TECHNICAL REPORT

NEI 20-07, Rev E.2

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

Prepared by the Nuclear Energy Institute
July 2025

Revision Table

Revision	Description of Changes	Date Modified	Responsible Person
Rev E.2	Incorporation of EPRI DEG, HAZCADS and DRAM changes. Incorporation of NRC feedback from Oct. 2024.	July 2025	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
	Andy Nack, Rivermist Engineering LLC
	Ray Herb, Southern Nuclear Company
	Jeremy Chenkovich, Dominion Energy
	Mark Samselski, Constellation Energy

Notice

Neither NEI, nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information apparatus, methods, or process disclosed in this report or that such may not infringe privately owned rights.

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. Digital (or software) CCF has been addressed through the implementation of independent and diverse Instrumentation and Control (I&C) systems. Other means of addressing digital CCF (e.g., extensive testing) are available; however, their applications are limited. 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; these design techniques, as with all 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 Defense-in-Depth and Diversity (D3) analysis for the facility using risk insights and hazards analysis techniques. This document establishes a safety case framework using claims, arguments, and evidence to demonstrate that vulnerabilities to digital CCF have been adequately addressed by this D3 analysis. The safety case depends on the outputs from EPRI engineering and diagnostic tools to provide evidence that supports claims and arguments described in this document. To prove that vulnerabilities to CCF have been adequately addressed, the D3 analysis must be able to demonstrate that:

1. Vulnerabilities to CCF have been adequately identified and addressed.

2. Each vulnerability to CCF has been reasonably prevented, mitigated, or is not risk significant.

This document provides the safety case framework that demonstrates 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. The safety case described within this document is broken into 3 "tiers" for descriptive purposes.

- Tier 1 establishes the primary objective of demonstrating that potential vulnerabilities of CCF have been adequately identified.

- Tier 2 provides sub-claims and arguments that demonstrate the efficacy of the EPRI HAZCADS and DRAM processes to identify and establish the criteria for each applicant to demonstrate they adequately executed these processes.

- Tier 3 will be completed by each applicant using this methodology. Tier 3 will consist of the arguments, and associated evidence required to complete the safety case using application-specific results from the EPRI HAZCADS and DRAM processes.

The completed safety case (i.e., this document AND the application specific Tier 3 information) constitutes a D3 analysis demonstrating that CCF in a HSSSR DI&C system has been adequately identified and addressed.

Table of Contents

Table of Figures

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. Digital (or software) CCF has been addressed through the implementation of independent and diverse Instrumentation and Control (I&C) systems. Other means of addressing digital CCF (e.g., extensive testing) are available; however, their applications are limited. 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; these design techniques, as with all 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 Defense-in-Depth and Diversity (D3) analysis for the facility using risk insights and hazards analysis techniques. This document establishes a safety case using claims, arguments, and evidence to demonstrate that vulnerabilities to digital CCF have been adequately addressed by this D3 analysis. 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 maintaining 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 an I&C 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 (or Stakeholder Loss): A loss, or stakeholder 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 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 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.

The EPRI HAZCADS and DRAM process analyzes the proposed DI&C system and its impact on the facility. As a result, the EPRI HAZCADS and DRAM process already addresses necessary manual actions through its diagnostic process and applies Control Methods commensurate with the risk significance to the plant. Like Point 4, EPRI HAZCADS and DRAM process assumes a digital CCF has occurred. The EPRI processes evaluate the risk impact of the postulated CCF to the nuclear power plant to identify vulnerabilities specific to the system design. The sensitivity analysis is performed consistent with risk-informed decision-making principles. Credited manual actions, or lack thereof, are accounted for in the risk sensitivity analysis resulting in insights into the plant design. This process used to address SRM-SECY-22-0076 Points 1-3 will identify the need for additional design features external to the DI&C system. For example, if the risk sensitivity analysis concludes a significant risk impact, the applicant is required to change the design. A design change may include the use of manual operator actions or design features intended to improve the facility’s defense-in-depth. External design features may be passive features of the reactor design or active features, such as an external watchdog not dependent on platform software that puts end devices in a safe state. The ability to maintain a commensurate level of safety is indicated by the change to the risk metrics used in the risk sensitivity analysis. These external features to the DI&C system should comply with applicable regulatory requirements including existing Human Factor Engineering (HFE) guidance for credited manual actions. This guidance is sufficient for evaluating time requirements associated with the location of manual actions. The EPRI processes are agnostic to reactor technology, focus on the critical risk metrics associated with the reactor design, rely on existing regulatory infrastructure, and, most importantly, demonstrate that the facility safety has been maintained.

3.2 Other Regulatory Requirements

Other regulatory requirements shall be addressed consistent with the applicants licensing basis. This guidance is only intended to address the applicant’s approach to addressing CCF consistent with SRM-SECY-22-0076.

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

The safety case developed in Section 5 is based on the execution of the EPRI HAZCADS and DRAM processes and the output documentation they produce. 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. The output of these processes will be used to provide evidence in the safety case detailed in Section 5. These processes, as leveraged in the safety case provided in Section 5, constitute a D3 analysis using risk insights.

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.

4.2 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. The following subsections are an overview of HAZCADS including the STPA process. For more information on these processes see References 14 and 36.

4.2.1 Identify Stakeholder Losses and System Hazards

In accordance with STPA, 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.

4.2.2 Model the Control Structure Hierarchy

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 structure should identify Controllers (which have programmed control algorithms and process models) and the Controlled Process(es). The interactions between the Controller and Controlled Process(es) are feedback (e.g., process variables indicating the status of the controlled process) and control actions (e.g., commands from the Controller to the Controlled Process element).

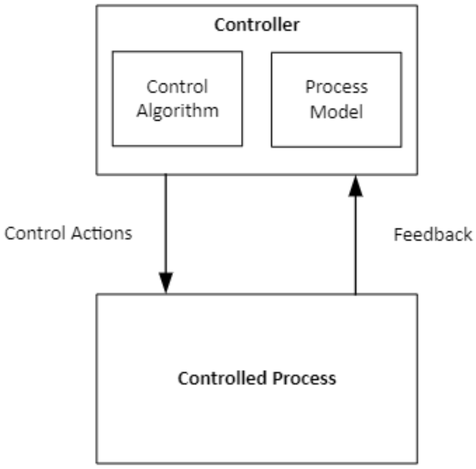


Figure 1: Generic Control Structure Hierarchy

The Control Structure Hierarchy provides a graphical representation of the system and its relationships for further analysis. As the design matures through the iterative DEG process, the Control Structure Hierarchy also matures in detail allowing for more granular insights. A controller can be a human or technology, in which case the Process Model and Control Algorithm are as follows:

Table 1: Types of Controllers and Their Attributes

Controller	Human	Technology
Process Model	Knowledge and beliefs of the Controlled Process	Programmer's knowledge and beliefs of the Controlled Process
Control Algorithm	Procedures	Internal Programming

As the design matures, the Control Structure Hierarchy will also mature to represent the same level of detail. During the initial design phase, one Controller may be representative of the entire system (e.g., Reactor Protection System) and one Controlled Process may be representative of all equipment under control. As the design matures, the Control Structure Hierarchy will represent the actual controllers (including operators), their allocated Feedback and Control Actions, the sensors providing the feedback, and end-devices (e.g., actuators) that execute the Control Actions.

4.2.3 Identify Unsafe Control Actions

The Control Actions identified during the control structure hierarchy 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 license 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.

4.2.4 Identify Risk Reduction Target

RRTs are identified based upon risk sensitivity analyses using a PRA model. The RRT can be developed from one of five different pathways, described below, 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.

EPRI HAZCADS includes Pathway 1 for systems that are not modeled, or whose failures do not contribute to top events, in the PRA. Pathway 1 provides guidance for a qualitative assessment of the risk associated with failure of these systems. This pathway is not anticipated to be used to support NEI 20-07.

Pathways 2 through 4 perform a risk sensitivity analysis assuming the DI&C system has failed. Pathways 2 through 4 are differentiated based upon their scope as follows:

- Pathway 2 - Scope of digital systems is associated with a system modeled in the PRA.
- Pathway 3: Scope of digital systems is associated with a sub-system (or components of a system) modeled in PRA.
- Pathway 4: Scope of digital system is associated with multiple plant systems modeled in PRA.

For large Light Water Reactors (LWRs) the result may be a change in Core Damage Frequency (CDF) and Large Early Release Frequency (LERF). Other 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 2: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

After EPRI HAZCADS has been used to diagnose an initial design, a set of Unsafe Control Actions (UCAs) will be identified. Pathway 5, Systems-Theoretic Informed Fault Tree (SIFT), may be used to map the UCAs to fault tree surrogate events to perform a risk sensitivity analysis. Risk sensitivity analyses are performed on UCAs, or combinations of UCAs (UCA Sets), to determine the risk impact each UCA (or UCA set). This provides the applicant more granular insights into each UCAs impact to plant risk.

4.2.5 Allocate RRT Scores

Once the UCAs are identified in Section 4.2.4, each UCA is assigned a Risk Reduction Target based on the selected pathway in Section 4.2.1. If Pathways 2-4 are used, all UCAs associated with the scope of the DI&C system will inherit the same RRT. If Pathway 5 is used, UCAs will be assigned an RRT commensurate with the results of the SIFT process.

4.2.6 Identify High-Level Loss Scenarios

Loss Scenarios are developed such that specific causes of UCAs are identified that can be prevented and/or detected. 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.

