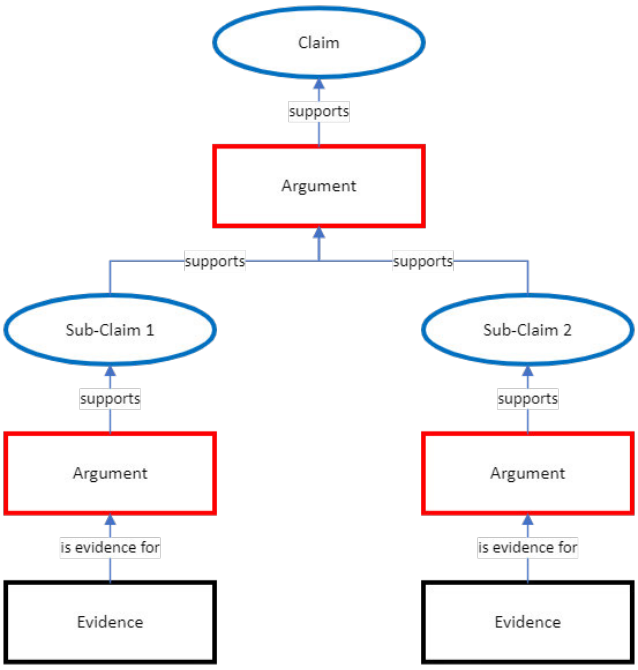

Figure 1: Safety Case Simplified Diagram

The results of the analysis performed should be described and summarized to provide arguments supporting the sub-claims, in conjunction, supporting a top claim. Each argument should be supported by analytical results. These detailed analytical results should be referenced and available for regulatory audit/inspection.

IAEA NP-T-3.27 provides an international perspective regarding establishing the dependability for safety-related DI&C systems. This approach is not intended to directly comply with this IAEA technical report; however, the concepts described in the general approach provide context for applicants establishing dependability. The technical report describes an approach that is "property based, vulnerability aware and standards informed."

- *A property based approach focuses directly on the behavior of, and constraints on, the system or software being assessed.*

  These attributes are described in typical design documents accompanying a new system design or plant modification. The EPRI DEG provides the design process associated with these properties to determine system requirements, interfaces with other plant SSCs, and testing requirements have been met.

- *Vulnerabilities are weaknesses in a system that could be detrimental to dependability (e.g., if division by zero is not caught by error handling) but are not strictly faults.*

  EPRI HAZCADS and DRAM provide the processes required to identify and address vulnerabilities to the system. [redacted]

- *Compliance with standards is an important part of the dependability assessment and […] adequate compliance with standards will need to be demonstrated as part of the overall licensing or approvals process.*

  Licensing processes associated with new reactor licensing or plant modifications require compliance with appropriate licensing basis standards.

5.1 Safety Case Structure

[redacted]

[redacted]

5.1.1 Safety Case Description

SRM-SECY-22-0076, Point 1 states:

> *The applicant must assess the defense in depth and diversity of the facility incorporating the proposed digital I&C system to demonstrate that vulnerabilities to digital CCFs have been adequately identified and addressed.*

The technical process described in EPRI HAZCADS and DRAM produces a diversity and defense-in-depth analysis that demonstrates vulnerabilities to digital CCF have been adequately identified and addressed.

[redacted]

5.1.2 Safety Case Uncertainty

[redacted]

5.2 Tier 1 Claim, Argument and Sub-Claims

[redacted]

[redacted]

5.3 Tier 2 Arguments, Evidence and Sub-Claims

[redacted]

5.3.1 EPRI HAZCADS and DRAM Efficacy

[redacted]

EPRI Research

EPRI HAZCADS and DRAM have been proven effective in identifying and addressing hazards and sources of failure in DI&C systems. EPRI performed research evaluating the effectiveness of hazard and failures analysis techniques in EPRI 3002000509, "Hazard Analysis Methods for Digital Instrumentation and Control Systems." The research report documents the comparative strengths and limitations of each of the evaluated methodologies. EPRI HAZCADS and DRAM leverage the results of this research to combine two (2) methods, STPA and FTA, to complement each other's strengths and limit the overall weakness of the combined process. Refer to EPRI 3002000509 for further information on the hazards and failure analysis methodologies researched.

