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

Prepared by the Nuclear Energy Institute
September 2021

Revision Table

Revision	Description of Changes	Date Modified	Responsible Person
Draft D	New draft utilizing Systems Theoretic Process Analysis.	8/31/21	Odess-Gillett, Warren Campbell, Alan Archambo, Neil

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: Odess-Gillett, Warren

Executive Summary

Implementation of digital technology at nuclear power stations can provide significant benefits in component and system reliability which can result in improved plant safety and availability. However, migrating I&C functions from analog to digital technology can introduce new hazards that could potentially create systematic failures including Common Cause Failures (CCFs). For High Safety Significant Safety-Related (HSSSR) systems, it becomes especially important to evaluate these hazards systematically and develop effective control measures to eliminate and/or mitigate them during the design process.

NRC Standard Review Plan, NUREG-0800, Branch Technical Position (BTP) 7-19, Revision 8, [17] provides three separate methods licensees can use to eliminate/mitigate CCF hazards from further consideration. These three methods are (1) use of diversity within the HSSSR system, (2) use of extensive testing, or (3) alternative methods approved by the NRC (e.g. defensive measures). NEI 20-07 is best aligned with the third method presented in BTP 7-19, Section 3.1.3 – alternative methods using defensive measures [17]. It is understood that BTP 7-19 [17] is an NRC staff review guidance document based on NRC SECY-93-087 and the associated Commission Staff Requirements Memorandum (SRM) [25]. The method described in this document is a risk-informed, performance-based approach to address potential HSSSR systematic failures, which is an alternative approach to addressing CCF than that described in SRM/SECY-93-087 [25].

The approach described herein uses Probabilistic Risk Assessment (PRA) insights combined with the hazard analysis methodology called System Theoretic Process Analysis (STPA) developed by the Massachusetts Institute of Technology (MIT) to create effective control methods to eliminate and/or mitigate potential HSSSR systematic failures that include CCF. This approach is an alternative to the 3-position approach for a Defense-in-Depth and Diversity (D3) analysis in SRM/SECY-93-087 [25].

The process has two major parts:

1. Establish a Risk Reduction Objective (RRO) using PRA insights and perform the first three steps of STPA to identify losses, hazards and unsafe control actions, and

2. Perform STPA step four to create the loss scenarios from the unsafe control actions and score the control method effectiveness to eliminate and/or mitigate the loss scenarios. These scores are compared to benchmark scores commensurate with the RRO established in Part 1 to ensure appropriate level of rigor is applied.

NEI 20-07 applies to all holders of operating licenses under Title 10 of the Code of Federal Regulations (10 CFR) Part 50, “Domestic Licensing of Production Facilities” [1] and all holders of combined licenses under 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants” [8]. Although the guidance in NEI 20-07 primarily focuses on power reactors, other licensees may also use the guidance in NEI 20-07 for addressing potential HSSSR systematic failures.

This document was developed by the NEI Digital I&C Working Group, in support of the industry response to Modernization Plan #1 (MP#1) Protection Against Common Cause Failure in the NRC’s Integrated Strategy to Modernize the Nuclear Regulatory Commission’s Digital Instrumentation and Control Regulatory Infrastructure (SECY-16-0070) [24]. MP#1, contained in Enclosure 1 of SECY-16-0070 [24], is identified as a high priority within the NRC Action Plan.

Table of Contents

1 INTRODUCTION

High Safety-Significant Safety-Related (HSSSR) systems that are deployed using digital instrumentation and control (DI&C) technology can be vulnerable to systematic failures as a result of the integration of functions and interfaces that could defeat the redundancy achieved by the system architecture.

The approach described herein uses Probabilistic Risk Assessment (PRA) insights combined with the Systems Theoretic Process Analysis (STPA) hazard analysis methodology developed by MIT to develop effective control methods to eliminate and/or mitigate potential HSSSR systematic failures that can cause a Common Cause Failure (CCF). This approach is an alternative to the 3-position approach for a Defense-in-Depth and Diversity (D3) analysis in SRM/SECY-93-087 [25].

The process has two major parts:

1. Establish a Risk Reduction Objective (RRO) using PRA insights and perform the first three steps of STPA to identify losses, hazards and unsafe control actions, and

2. Perform STPA step four to create the loss scenarios from the unsafe control actions and score the control method effectiveness to eliminate and/or mitigate the loss scenario. These scores are compared to benchmark scores commensurate with the RRO established in Part 1.

CCF are failures "due to latent design defects" [17] introduced to multiple structures, systems or components. STPA utilizes the term "Systematic Failure" which bounds CCF. Assessing potential systematic failures requires a rigorous, systematic process to consistently identify potential systematic failures of an HSSSR system. STPA has been used in the automotive industry and in the airline industry to effectively determine causes of catastrophic systematic failures. NuScale Power used STPA for their hazards analysis for their NuScale Small Module Reactor protection system as described in their Final Safety Analysis Report [18]. Using STPA in the front-end of the development process for an HSSSR system provides an effective means to establish requirements to prevent such systematic failures using systems theory principles. The process is repeated throughout the design process to reflect the available design detail considerations. This approach utilizes a multi-discipline team to analyze how the complete system interacts internally and externally and associates potential loss scenarios with these system interactions. By continuously analyzing the complex, digital HSSSR I&C system with a multi-discipline team, potential loss scenarios are considered and eliminated/mitigated throughout the design process through the application of control methods. Refer to Section 3.5 for application examples.