Four classes of Loss Scenarios are defined with syntax provided depending on the associated UCA. Each scenario class is provided with specific syntax to direct the user’s analysis.

- Class 1 Scenario: The controller is provided with correct feedback or information, but the control misbehaves and issues a UCA.
- Class 2 Scenario: The controller is provided with unsafe feedback or information and issues a UCA in response.
- Class 3 Scenario: The controller issues a safe control action, but this becomes unsafe on the way to the controlled process.
- Class 4 Scenario: The controller and control pathway are both functioning safely, but the controlled process enters an unsafe condition.

The STPA Handbook and EPRI HAZCADS guidance provides explicit direction on the appropriate syntax for each type of UCA (i.e., providing, not providing, timing, and duration).

In addition to identifying high-level loss scenarios, practitioners will identify preliminary control methods to facilitate later control method activities. The preliminary control methods at this stage are not scored until they are validated in later downstream processes (e.g., EPRI DRAM).

4.3 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. Both systematic and random failures are addressed by EPRI DRAM. This document only describes processes used to address systematic failures. For more information on DRAM see Reference 15.

4.3.1 Initiation

EPRI DRAM is a continuation of the HAZCADS process that provides guidance on analyzing the digital system reliability. Initial steps provided in the EPRI DRAM process provide direction on reviewing work completed in the EPRI DEG and EPRI HAZCADS processes including determining the scope of the DRAM assessment, reviewing the DEG design information, reviewing the HAZCADS control structure and UCAs, and reviewing the RRTs and Relationship Sets from DEG and HAZCADS.

4.3.2 Identify Control Effectiveness Profile

The Control Effectiveness Profile (CEP) is the random or systematic capability required for the system(s), achieved by the system architecture, design and allocated control methods. The process defined within this process is intended to solely address systematic failures; therefore, only the systematic capability is considered. The target CEP is equivalent to the HAZCADS RRT.

Table 3: Target CEP for Systematic Capability

HAZCADS RRT	Target CEP for Systematic Capability
A	A
B	B
C	C
D	D

The Target CEP for Systematic Capability is established for both the platform level and application/integration level. The application/integration level CEP is met through the application of Control Methods (refer to Section 4.3.4). The platform level is met using IEC 61508 Safety Integrity Level (SIL) certified equipment OR by establishing the adequacy of non-certified equipment. EPRI DRAM establishes the adequacy of non-certified equipment by demonstrating compliance with IEC 61508 Parts

1-3. Refer to Section 4.4.2 for information on establishing platform adequacy for the purposes of NEI 20-07.

4.3.3 Refining Loss Scenarios

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 for large LWRs) should be considered.

These Loss Scenarios may be due to Random Failures or Systematic Failures. EPRI DRAM provides the following definitions:

> *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 (SPV).*
>
> *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).*

All Loss Scenarios will be addressed by the practitioner using EPRI DRAM; however, ONLY Systematic Loss Scenarios are within the scope of NEI 20-07. The following sections contain examples of both Random and Systematic Loss Scenarios to describe the full EPRI DRAM process.

4.3.3.1 Class 1 Loss Scenarios - Inadequate Controller Behavior

Inadequate Controller Behavior applies to system controllers (including human operators). Where control actions are allocated to humans, human factors engineering processes are used to analyze the human operator’s capability to execute adequately. The focus of the process described in this document is to ensure controllers have adequately addressed systematic failures. Loss scenarios associated with random failures (including support SSCs) are considered as part of EPRI DRAM but will not be included as part of the CCF analysis. Practitioners should refer to EPRI DRAM to complete the analysis considering the following for each UCA:

- Function allocation
- Control algorithm
- Controller state
- Process model
- Controller interpretation

- Conflicting input (e.g., feedback, control actions from other controllers, other information, etc.)

EPRI DRAM provides Design Objectives that have been adapted from IEC Std. 61508-3 that should be considered during the design process to protect against inadequate control algorithms.

4.3.3.2 Class 2 Loss Scenarios - Inadequate Feedback or Information

Inadequate Feedback or Information Loss Scenarios address issues with sensors or elements where:

- Feedback or information is adequately sent but not received by the Controller.
- Feedback or information is inadequately sent to the Controller.

Loss Scenarios associated with the Controller inadequately processing feedback or information are addressed in Section 4.3.3.1, Inadequate Controller Behavior, and/or Section 4.3.3.2, Inadequate Control Algorithm Loss Scenarios. The Inadequate Feedback or Information Loss Scenarios associated with systematic failures may include:

- Feedback or information is accurately measured and correctly sent by sensor(s), but it is not received by the controller.
- Feedback or information is accurately measured by sensor(s), but it is not sent to the controller.
- Feedback or information is accurately measured and correctly sent by sensor(s), but it is inadequate upon receipt by the controller.
- Feedback or information is not received by or applied to sensor(s).
- Feedback or information is correctly received by or applied to sensor(s) but is inadequate when sent to the controller.
- Sensor(s) receive inadequate feedback or information from the controlled process
- Sensor(s) not capable or designed for necessary feedback or information.

EPRI DRAM provides potential contributing factors that should be considered when developing these types of Loss Scenarios.

4.3.3.3 Class 3 Loss Scenarios - Inadequate Control Pathway

Inadequate Control Pathway Loss Scenarios include elements (e.g., actuators) that execute Control Actions from a Controller on a Controlled Process. The Inadequate Control Pathway Loss Scenarios associated with systematic failures may include:

- Control action is sent correctly by the controller, but it is not received by actuator(s).
- Control action is correctly formulated by the controller, but it is not sent to actuator(s).

- Control action is correctly sent by the controller, but it is inadequate upon receipt at the actuator(s).

- Actuator or associated control pathway element is not designed or capable of providing the necessary response to the control action.

EPRI DRAM provides potential contributing factors that should be considered when developing these types of Loss Scenarios.

4.3.3.4 Class 4 Inadequate Process Behavior

Inadequate Process Behavior Loss Scenarios address issues during the design or operation of equipment under control that may lead to a UCA. EPRI DRAM states:

> *This methodology is not concerned with the full set of loss scenarios that could be developed for the entire spectrum of controlled process inadequacies, such as equipment aging or degradation mechanisms, or inadequate maintenance, that can lead to losses unrelated to the I&C. The focus here is on controlled process loss scenarios that can be reasonably mitigated by engineered controls allocated to the I&C equipment, or administrative controls allocated to humans that might be prompted by feedback or information provided by the I&C equipment.*
>
> *[…]The STPA Handbook [14] generally describes this type of loss scenario as one where everything else in the control structure is behaving correctly, but the controlled process behaves as if a UCA is commanded.*

The Inadequate Process Behavior Loss Scenarios associated with systematic failures may include:

- Assumptions about the Controlled Process are inadequate

- Equipment under control is not capable or designed for necessary response

EPRI DRAM provides potential contributing factors that should be considered when developing these types of Loss Scenarios.

4.3.4 Addressing Loss Scenarios

Loss Scenarios are addressed through the identification and application of Control Methods. A Control Method is a method that can be implemented to prevent, mitigate, or respond/recover from a Loss Scenario. EPRI DRAM provides methodology for addressing random Loss Scenarios (for both SIL certified and non-SIL certified equipment) and systematic Loss Scenarios; however, NEI 20-07 is limited to addressing systematic Loss Scenarios.

4.3.4.1 Identify Control Methods

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).

Control Methods use the concept of “reliability functions” to separate the effectiveness calculations described in Section 4.3.4.2. This encourages the system designer to address the overall system reliability in terms of “protect,” “detect,” and “respond and recover” to provide a more comprehensive approach. Each of these reliability functions is evaluated when identifying Control Methods.

Each identified Control Method is evaluated based on the following:

- Control Method Strength – Qualitative measure of a Control Methods ability to fulfill a reliability function.
- Control Method Type – Qualitative measure of the degree to which the implementation of a Control Method is assured.
- Control Method Configurability – Qualitative measure of the complexity of the Control Method. Higher complexity Control Methods provide less “weight” in the calculation of the Control Method Effectiveness (CME) (i.e., simple Control Methods provide higher CME scores).
- Control Method Verifiability – Qualitative measure of the degree to which a Control Method can be verified in its intended configuration throughout the system life cycle.

Each identified Control Method is evaluated against the criteria provided in the EPRI DRAM. The results are used to calculate the CME.

4.3.4.2 Score and Allocate Control Methods

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 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. As described in Section 4.3.4.1, each Control Method is evaluated to define its Control Method Strength, Control Method Type, Control Method Configurability, and Control Method Verifiability. EPRI DRAM provides weighting factors for each selection. These weighting factors are used to calculate the CME using the principles of information entropy. Refer to EPRI DRAM for details regarding the CME scoring formula and basis. Using the EPRI DRAM provided weighted values, each Control Method is scored on a scale from 0.1 to 3.0.

   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; rather, it provides a scale for qualitatively calculating the efficacy of each control method relative to the strength of other control methods. 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. The following table provides the CME thresholds aligned with required RRT.