EPRI provided further research on the application of hazards/failure analyses in EPRI 3002004995, "Program on Technology Innovation: Analysis of Hazard Models for Cyber Security, Phase I." EPRI 3002004995 concludes that "hazards methods currently are not well-equipped to assess certain phenomena important to cyber security…" The EPRI report goes on to state that "Phase II will evaluate a blended approach involving FTA and STPA, which could allow for a more complete analysis." Phase II (EPRI 3002004997) focused its research on the application of the blended approach as applied to cyber security. While these research results were primarily focused on cyber security hazards, their conclusions contributed to the creation of the HAZCADS methodology blending two techniques for hazards/failure analysis. Refer to EPRI 3002004995 and EPRI 3002004997 for further information.

EPRI HAZCADS provides additional information regarding the underlying research in Section 1.5 and Appendix C.

Available Evidence: EPRI 3002004995, EPRI 3002004997, EPRI 3002000509

NRC Research

NRC has conducted its own research on the efficacy of hazards analysis and STPA. TLR-RES/DE-2022-006, "Hazard Analysis: An Outline of Technical Bases for the Evaluation of Criteria, Methodology, and Results," documents an evaluation of the need "to develop criteria for technical bases supporting the evaluation of the criteria and methodology for, and of the results from, […] hazards analysis." In the process of this evaluation, the report identifies many significant conclusions including:

- *Current and recently concluded research efforts concerning a particular type of hazard analysis, concerning the use of operating experience and risk considerations, and concerning the implications and mitigation of common-cause failures in redundant actuation channels that employ digital technology, also provide insights into the necessary scope and content of hazard analyses.*

- *[…] hazard analysis may well be the only available avenue for attaining adequate assurance of acceptable operation of digital systems of more than trivial complexity.*

NRC staff also produced a research report, "Investigation of the Use of System-Theoretic Process Analysis at the NRC," (Reference 37) that "is part of a broader effort to enable the NRC staff to apply STPA for evaluating the HA portion of applicants' or licensees' I&C design submittals […] when these submittals are based on the STPA method." The report concludes:

- *The NRC participants recognized that STPA is a good complement to existing regulatory activities because STPA systematically analyzes areas that are not well represented in the current NRC regulatory review and oversight processes (e.g., hazards associated with the maintenance and operation of safety systems, complex software interactions, and identification of hazards associated with emergent properties). The current version of the NRC's SRP Chapter 7 does not provide guidance for reviewing whether such hazardous scenarios are identified and controlled.*

- *The NRC staff was able to use STPA to discover real flaws in I&C design, requirements, and architecture that were overlooked by teams using traditional methods.*

- *The NRC staff sees the potential benefit of using STPA in regulatory review and oversight.*

These two research reports provide NRC insights into the value of hazards analysis in NRC review activities. The NRC also acknowledges the effectiveness of the STPA process providing a structured approach to analyzing complex systems.

Available Evidence: ML22172A099, ML22272A315

STPA Use in Other Safety Critical Industries

STPA is used extensively in other safety industries and advanced reactor design certification as an effective means of hazard analysis. Many entities self-report utilization of STPA methodologies including, but not limited to:

Airbus DS	Google	Shell
Alstom	Gulfstream Aerospace	Toyota Motor North America
Amazon	Honda Motor Co., Ltd.	US Air Force
BAE Systems Inc	Hyundai UAM	US Army
Boeing	Intel Corp	US Department of Defense
Chevron	Lockheed Martin	US Department of Transportation
Collins Aerospace	Mazda Motor Corporation	US Federal Aviation Administration
Delta Airlines	Mitsubishi (Chemical/Electric/Heavy Industries)	US Federal Railroad Administration
Embraer	NASA	US Food and Drug Administration
Federal Aviation Administration	Nissan Motor Co., Ltd.	US National Transportation Safety Board
Ford Motor Company	Northrup Grumman	US Navy
General Dynamics	NuScale	US Space Force
GE Aviation	Raytheon	Volvo (Autonomous Systems and Cars)
GM	Rolls Royce	Whitely Aerospace

Table 2: Example STPA Users

The following provide examples of specific use-cases for STPA:

- The U.S. Department of Transportation developed an STPA software tool, SafetyHAT, that is available for public use to facilitate use of STPA for analyzing advanced vehicle technology.