Table 4: Target CEP Thresholds

HAZCADS RRT	Target CEP Threshold
A	CME ≥ 2.25
B	CME ≥ 1.50
C	CME ≥ 0.75
D	CME ≥ 0.10

4.3.5 Relationship Sets

Relationship Sets are groupings of system elements based on common characteristics. The goal of relationship sets is to better understand the relationship or dependencies between system elements within a design. Relationship Set types are:

- Functional – System elements that depend on each other to accomplish a specific function.
- Connectivity – System elements that provide data or control flow pathways.
- Spatial – System elements that that have a common space or location.
- Programmatic – System elements that are operated, maintained, or controlled by common administrative programs.
- Acquisition – System elements that are acquired from a common supplier.

EPRI DEG provides guidance for establishing Relationship Sets. Relationship Sets may be used to evaluate UCAs, better understand common Systematic Loss Scenarios, and establish common Control Methods to address Systematic Loss Scenarios to system elements in a Relationship Set.

4.4 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.

4.4.1 EPRI HAZCADS Clarifications

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

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

    b. 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 DI&C system reliability is bounded by the conservative results.

2. System Hazards pertinent to this regulatory application shall address nuclear safety factors appropriate for the reactor technology.

For large LWR technology, the following nuclear safety factors are used for risk-informed applications:

a. Reactor core damage as measured by ΔCDF.

b. Radioactive material release to the public as measured by ΔLERF.

Non-LWR technology, or some small-LWR technology, may have different nuclear safety factors identified and approved to risk-inform their design.

3. UCAs present in multiple redundancies of a HSSSR DI&C system AND associated with the System Hazards identified in Section 4.4.1.2 are considered potential CCFs within the scope of this process.

4.4.2 EPRI DRAM Clarifications

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

1. For the intended purpose of this Safety Case, platform adequacy may be established using the means established in EPRI DRAM. Alternatively, platform adequacy may be established by using platforms approved for use by the NRC (i.e., approved via Safety Evaluation Report). Applicants using NRC-approved platforms should ensure that application specific action items are addressed in the licensing application.
2. For the intended purpose of the Safety Case, only Systematic Loss Scenarios and their associated systematic Control Methods identified in EPRI DRAM should be within the scope of addressing CCF.
3. EPRI DRAM provides Control Method classifications of “protect, detect, and respond and recover.” These classifications bound the SRM-SECY-22-0076 terms “prevent” and “mitigate.” SRM-SECY-22-0076 also states the applicant may determine a potential CCF is not risk significant. This determination will be made in the EPRI HAZCADS RRT process.
4. Relationship sets should be created for common hardware and/or software present in multiple redundancies of the proposed DI&C system.
5. A Control Method should be established crediting system health monitoring and preventative maintenance activities that address ongoing reliability indicators for the DI&C system. These Control Methods support compliance with Regulatory Guide 1.174 requirements for ongoing monitoring.

5 SAFETY CASE DEVELOPMENT

The safety case structure provided in this section was informed by 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.

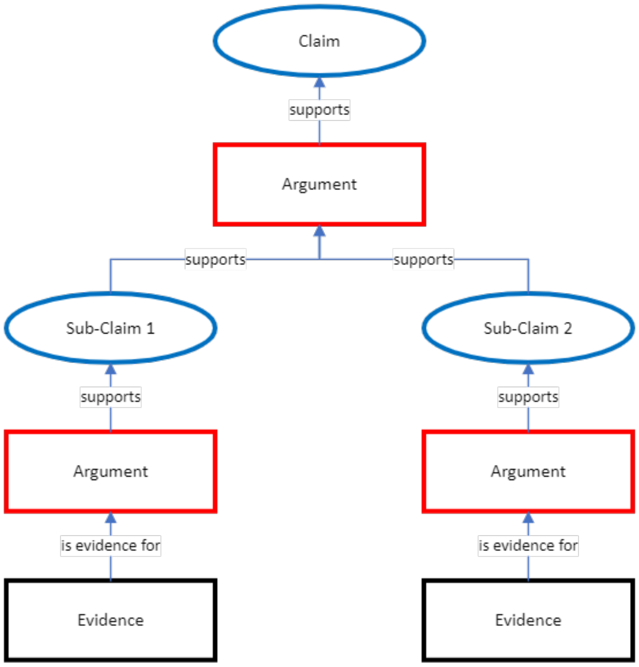


Figure 2: Safety Case Simplified Diagram

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. The safety case provided in the remainder of Section 5 focuses on the adequacy of these processes and their implementation to support this overall approach.

- *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 already require compliance with appropriate license basis standards.

5.1 Safety Case Structure

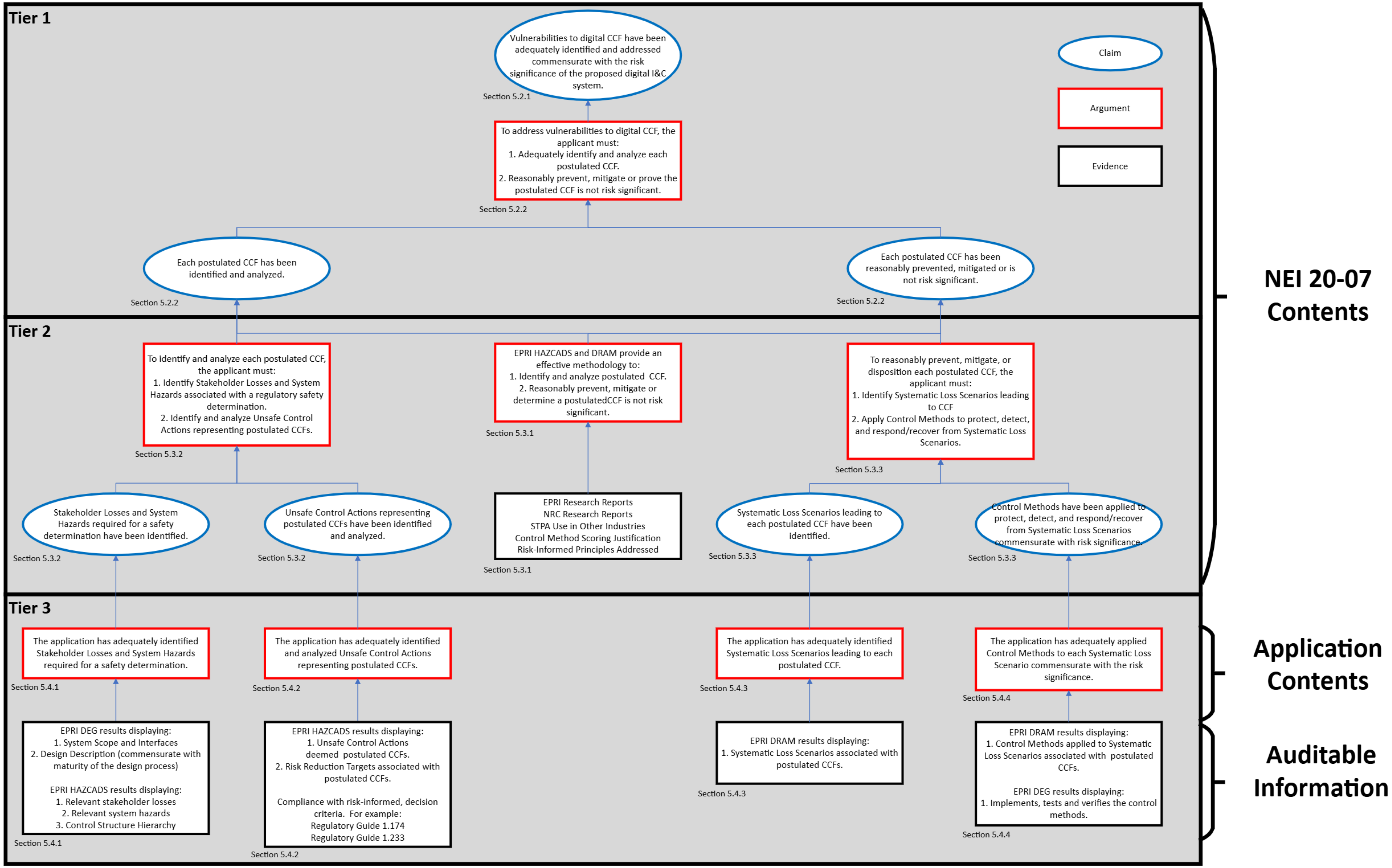
The safety case described within this document is broken into 3 tiers for descriptive purposes. The contents of this document are intended to demonstrate the overall adequacy of the proposed safety case and direct an applicant to provide the appropriate application contents demonstrating CCF has been adequately addressed.

- Tier 1 establishes the primary objective of demonstrating that potential vulnerabilities of CCF have been adequately identified. The supporting argument provides the two primary criteria that, if addressed, support the top claim. The Tier 1 Claim is consistent with SRM-SECY-22-0076 Point 1 and the two criteria in the argument are consistent with SRM-SECY-22-0076 Points 2 and 3. Refer to Section 3.1.2 for information on SRM-SECY-22-0076 Point 4.

- Tier 2 provides two sub-claims that support the Tier 1 Top Claim and argument criteria. Each sub-claim is supported by a common argument, and its associated evidence, that EPRI HAZCADS and DRAM are effective in achieving the intended result of each Tier 2 sub-claim. Furthermore, each sub-claim is supported by an argument that details the criteria by which each respective sub-claim is met. This argument establishes the required information to be provided by the applicant to demonstrate they have adequately performed the EPRI HAZCADS and DRAM processes and documents their conclusions. Tier 2 provides additional sub-claims to be resolved by each applicant using application specific information detailed in Tier 3.

- Tier 3 will be completed by each applicant using this methodology. Tier 3 will consist of the arguments, and associated evidence required to satisfy the incomplete Tier 2 sub-claims. The Tier 3 arguments will be included in the DI&C system application (either License Amendment Request or new reactor license application). The Tier 3 evidence will be available for regulatory audit/inspection and will consist of the EPRI HAZCADS and DRAM output documentation.

The completed safety case (i.e., this document AND the application specific Tier 3 information) constitutes a D3 analysis demonstrating that CCF in a HSSSR DI&C system has been adequately identified and addressed. The safety case described in this document is NOT descriptive of the actual EPRI processes which provide the technical approach. Rather, the safety case provides a set of logical claims, arguments and evidence that, if adequately performed, demonstrate that CCF has been adequately addressed.



Vulnerabilities to digital CCF have been adequately identified and addressed commensurate with the risk significance of the proposed digital I&C system.

To address vulnerabilities to digital CCF, the applicant must:
1. Adequately identify and analyze each postulated CCF.
2. Reasonably prevent, mitigate or prove the postulated CCF is not risk significant.

Each postulated CCF has been identified and analyzed.

Each postulated CCF has been reasonably prevented, mitigated or is not risk significant.

To identify and analyze each postulated CCF, the applicant must:
1. Identify Stakeholder Losses and System Hazards associated with a regulatory safety determination.
2. Identify and analyze Unsafe Control Actions representing postulated CCFs.

EPRI HAZCADS and DRAM provide an effective methodology to:
1. Identify and analyze postulated CCF.
2. Reasonably prevent, mitigate or determine a postulatedCCF is not risk significant.

To reasonably prevent, mitigate, or disposition each postulated CCF, the applicant must:
1. Identify Systematic Loss Scenarios leading to CCF
2. Apply Control Methods to protect, detect, and respond/recover from Systematic Loss Scenarios.

Stakeholder Losses and System Hazards required for a safety determination have been identified.

Unsafe Control Actions representing postulated CCFs have been identified and analyzed.

EPRI Research Reports
NRC Research Reports
STPA Use in Other Industries
Control Method Scoring Justification
Risk-Informed Principles Addressed

Systematic Loss Scenarios leading to each postulated CCF have been identified.

Control Methods have been applied to protect, detect, and respond/recover from Systematic Loss Scenarios commensurate with risk significance.

The application has adequately identified Stakeholder Losses and System Hazards required for a safety determination.

The application has adequately identified and analyzed Unsafe Control Actions representing postulated CCFs.

The application has adequately identified Systematic Loss Scenarios leading to each postulated CCF.

The application has adequately applied Control Methods to each Systematic Loss Scenario commensurate with the risk significance.

EPRI DEG results displaying:
1. System Scope and Interfaces
2. Design Description (commensurate with maturity of the design process)

EPRI HAZCADS results displaying:
1. Relevant stakeholder losses
2. Relevant system hazards
3. Control Structure Hierarchy

EPRI HAZCADS results displaying:
1. Unsafe Control Actions deemed postulated CCFs.
2. Risk Reduction Targets associated with postulated CCFs.

Compliance with risk-informed, decision criteria. For example:
Regulatory Guide 1.174
Regulatory Guide 1.233

EPRI DRAM results displaying:
1. Systematic Loss Scenarios associated with postulated CCFs.

EPRI DRAM results displaying:
1. Control Methods applied to Systematic Loss Scenarios associated with postulated CCFs.

EPRI DEG results displaying:
1. Implements, tests and verifies the control methods.

Figure 3: Digital CCF Safety Case

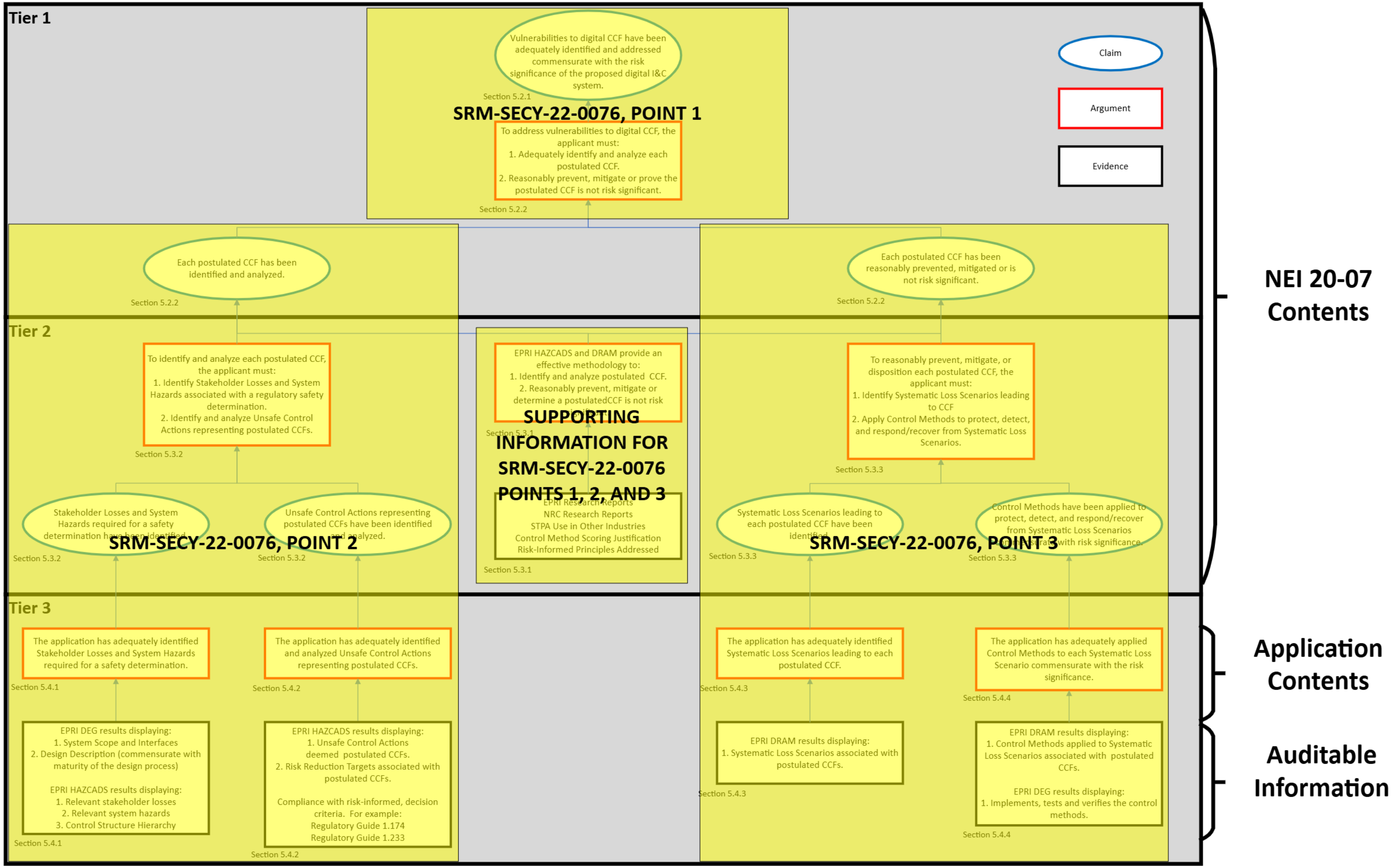

Tier 1
Vulnerabilities to digital CCF have been adequately identified and addressed commensurate with the risk significance of the proposed digital I&C system.
Section 5.2.1
SRM-SECY-22-0076, POINT 1
To address vulnerabilities to digital CCF, the applicant must:
1. Adequately identify and analyze each postulated CCF.
2. Reasonably prevent, mitigate or prove the postulated CCF is not risk significant.
Section 5.2.2
Claim
Argument
Evidence
Each postulated CCF has been identified and analyzed.
Section 5.2.2
Each postulated CCF has been reasonably prevented, mitigated or is not risk significant.
Section 5.2.2
Tier 2
To identify and analyze each postulated CCF, the applicant must:
1. Identify Stakeholder Losses and System Hazards associated with a regulatory safety determination.
2. Identify and analyze Unsafe Control Actions representing postulated CCFs.
Section 5.3.2
EPRI HAZCADS and DRAM provide an effective methodology to:
1. Identify and analyze postulated CCF.
2. Reasonably prevent, mitigate or determine a postulatedCCF is not risk significant.
Section 5.3.1
SUPPORTING INFORMATION FOR SRM-SECY-22-0076 POINTS 1, 2, AND 3
EPRI Research Reports
NRC Research Reports
STPA Use in Other Industries
Control Method Scoring Justification
Risk-Informed Principles Addressed
Section 5.3.1
To reasonably prevent, mitigate, or disposition each postulated CCF, the applicant must:
1. Identify Systematic Loss Scenarios leading to CCF
2. Apply Control Methods to protect, detect, and respond/recover from Systematic Loss Scenarios.
Section 5.3.3
Stakeholder Losses and System Hazards required for a safety determination have been identified.
Section 5.3.2
Unsafe Control Actions representing postulated CCFs have been identified and analyzed.
Section 5.3.2
SRM-SECY-22-0076, POINT 2
Systematic Loss Scenarios leading to each postulated CCF have been identified.
Section 5.3.3
Control Methods have been applied to protect, detect, and respond/recover from Systematic Loss Scenarios commensurate with risk significance.
Section 5.3.3
SRM-SECY-22-0076, POINT 3
Tier 3
The application has adequately identified Stakeholder Losses and System Hazards required for a safety determination.
Section 5.4.1
The application has adequately identified and analyzed Unsafe Control Actions representing postulated CCFs.
Section 5.4.2
The application has adequately identified Systematic Loss Scenarios leading to each postulated CCF.
Section 5.4.3
The application has adequately applied Control Methods to each Systematic Loss Scenario commensurate with the risk significance.
Section 5.4.4
EPRI DEG results displaying:
1. System Scope and Interfaces
2. Design Description (commensurate with maturity of the design process)
EPRI HAZCADS results displaying:
1. Relevant stakeholder losses
2. Relevant system hazards
3. Control Structure Hierarchy
Section 5.4.1
EPRI HAZCADS results displaying:
1. Unsafe Control Actions deemed postulated CCFs.
2. Risk Reduction Targets associated with postulated CCFs.
Compliance with risk-informed, decision criteria. For example:
Regulatory Guide 1.174
Regulatory Guide 1.233
Section 5.4.2
EPRI DRAM results displaying:
1. Systematic Loss Scenarios associated with postulated CCFs.
Section 5.4.3
EPRI DRAM results displaying:
1. Control Methods applied to Systematic Loss Scenarios associated with postulated CCFs.
EPRI DEG results displaying:
1. Implements, tests and verifies the control methods.
Section 5.4.4
NEI 20-07 Contents
Application Contents
Auditable Information