- General Motors has fully integrated STPA into system safety processes for human-system interface projects to prevent driver error in safety critical systems.

- Boeing has utilized STPA to evaluate potential conflicts between large commercial air traffic and small un-crewed aircraft systems to provide requirements/Control Methods for air traffic control systems.

- NuScale performed a Hazard Analysis on four safety systems utilizing STPA methodology. The Hazard Analysis was included as part of the NuScale Final Safety Analysis Report and approved by the NRC in the Final Safety Evaluation Report (FSER). Per NuScale FSER, Section 7.1.8.6:

  > *The NRC staff concludes that the application provides information sufficient to demonstrate that the proposed [Hazard Analysis] has identified the hazards of concern, as well as the system requirements and constraints to eliminate, prevent, or control the*

> *hazards. The NRC staff also concludes that the [Hazard Analysis] information includes the necessary controls for the various contributory hazards, including design and implementation constraints, and the associated commitments.*

STPA is used in many non-nuclear industries with safety critical applications with successful results. Other industries demonstrate the value in using STPA to identify and resolve systematic failures during the design and development processes. Reference 35 provides a list of publications detailing various implementations of STPA across safety critical industries.

Available Evidence: References 21, 24, 25, 30, 34, 35, 39

Systematic Control Method Scoring

EPRI DRAM provides a methodology for qualitatively scoring the effectiveness of Systematic Control Methods. This is based on the premise that Systematic Control Methods are effective at addressing Systematic Loss Scenarios and applying multiple Systematic Control Methods improves overall effectiveness.

CME scores are generated based on information entropy calculations. Information theory is typically used to create a statistical description for data, and in this case, it is used to assess CME based on assigned scores for Control Method type and Control Method strength. Information theory calls this quantification process information entropy. Information entropy is described as the average level of information inherent in the variable's possible outcomes. In this case, the variable is the Control Method effectiveness based on Control Method attributes (e.g., type and strength). Quantifying information entropy is based on a log base 2 algorithm. Using the Information Theory entropy method for computing the CME is suitable for this process because it allows for the establishment of a reasonable scale for CME when combining the attributes. Using a scientific scoring process for this qualitative assessment of CME reduces the potential for human bias that may enter the assessment.

A combined CME score can be calculated when more than one Control Method is allocated to an I&C element to mitigate or eliminate a Loss Scenario. A benefit of using an information entropy-based scoring method for each individual Control Method, is that information entropy, by definition, is additive, but not merely the sum or mean of the Control Method effectiveness scores. A combined Control Method effectiveness score provides a geometrically weighted value. A geometrically weighted value reflects a situation when a shortage in one Control Method effectiveness limits the result and cannot be compensated by other Control Methods with better effectiveness scores. This prevents the practitioner from "stacking" low effectiveness Control Methods to meet a higher RRT.

Risk Informed Principles

SRM-SECY-22-0076 Point 2 states:

> *When using a risk-informed approach, the applicant must include an evaluation of the approach against the Commission's policy and guidance, including any applicable regulations, for risk-informed decision making.* ***The NRC staff will review applications that use risk-informed approaches for consistency with established NRC policy and guidance on risk-informed decision-making*** *(e.g., Regulatory Guide (RG) 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," RG 1.233, "Guidance for a Technology-inclusive, Risk-informed, and Performance-based*

Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors).” [emphasis added]

NRC Regulatory Guide (RG) 1.174 provides guidance for operating reactors using risk information for licensing basis changes. RG 1.233 provides guidance for new reactor applicants to establish licensing basis events, System, Structure and Component (SSC) classification, and defense-in-depth adequacy using risk information. When using NEI 20-07, the appropriate Regulatory Guide should be used to support. The following discussions provide information addressing key concepts in both documents.