Figure 4: Digital CCF Safety Case Alignment to SRM-SECY-22-0076

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 defense-in-depth and diversity analysis that demonstrates vulnerabilities to digital CCF have been adequately identified and addressed. To prove that vulnerabilities to CCF have been adequately addressed, a diversity and defense-in-depth analysis must be able to demonstrate that:

1. Postulated CCFs have been identified and analyzed.

   The safety case establishes that the applicant has adequately identified Stakeholder Losses, System Hazards and UCAs, and assigned the RRTs. The combination of these activities produces a bounding set of potential CCFs associated with the system design and analyzes the risk impact of these CCFs on the nuclear power plant. As noted in Section 4.2.1, UCAs present in multiple redundancies of a HSSSR DI&C system are considered potential CCFs. The CCFs within the scope of the license application are those that are traceable to System Hazards associated with approved risk metrics (e.g., CDF and LERF for large LWR). The risk impact of each CCF is analyzed via the risk sensitivity analysis performed via EPRI HAZCADS.

2. Each postulated CCF has been reasonably prevented, mitigated, or adequately dispositioned.

   The safety case also establishes that for each postulated CCF to be reasonably prevented, mitigated, or dispositioned, the applicant must: 1. Identify Systematic Loss Scenarios leading to a CCF; and 2. Apply Control Methods to protect, detect, and respond/recover from Systematic Loss Scenarios.

5.1.2 Safety Case Uncertainty

With the use of any tool, an argument can be presented that the resulting analysis is incomplete. In this case, a source of uncertainty can be presented that an applicant did not identify ALL potential CCF. EPRI HAZCADS and DRAM provide a cross-functional, iterative approach that uses input from plant staff such as Design Engineering, Strategic/Systems Engineering, Maintenance, Operations, and PRA. Additionally, this diagnostic process is used iteratively throughout the design phases to continually drive a more granular analysis. By starting at high levels of abstraction during initial design phases, the Stakeholder Losses, System Hazards, Unsafe Control Actions and Risk Reduction Targets are conservative and bounding. As the design matures, the HAZCADS and DRAM results become more granular. The result is a many-to-one relationship between Control Methods and Loss Scenarios commensurate with risk. Each Control Method is justified through its effectiveness score.

A traditional nuclear transient and accident analysis is developed upon the principle that licensing basis events do not represent all events that may occur at a nuclear power plant; however, the events identified are the most credible and bounding events. EPRI HAZCADS and DRAM apply the same concept.

5.2 Tier 1 Claim, Argument and Sub-Claims

5.2.1 Tier 1 Top Claim

Tier 1 establishes the top claim and supporting argument.

TIER 1, TOP CLAIM: VULNERABILITIES TO DIGITAL CCF HAVE BEEN ADEQUATELY IDENTIFIED AND ADDRESSED COMMENSURATE WITH THE RISK SIGNIFICANCE OF THE PROPOSED DIGITAL I&C SYSTEM.

This top claim is intended to address SRM-SECY-22-0076 Point 1 which 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 defense-in-depth and diversity assessment must be commensurate with the risk significance of the proposed digital I&C system.*

The EPRI HAZCADS and DRAM processes used to develop this safety case are diagnostic tools that assess the defense in depth and diversity of the facility using hazards and reliability analysis techniques. In doing so, the processes identify vulnerabilities to digital CCF and address them using Control Methods. Additionally, the risk significance of the HSSSR DI&C system (or portions thereof) is identified. The Control Methods used to address the vulnerabilities to digital CCF are applied commensurate with their associated risk significance. This point establishes the Tier 1 argument.

5.2.2 Tier 1 Argument and Sub-Claims

The SRM-SECY-22-0076 policy establishes the key criteria that must be demonstrated to prove that vulnerabilities to digital CCF have been adequately addressed. This safety case is directly aligned to address SRM-SECY-22-0076 Points 1-3. As previously stated, the top claim is intended to be consistent with SRM-SECY-22-0076 Point 1. SRM-SECY-22-0076 provides the elements that must be analyzed to demonstrate that vulnerabilities to digital CCF have been addressed. As such, the Tier 1 argument is intended to be consistent with SRM-SECY-22-0076 Points 2 and 3.

TIER 1, ARGUMENT 1: TO ADDRESS VULNERABILITIES TO DIGITAL CCF, THE APPLICANT MUST:

1. ADEQUATELY IDENTIFY AND ANALYZE EACH POSTULATED CCF.
2. REASONABLY PREVENT, MITIGATE OR PROVE THE POSTULATED CCF IS NOT RISK SIGNIFICANT.

The first element of this argument states that the applicant must adequately identify and analyze each postulated CCF which is consistent with SRM-SECY-22-0076 Point 2:

> 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.[…]*

The second element of this argument states that the applicant must reasonably prevent, mitigate or prove the postulated CCF is not risk significant. This language directly mirrors the language is SRM-SECY-22-0076 Point 3 which states:

> 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.[…]*

As a point of comparison, NUREG-6303 provides similar guidance for determining if vulnerabilities to CCF have been adequately addressed. Guidelines 1-3 provide information on establishing a block structure, diversity types, and types of failures to consider. Guidelines 4-9 provide analysis guidance for identifying and analyzing potential vulnerabilities to CCF; Guidelines 10-14 provide analysis guidance for addressing potential vulnerabilities to CCF using diversity (including manual operator action). These two primary activities (i.e., Identify and address) are consistent with the two elements of this argument which use the terms "identify and analyze" and "prevent, mitigate, and or prove the CCF is not risk significant."

Each element of the Tier 1 Argument is used to establish sub-claims to be addressed:

TIER 1, SUB-CLAIM 1: EACH POSTULATED CCF HAS BEEN IDENTIFIED AND ANALYZED.
TIER 1, SUB-CLAIM 2: EACH POSTULATED CCF HAS BEEN REASONABLY PREVENTED, MITIGATED OR IS NOT RISK SIGNIFICANT.

If an applicant can adequately demonstrate that EACH of these sub-claims is satisfied, then the Top Claim that vulnerabilities to CCF have been adequately addressed is satisfied. Tier 2 provides arguments, additional sub-claims, and evidence that are intended to resolve each of these sub-claims by proving that the processes used are adequate and the applicant has adequately used those processes to achieve the intended outcomes.

5.3 Tier 2 Arguments, Evidence and Sub-Claims

Tier 2 is used to describe three arguments needed to resolve the Tier 1 sub-claims that connect the portions of the EPRI processes to the SRM-SECY-22-0076 policy point they are used to meet. The first argument is used to support both Tier 1 sub-claims and summarizes evidence that the EPRI HAZCADS and DRAM processes are effective at identifying and addressing CCF. The remaining arguments provide the criteria required to adequately resolve the Tier 1 sub-claims.

5.3.1 Tier 2, Argument 1: EPRI HAZCADS and DRAM Efficacy

TIER 2, ARGUMENT 1: EPRI HAZCADS AND DRAM PROVIDE AN EFFECTIVE METHODOLOGY TO:

- IDENTIFY AND ANALYZE POSTULATED CCF.
- REASONABLY PREVENT, MITIGATE, OR DETERMINE A POSTULATED CCF IS NOT RISK SIGNIFICANT.

For either Tier 2 sub-claim to be adequately resolved, credible processes must be used to develop the evidence and arguments. EPRI HAZCADS is comprised of Systems Theoretic Process Analysis and Fault Tree Analysis. EPRI DRAM completes the STPA process and uses Control Method Scoring/Allocation. These underlying processes are integrated to create the EPRI HAZCADS and DRAM processes as described in Section 4. Additionally, these processes are embedded within a system engineering process, EPRI Digital Engineering Guideline, to develop and maintain highly reliable DI&C systems. Section 5.3.1.1 provides a description of the EPRI research that supported the creation of EPRI HAZCADS and DRAM and provides additional references documenting EPRI research. As of the issuance of this document, there have been no applications using the EPRI HAZCADS or DRAM processes. Therefore, the efficacy of the underlying processes should be used to demonstrate their integrated effectiveness.