RG 1.174 identifies a set of key principles to be addressed in risk-informed decision making (RIDM) for licensing basis changes. The five principles for risk-informed decision making are:

Principle 1: The proposed licensing basis change meets the current regulations unless it is explicitly related to a requested exemption (i.e., a specific exemption under 10 CFR 50.12).

Principle 2: The proposed licensing basis change is consistent with the defense-in-depth philosophy.

Principle 3: The proposed licensing basis change maintains sufficient safety margins.

Principle 4: When proposed licensing basis changes result in an increase in risk, the increases should be small and consistent with the intent of the Commission’s policy statement on safety goals for the operations of nuclear power plants.

Principle 5: The impact of the proposed licensing basis change should be monitored using performance measurement strategies.

The licensing and design processes of a HSSSR DI&C system should ensure that the DI&C system meets applicable regulations, be consistent with the defense-in-depth philosophy of the plant, maintain margins, manage risk such that it is acceptable, and continue to monitor performance. Principles 1, 2 and 3 are met through existing analysis required in licensing processes. Principles 4 and 5 are specific to the use of risk information and require supplemental information to be considered.

The objective of the NEI 20-07 methodology is to identify hazards, unsafe control actions, and Loss Scenarios as part of a systems-oriented, integrated DI&C evaluation. By utilizing this methodology, the failures in design and operations can be identified by modeling the potential interactions between software errors, human errors, component failures, and component interaction. By integrating hazard identification and PRA sensitivity analysis, RRTs can be derived in terms of order of magnitude of risk reduction that must be addressed with appropriate Control Methods in the design process and concept of operations; and still meet the five guiding principles. This process provides guidance for protection against DI&C CCFs through the identification of Loss Scenarios and Control Methods that reduce the identified risks, providing a defense-in-depth assessment basis. In other words, many of the defense-in-depth elements in terms of elimination and mitigation to different points in a potential Loss Scenario involving nuclear safety impacts are included.

The licensee implementing this process can demonstrate alignment with the five principles for risk-informed decision-making process in RG 1.174 using these concepts.

- Principle 1 Considerations: Existing licensing processes for new plants and operating plant modifications address requirements for ensuring current regulations are met unless an exemption is requested. No additional guidance is necessary.

- Principle 2 Considerations: Existing licensing processes for new plants and operating plant modifications address demonstration of the defense-in-depth philosophy. This approach provides evidence to support a safety claim that adequate defense-in-depth exists. No additional guidance is necessary.

- Principle 3 Considerations: Existing licensing processes for new plants and operating plant modifications address requirements for maintaining sufficient safety margins. No additional guidance is necessary.

- Principle 4 Considerations: Due to lack of consensus in quantifying software reliability, quantifying an absolute value of the proposed modification to plant risk is not considered in this approach. EPRI HAZCADS and DRAM does not provide a quantitative approach; rather, it describes a conservative, bounding risk analysis as allowed in RG 1.174 Section 2.2 which states:

  > *In other applications, calculated risk-importance measures or bounding risk calculations may be adequate.*

  The results of the risk sensitivity analysis are used to apply a graded approach to applying Control Methods to the proposed design iteratively throughout the design process. As previously described, the results derived from EPRI HAZCADS and DRAM do not represent an absolute value of the impact of the proposed modification on plant risk. Rather, the results inform the graded approach to allocating systematic Control Methods. The graded approach is consistent with the acceptance guidelines for changes to Core Damage Frequency and Large Early Release Frequency described in RG 1.174 Section 2.4. Aspects of the proposed modification that result in changes to CDF or LERF that map to Region 1 in RG 1.174 Figures 4 and 5 apply the most rigorous approach; whereas those that map to Region 3 apply the least rigor while maintaining the design basis commitments and consistency with the facility's defense-in-depth philosophy and safety margins.