EPRI HAZCADS is used to identify and analyze postulated CCF. STPA and FTA are used as the underlying processes for EPRI HAZCADS. STPA has been used extensively in other safety critical industries such as defense, aviation, automotive and process industries to identify random and systematic failures. Refer to Section 5.3.1.3 for more information and additional references for STPA use. Additionally, the NRC accepted the NuScale hazards analysis which used STPA to analyze potential hazards as described in the NuScale FSAR and FSER. EPRI research evaluated the effectiveness of hazards analysis techniques and determined STPA and FTA are complementary processes that effectively identify hazards (including systematic failures such as CCF) and their impact to plant risk (Refer to Section 5.3.1.1 and associated references).

EPRI DRAM is used to reasonably prevent or mitigate postulated CCF. DRAM addresses both random and systematic failures at the platform and application/integration layers. The control method scoring process was developed by Sandia National Labs in support of the EPRI Technical Assessment Methodology (TAM) and adapted for the EPRI DRAM process. EPRI TAM is a downstream process of the EPRI DEG and HAZCADS that addresses hazards associated with Cyber Security. EPRI TAM identifies Exploit Sequences similar to EPRI DRAM Loss Scenarios and identifies, scores, and allocates Control Methods. Vogtle 3&4 used EPRI TAM as the basis for their cyber security assessments. The associated Cyber Security Plan was accepted by the NRC and subsequent inspections did not identify any violations associated with the Vogtle 3&4 inspection. The EPRI TAM control method scoring methodology uses the same approach using information theory (or information entropy) to create relative scoring to compare the efficacy of potential control methods (or potential combined control methods). The control method characteristics used by EPRI TAM and EPRI DRAM are different as the critical attributes for cyber security are different than those used to evaluate digital system reliability. Section 5.1.3.4 provides additional information regarding Control Methods.

Lastly, SRM-SECY-22-0076 requires that risk-informed approaches to addressing digital CCF must be consistent with current risk-informed guidance. NEI 20-07 is consistent with the risk-informed principles described in Regulatory Guide 1.174 and can be used in conjunction with the risk-informed licensing approach described in Regulatory Guide 1.233. Refer to Section 5.3.1.5 for more information.

5.3.1.1 Supporting Evidence: EPRI Research

The foundational processes described in EPRI HAZCADS and DRAM (e.g., STPA, FTA, etc.) have been proven effective in identifying and addressing hazards and sources of failure in DI&C systems including systematic failures such as digital CCF. 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

5.3.1.2 Supporting Evidence: 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

5.3.1.3 Supporting Evidence: 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 5: 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

5.3.1.4 Supporting Evidence: 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.

5.3.1.5 Supporting Evidence: 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 provide guidance for risk-informed applications. 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 to address vulnerabilities to CCF 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 do 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.

For large LWR, 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.

For other reactor technologies, approved risk metrics should be established to use risk-informed approaches. Additionally, "regions" similar to RG 1.174 Figures 4 and 5 should be established to be consistent with the graded approach described within this document.

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 into potential sources of failure and provides insights into the most risk-significant CCF vulnerabilities that need to be addressed. Control Methods applied to address these CCF 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 CCF 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 CCFs.

5.3.2 Tier 2, Argument 2: Postulated CCF Identification/Analysis

Tier 2, Argument 2, establishes which portions of EPRI DEG and HAZCADS are used to identify and analyze postulated CCF.

TIER 2, ARGUMENT 2: TO IDENTIFY AND ANALYZE EACH POSTULATED CCF, THE APPLICANT MUST:

1. IDENTIFY STAKEHOLDER LOSSES AND SYSTEM HAZARDS ASSOCIATED WITH A REGULATORY SAFETY DETERMINATION.
2. IDENTIFY AND ANALYZE UNSAFE CONTROL ACTIONS REPRESENTING POSTULATED CCFS.

This portion of the safety case is intended to address SRM-SECY-22-0076 Point 2 which requires each postulated CCF to be analyzed using best estimate or risk-informed methods. This argument establishes the elements of the technical process described in Section 4 to demonstrate that potential vulnerabilities to CCF have been identified and analyzed. Two elements are essential to meeting the claim that potential vulnerabilities to CCF have been identified and analyzed. EPRI HAZCADS uses the STPA and FTA processes to achieve these goals.

A D3 analysis using NUREG-6303 identifies the impacts of each postulated CCF concurrent with accidents analyzed in the plant accident analysis. This methodology is consistent with NRC risk-informed decision-making guidance (e.g., Regulatory Guide 1.174 or Regulatory Guide 1.233) which determines the risk impacts of each postulated CCF via a PRA model. For the purposes of this document, potential vulnerabilities to CCF must be identified in terminology consistent with EPRI DEG, HAZCADS and DRAM. Within the scope of this process, potential vulnerabilities to CCF are equivalent to UCAs that are present in multiple redundancies of a HSSSR DI&C system and contribute to System Hazards and Stakeholder Losses associated with a regulatory safety determination. Regardless of their causal factors or how likely they are, UCAs identify impacts to System Hazards and Stakeholder Losses due to a Control Action executed improperly.

EPRI HAZCADS identifies Stakeholder Losses associated with the appropriate regulatory safety factors (dependent on reactor technology) and identifies System Hazards that may result in those Stakeholder Losses. Only losses and plant/System Hazards associated with a regulatory safety determination should be considered within the scope of addressing digital CCF. Other Stakeholder Losses (e.g., financial loss or reputational loss) and their associated System Hazards will be addressed by the practitioners; however, they are not relevant to a regulatory decision. The Control Structure Hierarchy is developed to represent the control system and its relationships with each element within the hierarchy including sensors, control devices, feedback loops, control actions, control algorithms, controllers, and human controllers. Through this process, a bounded set of Control Actions is developed based on the interrelationships between humans (e.g., Operations), controls system (e.g., safety system platform), and controlled processes (e.g., actuators and plant response).

Relationship Sets may offer insights that aid the practitioner in identifying postulated CCFs. Relationship sets can be used to group SSCs by their spatial relationships, network dependencies, or other common dependencies. See Reference 15 for more information on relationship sets.

The process of developing Unsafe Control Actions identifies possible ways each Control Action could fail that may result in the System Hazard. This structured approach is effective at identifying the effects of spurious operations, halted operation of the control system, sequencing errors, and many other forms of UCAs. The likelihood of any given UCA is not considered during their identification. All identified UCAs are considered throughout the analysis. The results of the risk sensitivity analysis may be applied to all UCAs associated with a given System Hazard, or to individual UCAs for more granularity based on the chosen pathway described in Section 4.2.1. Through these processes a set of postulated CCFs is identified and the risk significance is analyzed either at a system level (more conservative) or UCA level (more granular).

Once the potential vulnerabilities to CCF are identified, they must be analyzed. SRM-SECY-22-0076 Point 2 allows for risk-informed approaches to analyze the potential vulnerabilities to CCF. EPRI HAZCADS uses Fault Tree Analysis to determine the impact on the appropriate risk metrics. Refer to Section 4.2.1 for a description of the RRT development process. RRTs are allocated to UCAs and the associated DI&C system elements. This analysis provides the applicant risk insights into the impact of potential vulnerabilities to CCF.

TIER 2, SUB-CLAIM 1: STAKEHOLDER LOSSES AND SYSTEM HAZARDS REQUIRED FOR A SAFETY DETERMINATION HAVE BEEN IDENTIFIED.

TIER 2, SUB-CLAIM 2: UNSAFE CONTROL ACTIONS REPRESENTING POSTULATED CCFS HAVE BEEN IDENTIFIED AND ANALYZED.

Two (2) Tier 2 sub-claims are established to connect the application specific arguments and evidence to the safety case established within this document. It is the applicant's responsibility within Tier 3 to provide the arguments and evidence specific to the application to resolve these Tier 2 sub-claims. Section 5.4 provides additional information regarding Tier 3 information.

5.3.3 Tier 2, Argument 3: Addressing Postulated CCF

The last Tier 2 argument establishes that these processes have been effectively used to address each postulated CCF.

TIER 2, ARGUMENT 3: TO REASONABLY PREVENT, MITIGATE, OR DISPOSITION EACH POSTULATED CCF, THE APPLICANT MUST:

1. IDENTIFY SYSTEMATIC LOSS SCENARIOS LEADING TO CCF.
2. APPLY CONTROL METHODS TO PROTECT, DETECT, AND RESPOND/RECOVER FROM SYSTEMATIC LOSS SCENARIOS.

This portion of the safety case is intended to address SRM-SECY-22-0076 Point 3 which requires each potential vulnerability to CCF to be reasonably prevented, mitigated or determined not risk significant.

> *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.*

For risk-informed approaches, this policy point describes the following criteria for addressing postulated CCF.

1. Demonstrate the adequacy techniques and/or measures credited to prevent or mitigate each postulated CCF.

2. Justify the adequacy commensurate with the risk significance of each postulated CCF.

3. Apply diverse means to any risk significant postulated CCF if other techniques or measures cannot be adequately justified.