  To use this method, certain PRA model attributes need to be met. These are:

  1. The PRA models the as-built, as-operated and maintained HSSSR system being replaced and reflects the operating experience. New plants without as-built PRA models will utilize up-to-date PRA models that reflect the current design status of the plant.

  2. Key assumptions and sources of uncertainty in the PRA models that can impact the assessment are addressed by assuming everything in the HSSSR system fails. By assuming the CCF occurs, uncertainty associated with the HSSSR DI&C system is a negligible factor since this process provides a bounding assessment of the failure of the HSSSR DI&C system. Because this process requires the use of a high-fidelity PRA model, other sources of uncertainty (e.g., parameter uncertainty) are unaffected by the sensitivity analysis performed by this process.

Additionally, RG 1.174 Section 2.6 states:

> *In making a regulatory decision, risk insights (including their associated uncertainties) are integrated with considerations of defense in depth and safety margins. The degree to which the risk insights (and their uncertainties) play a role […] depends on the application. […]*
>
> *Traditional engineering analysis provides insight into available margins and defense in depth. With few exceptions, these assessments are performed without any quantification of risk. However, a PRA can provide insights into the strengths and weaknesses of the plant design and operation relative to defense in depth.*

The process described in EPRI HAZCADS and DRAM combines risk insights from the PRA sensitivity study with a hazards analysis performed by a multidisciplinary team to identify the potential vulnerabilities to CCF, their impact on the plant, and identify effective measures to address risk-significant vulnerabilities. This process provides the system designers with greater insights to potential sources of failure and provides insights to the most risk-significant vulnerabilities that need to be addressed. Control Methods applied to address these vulnerabilities are qualitatively scored by a multidisciplinary team and applied in a graded approach.

- Principle 5 Considerations: RG 1.174 Section 3 states:

> *The licensee should propose monitoring programs that adequately track the performance of equipment that, when degraded, can affect the conclusions of the licensee's engineering evaluation and integrated decision-making that support the change to the licensing basis. The program should be capable of trending equipment performance after a change has been implemented to demonstrate that performance is consistent with the assumptions in the traditional engineering and probabilistic analyses conducted to justify the change. […] The program should be structured such that (1) SSCs are monitored commensurate with their safety importance (i.e., monitoring for SSCs categorized as having low safety significance may be less rigorous than that for SSCs of high safety significance), (2) feedback of information and corrective actions is timely, and (3) degradation in SSC performance is detected and corrected before plant safety can be compromised. The potential impact of observed SSC degradation on similar components in different systems throughout the plant should be considered.*

EPRI DRAM describes the application of Control Methods that are applied to address identified potential vulnerabilities. Control Methods are scored for their ability to Protect, Detect, and Respond & Recover. These three elements are considered for each Loss Scenario identified. The Protect function is intended to prevent a Loss Scenario from occurring and may include monitoring programs to detect adverse trends. The Detect function is intended to monitor system performance, identify a degraded system condition, and notify plant personnel prior to an adverse plant event from occurring. The Respond & Recover function is intended to provide a means of response after a loss occurs. The combination of these three functions ensures the Control Methods that have been applied to any given Loss Scenario provide appropriate rigor to ensure SSCs perform their intended functions OR the degraded condition is identified, and the plant remains in a safe state.

The practitioner should ensure system health monitoring and preventative maintenance activities address ongoing reliability indicators for the DI&C system. These activities can be credited for tracking and trending the DI&C system performance.

The process does not rely on the reliability of the DI&C system to be modeled in the PRA to address CCF; therefore, ongoing monitoring activities associated with ensuring the as-built PRA model is consistent with the results of this process are not necessary. Subsequent changes to the plant and PRA model after the implementation of the HSSSR DI&C system should consider the impacts of the change on the results of this process.

RG 1.233 "contains the NRC staff's general guidance on using the methodology described in NEI 18-04 to select [Licensing Basis Events], classify SSCs, assess the adequacy of a design in terms of providing layers of DID, identify appropriate programmatic controls, and help determine the appropriate scope and level of detail for information provided in applications for licenses, permits, certifications, and approvals for advanced non-LWR designs." EPRI HAZCADS and DRAM do not provide quantitative reliability data for DI&C systems. RG 1.233 provides the scope of functions under control and reliability targets for a safety-related DI&C system via the Licensing Basis Event selection and SSC classification (including defense-in-depth functions). These criteria are inputs to the initial/conceptual design phase. EPRI HAZCADS and DRAM can be used as a diagnostic tool based on the early design and continues through detailed design to provide insights used to identify and inform special treatments to address postulated CCF.

5.3.2 Postulated CCF Identification/Analysis Efficacy

[redacted]

[redacted]

5.3.3 Addressing Postulated CCF Efficacy

[redacted]

[redacted]

[redacted]

5.4 Tier 3 Arguments and Evidence

[redacted]

5.4.1 Resolution of Tier 2, Sub-Claim 1

[redacted]

5.4.2 Resolution of Tier 2, Sub-Claim 2

[redacted]

[redacted]

5.4.3 Resolution of Tier 2, Sub-Claim 3

[redacted]

5.4.4 Resolution of Tier 2, Sub-Claim 4

[redacted]

[redacted]

6 CONCLUSION

Using DI&C system design documentation provided from EPRI DEG output documents, the EPRI HAZCADS process is effective at identifying Stakeholder Losses, System Hazards, UCAs and RRTs. UCAs that are present in multiple redundancies of a DI&C system and impact core damage or large early releases are considered CCF. This process is effective at identifying the most likely and credible CCFs at a nuclear power plant. EPRI DRAM uses the EPRI HAZCADS results to identify Systematic Loss Scenarios that may lead to each CCF. Using the RRT and Systematic Loss Scenarios, Control Methods are applied to each causal factor commensurate with the risk significance identified.

The safety case provided within this document presents a clear, logical approach to demonstrating that vulnerabilities to CCF have been adequately addressed in DI&C systems for both operating and new reactors. The safety case provides the claims, arguments, and evidence necessary to demonstrate alignment with the Commission direction in SRM-SECY-22-0076.

7 REFERENCES

1. 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities”
2. 10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants”
3. 10 CFR Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”
4. 10 CFR Part 50.12, “Specific exemptions”
5. 10 CFR Part 50.54, “Conditions of licenses”
6. 10 CFR Part 50.55a, “Codes and standards”
7. 10 CFR Part 50.59, “Changes, tests and experiments”
8. 10 CFR Part 52, “Licenses, certifications, and approvals for nuclear power plants”
9. DI&C-ISG-06, “Digital Instrumentation and Controls Interim Staff Guidance, Revision 2, December 2018, U.S. NRC ADAMS Accession # ML18269A259
10. EPRI Report 3002000509, “Hazard Analysis Methods for Digital Instrumentation and Control Systems,” Revision 0, June 2013
11. EPRI Report 3002004995, “Program on Technology Innovation: Analysis of Hazard Models for Cyber Security: Phase I,” Revision 0, Nov. 2015
12. EPRI Report 3002004997, “Program on Technology Innovation: Cyber Hazards Analysis Risk Methodology, Phase II: A Risk Informed Approach,” Revision 0, Dec. 2015

13. EPRI Report 3002011816, “Digital Engineering Guide – Decision Making Using Systems Engineering,” Revision 0, January 2021

14. EPRI Report 3002016698, “HAZCADS: Hazards and Consequences Analysis for Digital Systems,” Revision 1, July 2021

15. EPRI Report 3002018387, “DRAM: Digital Reliability Analysis Methodology,” Revision 0, July 2021

16. IAEA NP-T-3.27, “Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants,” 2018

17. IEC 61508, Edition 2.0, 2010-04, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems”

18. IEEE 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations”

19. IEEE 603-1991, “Criteria for Safety Systems for Nuclear Power Generating Stations”

20. ISO/IEC/IEEE 15026-2:2022, “Systems and software engineering – Systems and software assurance – Part 2: Assurance case”