EPRI DRAM performs these functions by identifying Loss Scenarios (refer to Section 4.3.3) and applying Control Method (refer to Section 4.3.4). Loss Scenarios are used to identify potential errors that may lead to a postulated CCF. Loss Scenario identification is a diagnostic process which results in new, or revised, system requirements, changes to the system design, and/or the application of Control Methods. Control Methods may be design techniques, prevention measures, or mitigation measures. These Control Methods are scored and combined to demonstrate their cumulative adequacy in preventing or mitigating each Loss Scenario commensurate with its RRT (i.e., risk significance). Each Loss Scenario is addressed independently which results in a comprehensive method for addressing each UCA. As previously described, postulated CCFs are equivalent to UCAs in for EPRI HAZCADS/DRAM. Figure 5 demonstrates this “many-to-one” concept to address postulated CCF in which one UCA is addressed through the identification of many Loss Scenarios and many Control Methods.

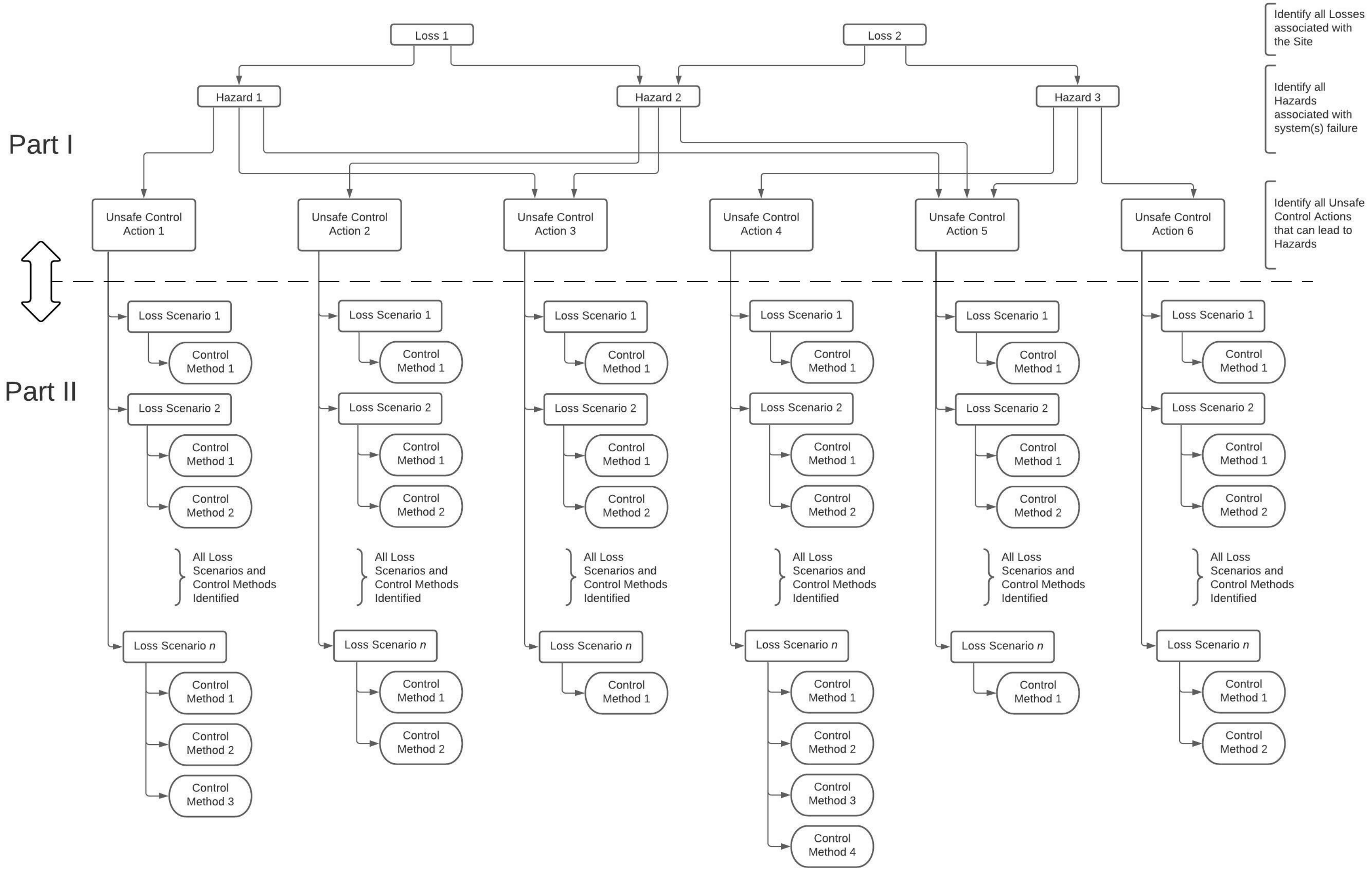


Figure 5: EPRI HAZCADS and DRAM Conceptual Implementation

A Tier 2 sub-claim is established within this portion of the safety case as follows:

TIER 2, SUB-CLAIM 3: SYSTEMATIC LOSS SCENARIOS LEADING TO EACH POSTULATED CCF HAVE BEEN IDENTIFIED.

Furthermore, SRM-SECY-22-0076 Point 3 uses the terms "design techniques, prevention measures, or mitigation measures, other than diversity, that are credited in the assessment." EPRI DRAM uses a single term "Control Methods" that bounds the SRM-SECY-22-0076 terms. SRM-SECY-22-0076 also uses the terms "prevent" and "mitigate" while EPRI DRAM uses the terms "protect," "detect," and "respond and recover." EPRI DRAM provides the following definitions:

> *Protect – the control method provides a means of preventing a loss scenario from becoming one or more of the UCAs and related losses determined by HAZCADS.*
>
> *Detect – the control method provides a means of detecting a loss scenario.*
>
> *Respond and Recover – the control method provides a means of responding and recovering from a loss scenario when it is detected.*

Based upon these definitions, the EPRI term "protect" bounds the NRC term "prevent," and the EPRI terms "detect" and "respond and recover" bounds the NRC term "mitigate." The NRC also states that a CCF can be determined to be "not risk significant." The process of determining a CCF is "not risk significant" occurs during the development of RRTs in HAZCADS.

Control methods are evaluated on their ability to protect, detect, and respond and recover from EACH systematic Loss Scenario that may lead to a UCA considered a postulated CCF. Control methods are applied commensurate with their RRT (or risk significance category). A systematic Loss Scenario associated with a high RRT (RRT A) requires highly effective Control Methods that demonstrate the ability to protect, detect, and respond and recover. A systematic Loss Scenario associated with a low RRT (RRT D) requires less effective (or fewer) Control Methods, but still must demonstrate the ability to protect, detect, and respond and recover.

As a result, each systematic Loss Scenario associated with the UCA considered a postulated CCF is individually addressed by Control Methods commensurate with the UCA's risk. These Control Methods are scored based upon their effectiveness using attributes defined in EPRI DRAM. These attributes may include Control Method type (e.g., technical, procedural, etc.), strength, configurability, and/or verifiability. Control method attributes are qualitatively "scored" and produce a Control Method Effectiveness. Control Methods can be combined; however, the Control Method Effectiveness scores are not purely additive. Instead, the combined CME scoring uses a geometric weighting preventing the practitioner from "stacking" less effective Control Methods. This scoring methodology provides the technical justification of the adequacy of the applied Control Method(s) commensurate with their risk.

A Tier 2 sub-claim is established within this portion of the safety case as follows:

TIER 2, SUB-CLAIM 4: CONTROL METHODS HAVE BEEN APPLIED TO PROTECT, DETECT, AND RESPOND/RECOVER FROM SYSTEMATIC LOSS SCENARIOS COMMENSURATE WITH RISK SIGNIFICANCE.

Both Tier 2 sub-claims associated with this argument are left un-resolved by NEI 20-07. It is the applicant's responsibility within Tier 3 to provide the arguments and evidence specific to the application to resolve these sub-claims. Section 5.4 provides additional information regarding Tier 3 information.

5.4 Tier 3 Arguments and Evidence

Tier 3 of the safety case provides arguments and evidence completed by each applicant to complete all open Tier 2 arguments with application specific information. Each of the Tier 2 sub-claims described in Section 5.3 are intended to be addressed by the applicant via the arguments described in this section. The four Tier 2 subclaims discussed in Section 5.3 are:

- Tier 2, Sub-Claim 1: Stakeholder losses and System Hazards required for a safety determination have been identified.
- Tier 2, Sub-Claim 2: Unsafe Control Actions representing postulated CCFs have been identified and analyzed.
- Tier 2, Sub-Claim 3: Systematic Loss Scenarios leading to each postulated CCF have been identified.
- Tier 2, Sub-Claim 4: Control Methods have been applied to protect, detect, and respond/recover from Systematic Loss Scenarios commensurate with RRT.

Tier 3 provides direction for applicants to construct meaningful arguments and required criteria for evidence to support the resolution of these sub-claims. The applicants' arguments described in this section should be used to construct a D3 (CCF coping) analysis and provided as part of the application associated with the proposed DI&C system (e.g., License Amendment Request, new plant application, etc.). The applicant's evidence associated with each argument in the D3 analysis will be made available for audit/inspection.

5.4.1 Resolution of Tier 2, Sub-Claim 1

To resolve Tier 2, Sub-Claim 1, the applicant should provide an argument that the application has adequately identified Stakeholder Losses and System Hazards required for a safety determination. In doing so, the application should describe relevant information and conclusions identified in EPRI DEG and EPRI HAZCADS outputs.

TIER 3, ARGUMENT 1: THE APPLICATION HAS ADEQUATELY IDENTIFIED STAKEHOLDER LOSSES AND SYSTEM HAZARDS REQUIRED FOR A SAFETY DETERMINATION.

The elements of this argument should provide the overall context of the DI&C system, impact to other plant systems, Stakeholder Losses, and System Hazards. As a result, the applicant may conclude that the identified Stakeholder Losses and System Hazards associated with a safety determination have been adequately identified.

The applicant should summarize, and provide references to, the complete engineering analysis documenting each of the criteria described below. This summary should be part of the application, and the references should be made available for regulatory audit.

Acceptance Criteria

1. The application should provide, or reference a docketed submittal providing, a system description consistent with DI&C-ISG-06, NUREG-0800 Chapter 7, Digital I&C Design Review Guide (DRG), or equivalent.

2. The application should describe the adequacy of the selected platform technology. IEC 61508 SIL certified platforms commensurate with the target Systematic Capability or NRC approved platforms may be used to demonstrate platform-level CCF has been adequately addressed.

3. The application should provide, or reference a docketed submittal providing, a description of the DI&C design consistent with DI&C-ISG-06, NUREG-0800 Chapter 7, Digital I&C Design Review Guide (DRG), or equivalent. The summary for Tier 3 Argument 1 should describe the EPRI HAZCADS Control Structure hierarchy used as the basis for analysis.

4. The application should include a summary description of Stakeholder Losses identified during the execution of EPRI HAZCADS associated with nuclear safety.

    a. Examples of Stakeholder Losses associated with nuclear safety for a Light Water Reactor are core damage and radiological release. For non-LWR plants, other factors may be considered.

    b. The applicant should provide justification for the completeness and thoroughness of the Stakeholder Losses included.

5. The application should include a summary description of System Hazards identified during the execution of EPRI HAZCADs that may result in the Stakeholder Losses associated with nuclear safety.

    a. The description should provide sufficient information to describe the system's state and its impact on the identified Stakeholder Losses.

    b. The system's state should be consistent with the design basis of the plant and/or best-estimate methodology.

    c. The applicant should provide justification for the completeness and thoroughness of the System Hazards included.

5.4.2 Resolution of Tier 2, Sub-Claim 2

To resolve Tier 2, Sub-Claim 2, the applicant should provide an argument that the application has adequately identified and analyzed UCAs representing postulated CCFs. In doing so, the application should describe relevant information and conclusions identified in EPRI HAZCADS outputs.

TIER 3, ARGUMENT 2: THE APPLICATION HAS ADEQUATELY IDENTIFIED AND ANALYZED UNSAFE CONTROL ACTIONS REPRESENTING POSTULATED CCFS.

The elements of this argument should provide a representation of the DI&C system that provides sufficient information to determine relevant UCAs and their associated RRTs. Additionally, the applicant should provide information associated with the quality and scope of the PRA model, as well as any design features external to the DI&C system that may be credited such as manual operator actions and passive design features. As a result, the applicant may conclude that the postulated CCFs have been adequately identified and analyzed.

The applicant should summarize and provide references to the complete engineering analysis documenting each of the criteria described below. These references should be made available for regulatory audit. The summary should also describe how the criteria stated in Section 5.3.2 have been met.

Acceptance Criteria

1. The application should describe UCAs deemed postulated CCFs associated with the Control Structure Hierarchy described in Section 5.3.2.

   a. The application should describe the criteria used to determine whether the UCAs are CCFs (e.g., identical software, common dependencies, identical equipment, etc.) and justification for their selection of CCFs.

   b. The application should also demonstrate the thoroughness of the evaluation.

   c. UCAs that identify adverse impacts of spurious operations should be highlighted.

2. The application should describe the Risk Reduction Targets associated with the UCAs deemed postulated CCFs.

   a. The application should describe EPRI HAZCADS pathway and provide justification for it’s use.

3. The application should demonstrate compliance with the appropriate risk-informed, decision-making framework (e.g., Regulatory Guide 1.174, Regulatory Guide 1.233, etc.). Examples of PRA information include:

   a. Identify the base PRA and its technical acceptability (compliance to PRA standard and reflects the plant or design at the time of the application).

   b. If PRA hazards or operating modes are excluded from the assessment, justify the appropriateness of the exclusions.

   c. Justify surrogate events bounding the impact of the CCF on plant equipment, functions, and operator actions modeled in the PRA.

d. Justify if the impact of the CCF is deemed not risk significant.

e. Identify and disposition key assumptions and sources of uncertainty in accordance with appropriate PRA guidance (e.g., Regulatory Guide 1.200 for LWRs).

5.4.3 Resolution of Tier 2, Sub-Claim 3

To resolve Tier 2, Sub-Claim 3, the applicant should provide an argument that the application has adequately identified Systematic Loss Scenarios leading to a postulated CCF (i.e., UCAs that have been identified as CCF vulnerabilities in Section 5.4.2). In doing so, the application should describe relevant information and conclusions identified in EPRI DEG, EPRI HAZCADS, and EPRI DRAM outputs.

TIER 3, ARGUMENT 3: THE APPLICATION HAS ADEQUATELY IDENTIFIED SYSTEMATIC LOSS SCENARIOS LEADING TO EACH POSTULATED CCF.

The elements of this argument should describe the relationships between postulated CCFs (e.g., common equipment, common location) that will provide further insights into the design and aid in the resolution of systematic Loss Scenarios. This argument should also describe the systematic Loss Scenarios associated with each postulated CCF. The objective is to demonstrate that the analysis has identified postulated CCF sources and thus be able to conclude that the Systematic Loss Scenarios for each postulated CCF have been adequately identified.

Acceptance Criteria

1. The application should describe Systematic Loss Scenarios associated with each postulated CCF.

   a. For each postulated CCF (as identified by a UCA or UCA Set), the applicant should:

      i. Describe the Systematic Loss Scenarios identified.

      ii. Provide references to evidence documenting the results of the EPRI DRAM process.

      iii. Describe the thoroughness of the evaluation.

   b. Random Loss Scenarios are not applicable to this evaluation.

5.4.4 Resolution of Tier 2, Sub-Claim 4

To resolve Tier 2, Sub-Claim 4, the applicant should provide an argument that the application has adequately applied Control Methods to each Systematic Loss Scenarios commensurate with the risk significance. In doing so, the application should describe relevant information and conclusions identified in EPRI HAZCADS and EPRI DRAM outputs.

TIER 3, ARGUMENT 4: THE APPLICATION HAS ADEQUATELY APPLIED CONTROL METHODS TO EACH SYSTEMATIC LOSS SCENARIO COMMENSURATE WITH THE RISK SIGNIFICANCE.

The elements of this argument should describe the Control Methods applied to each Systematic Loss Scenario. This description should provide enough detail and justification to demonstrate that the Control Methods are allocated commensurate with their RRT, concluding that Control Methods are applied adequately to each Systematic Loss Scenario.

Acceptance Criteria

1. The application should describe the Control Methods applied to each Systematic Loss Scenario associated with postulated CCFs.
    a. The description should include the Types of Reliability Functions (i.e., Protect, Detect, and Respond and Recover) and Control Method Types.
2. The application should justify how the applied Control Methods have adequately addressed the Systematic Loss Scenarios associated with postulated CCFs.
    a. The application should demonstrate the Control Method Effectiveness (or Combined Control Method Effectiveness) meets the Risk Reduction Target (RRT).
    b. If the application deviates from the EPRI DRAM scoring methodology (e.g., recommended weighting values, RRT thresholds, scoring variables, etc.), the application should provide justification for the deviation.
3. The application should justify how the cumulative effect of all applied Control Methods has adequately addressed each postulated CCF.
4. The application should demonstrate how Control Methods will be implemented in the design (e.g., incorporation into requirements, demonstrated in design documents, or included in testing plans).

The applicant should provide references to the evidence documenting each of the criteria described in this section. The output documents associated with these processes should be made available for regulatory audit.

6 CONCLUSION

Using DI&C system design information provided from EPRI DEG output documents, the EPRI HAZCADS process is effective at identifying Stakeholder Losses, System Hazards, UCAs that can lead to a postulated CCF, and RRTs to assess CCF risk significance. UCAs that are present in multiple redundancies of a DI&C system and impact plant risk metrics (e.g., CDF and/or LERF for large LWR technology) are considered CCFs. 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 (i.e., Loss Scenario) commensurate with the risk significance identified.

The safety case provided within this document presents a clear, logical approach for the applicant to demonstrate that vulnerabilities to CCF have been adequately addressed in HSSSR 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. SAMPLE TEMPLATE

This Appendix describes a sample template for a submittal using NEI 20-07. The submittal could be in support of a new reactor application using any licensing framework (10 CFR 50, 10 CFR 52, etc.) or license amendment request.

A.1. Purpose and Scope

A.2. Losses and Hazards

A.2.1. System Scope and Interfaces

A.2.2. DI&C Platform Adequacy

A.2.3. DI&C Design

A.2.4. Control Structure Hierarchy

A.2.5. Stakeholder Losses

A.2.6. System Hazards

A.3. Common Cause Failures Analysis

A.3.1. Unsafe Control Actions Deemed Postulated CCFs

A.3.2. PRA Information

A.3.3. Risk Reduction Targets and Control Effectiveness Profiles

A.4. Systematic Loss Scenarios

A.4.1. Relationship Sets

A.4.2. Systematic Loss Scenarios

A.5. Control Methods

A.5.1. Allocated Control Methods

A.5.2. Control Method Scoring

A.6. Conclusions