21. MIT Partnership for Systems Approaches to Safety and Security (PSASS), 2023 STAMP Workshop General Information (http://psas.scripts.mit.edu/home/2023-stamp-workshop-information/)

22. NEI 20-04, “The Nexus Between Safety and Operational Performance in the U.S. Nuclear Industry,” March 2020

23. NUREG-0800, Branch Technical Position (BTP) 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” Revision 8, Jan. 2021

24. NuScale Standard Plant Final Safety Analysis Report, Chapter Seven, Instrumentation and Controls, Part 2 – Tier 2, NuScale Power, ADAMS Accession # ML20224A495

25. NuScale Final Safety Evaluation Report, Chapter Seven, Instrumentation and Controls, ADAMS Accession # ML20204B028

26. Regulatory Guide 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Revision. 2, May 2011

27. Regulatory Guide 1.200, “Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities,” Revision 3, Dec. 2020

28. Regulatory Guide 1.201, “Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance,” Revision 1, May 2006

29. Regulatory Guide 1.233, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors," Revision 0, June 2020

30. SafetyHAT: A Transportation System Safety Hazard Analysis Tool, US Department of Transportation Volpe Center, Last Updated March 14, 2014 (https://www.volpe.dot.gov/infrastructure-systems-and-technology/advanced-vehicle-technology/safetyhat-transportation-system)

31. SECY-16-0070, "Integrated Strategy to Modernize the Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory Infrastructure," ADAMS Accession No. ML16126A140

32. SRM-SECY-22-0076, "Staff Requirements – SECY-22-0076 – Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems," May 25, 2023, ADAMS Accession No. ML23145A181

33. SRM-SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," July 21, 1993, ADAMS Accession No. ML003708056

34. Stanley, P. and Arcos Barraquero, V., "STPA Evaluation of Potential Conflicts Between Large Commercial Air Traffic and Small Uncrewed Aircraft Systems in the Terminal Airspace," MIT STAMP/STPA Workshop, June 2021 (http://psas.scripts.mit.edu/home/wp-content/uploads/2021/06/2021-06-30-1110__Stanley.pdf)

35. STAMP Publications, (http://sunnyday.mit.edu/theses/STAMP-publications-sorted-new.pdf)

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

37. Thomas, John, "Investigation of the Use of System-Theoretic Process Analysis at the NRC," September 2021, ADAMS Accession No. ML22272A315

38. TLR-RES/DE-2022-006, "Hazard Analysis: An Outline of Technical Bases for the Evaluation of Criteria, Methodology, and Results," June 17, 2022, ADAMS Accession No. ML22172A099

39. Vernacchia, Mark A., "Integration of STPA into GM System Safety Process," MIT STAMP Workshop, March 27, 2018 (http://psas.scripts.mit.edu/home/wp-content/uploads/2018/04/STPA-Integrated-into-GM-Safety-Process-20feb18-Approved-Rev1.pdf)

APPENDIX A. RELEVANT NRC REGULATORY FRAMEWORK

This Appendix describes the relationship between the process described in this document and the NRC regulatory framework.

Note that the regulations listed below may not necessarily apply to all applicants and licensees. The applicability of the regulatory requirements is determined by the plant-specific licensing basis and any proposed changes to the licensing basis associated with the proposed DI&C system under evaluation.

A.1. 10 CFR 50.54(jj), 10 CFR 50.55a(h)

IEEE 603-1991 or IEEE 279 -1971 as incorporated by reference requires, in part, that components and modules shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program.

It is assumed in this document that the HSSSR system is developed in accordance with these regulatory criteria. Pre-scored Systematic Control Methods are techniques and measures that may, in some cases, exceed the current regulatory guidance for meeting these regulatory criteria.

A.2. 10 CFR Part 50, Appendix A, “General Design Criteria (GDC)”

A.2.1. GDC 1, “Quality Standards and Records”

GDC 1, “Quality Standards and Records” – states, in part, that “Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.”

Since HSSSR systems are considered of high significance regarding the importance of safety functions to be performed, this GDC applies. It is assumed in this document that the HSSSR system is developed in accordance with these regulatory criteria. Pre-scored Systematic Control Methods are techniques and measures that may, in some cases, exceed the current regulatory guidance for meeting these regulatory criteria.

GDC 1 also states, in part, “Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function.”

It is assumed in this document that the HSSSR system is developed in accordance with the recognized industry codes and standards. Pre-scored Systematic Control Methods are techniques and measures that may, synthesized from the industry standard IEC 61508 Part 3, normative Annex A which is a recognized safety standard in the petrochemical industry.

GDC 1 also states, in part, “A quality assurance program shall be established and implemented to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.”

It is assumed in this document that the HSSSR system is developed in accordance with this regulatory criterion.

A.2.2. GDC 13, “Instrumentation and Control”

GDC 13, “Instrumentation and Control,” states, “Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.”

The HSSSR system requirements development needs to address the functional requirements stated in this GDC. The Control Methods generated from the EPRI DRAM ensures that HSSSR systematic failures like CCF do not prevent the HSSSR system from performing its safety function.

A.2.3. GDC 19, “Control Room”

GDC 19, “Control Room,” states, in part, “Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.”

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. The HSSSR system requirements development needs to address the functional requirements stated in this GDC. EPRI HAZCADS and DRAM take into consideration all HSSSR system equipment necessary to perform these functions.

A.2.4. GDC 20, “Protection System Functions”

GDC 20, “Protection System Functions” states, “The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.”

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. EPRI HAZCADS defines these as control actions, and then analyzes the hazards associated with these control actions when performed in an unsafe manner. EPRI HAZCADS and DRAM also take into consideration inadequate feedback from sensors and control actions that are not executed or not executed properly.

A.2.5. GDC 21, “Protection System Reliability and Testability”

GDC 21, “Protection System Reliability and Testability,” states, “The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the

acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred."

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. It is assumed that the HSSSR system must meet the single failure criterion as stated in the GDC. This process assesses HSSSR systematic failures including CCF.

A.2.6. GDC 22, "Protective System Independence"

GDC 22, "Protective System Independence," states in part, "Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. The design basis for operating nuclear plants includes functional diversity for the protective functions. For new plants, the safety analysis for the plant design will develop the necessary functional diversity. EPRI HAZCADS and DRAM evaluate the potential systematic failures of the HSSSR system including CCF. An important aspect of this process is identifying HSSSR systematic misbehaviors in the absence of any HSSSR system faults and failures.

A.2.7. GDC 23, "Protective System Failure Modes"

GDC 23, "Protective System Failure Modes," states, "The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced."

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. EPRI HAZCADS and DRAM identifies the potential UCAs and the Loss Scenarios that can cause these unsafe control actions. Failing in a safe state is a consideration in the EPRI HAZCADS process.

A.2.8. GDC 24, "Separation of Protection and Control"

GDC 24, "Separation of Protection and Control," states, "The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited to assure that safety is not significantly impaired."

It is assumed in this document that the HSSSR system must meet this regulation. EPRI HAZCADS and DRAM consider all interfaces to the HSSSR system to effectively evaluate the potential systematic failures including CCF.

A.2.9. GDC 25, “Protection System Requirements for Reactivity Control Malfunctions”

GDC 25, “Protection System Requirements for Reactivity Control Malfunctions,” states, “The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods.”

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. Not meeting this GDC would be considered a hazard in EPRI HAZCADS and DRAM for assessing the potential HSSSR systematic failures including CCF.

A.2.10. GDC 28, “Reactivity Limits”

GDC 28, “Reactivity Limits” states, “The reactivity control systems shall be designed to have a combined capability, in conjunction with poison addition by the emergency core cooling system, of reliably controlling reactivity changes to assure that under postulated accident conditions and with appropriate margin for stuck rods the capability to cool the core is maintained.”

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. Not meeting this GDC would be considered a hazard in EPRI HAZCADS and DRAM for assessing the potential HSSSR systematic failures including CCF.