The risk-informed process establishes the benchmark (RRO) that control measures need to meet based on the risk significance of system loss. These control measures are evaluated for their capability to detect, prevent, and respond/recover from potential systematic failures. Their effectiveness needs to be commensurate with the RRO established in Part 1.

The process described in this report complements the EPRI Digital Engineering Guide [10] (DEG) when it calls for hazard analysis in the conceptual design phase or the detailed design phase of an I&C project. This process complements the EPRI Hazards and Consequences Analysis for Digital Systems (HAZCADS) [11] and Digital Reliability Analysis Methodology (DRAM) [12] processes that implement the EPRI DEG [10] hazard analysis. This process is a design diagnostic tool for identifying losses, hazards, and the associated unsafe control actions as well as assessing the risk sensitivity.

It is assumed that this guidance would be applied to a License Amendment Request (LAR) for an HSSSR system replacement that is submitted to the NRC for review and approval. The intention is not to apply this guidance to a plant modification under the 10 CFR 50.59 [7] process.

2 DEFINITIONS

Common Cause Failure (CCF) – Loss of function to multiple structures, systems, or components due to a shared root cause.

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.

Defensive Measures – Design attributes to prevent, limit, or reduce the likelihood of a CCF.

Design Attributes – Hardware and software design features that contribute to high dependability. Such features include built-in fault detection and failure management schemes, internal redundancy and diagnostics, and use of software and hardware architectures designed to minimize failure consequences and facilitate problem diagnosis.

Hazard - A system state or set of conditions that will lead to a loss. [27]

High Safety Significant Safety-Related (HSSSR) –Safety-related systems, structures or components (SSCs) that perform safety-significant functions (e.g., Reactor Protection Systems and Engineered Safety Features Actuation Systems). These SSCs have one or more of the following: 1. Credited in FSAR to perform design functions that significantly contribute to plant safety; 2. Relied upon to initiate and complete control actions essential to maintaining plant parameters within acceptable limits for a Design Basis Event or maintain the plant in safe state after safe shutdown; and 3. Failure could directly lead to accident conditions that have unacceptable consequences. [17] Systems categorized as Risk Informed Safety Category 1 (RISC-1) in accordance with Regulatory Guide 1.201 [22] 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.

Loss - Something of value to stakeholders, whether it be the plant owner, the general public, or a government agency. 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. [27]

Loss Scenario - The causal factors that can lead to the Unsafe Control Actions and to Hazards [27].

Relationship Set - A grouping of digital components that have a common set of characteristics related to functional coupling, data and control flow, physical location, or shared common procedure or program scope. [12]

Risk Reduction Objective (RRO) – An objective derived from a PRA sensitivity study in which the HSSSR system is assumed to completely fail in the PRA. The Δ CDF and Δ LERF are then mapped to the regions in Figures 4 and 5 in RG 1.174 [20]. The RRO is the level of risk reduction needed to make the delta CDF and delta LERF non-risk significant. [11]

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 – Defined as either protection, control or monitoring and comprised of one or more programmable electronic devices, including integrated and supporting elements such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices [13].

Systematic Capability – Measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified Safety Integrity Level (SIL), in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element. [13]

Systematic Control Method - A method that can be implemented to eliminate or mitigate a loss scenario.

Systematic Failure – Related in a deterministic way to a certain cause, which can only be eliminated/mitigated by a modification of the design or of the manufacturing process, operation procedures, documentation, or other relevant factors. [13]

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). [27]

Unsafe Control Action (UCA) - A control action that, in a particular context and worst-case environment, will lead to a Hazard. [27]

3 REGULATORY BASIS

The purpose of this document is to describe an alternative approach to addressing CCF from that described in SRM/SECY-93-087 [25]. STPA is used in conjunction with PRA insights as a method to identify systematic loss scenarios and then develop control methods commensurate with the level of risk to eliminate or mitigate those loss scenarios. This approach would be an alternative to the consequence-based analysis described in NUREG-0800, Chapter 7, Branch Technical Position 7-19 (BTP 7-19) [17], also referred to as the D3 analysis.

This document describes an alternate approach to addressing CCF for a HSSSR System License Amendment Request submitted to the NRC for review and approval.

3.1 SRM/SECY-93-087

SRM/SECY-93-087 provides NRC Commission direction regarding policy, technical and licensing issues for light water reactors. The approach provided within this technical report provides a risk-informed, performance-based analysis technique that identifies unsafe actions, determines scenarios in which those unsafe actions may occur and applies defensive measures. As such, the process described here within does NOT wholly conform to the four (4) positions in SRM/SECY-93-087, Section 18 [25]. A policy change to allow for risk-informed, performance-based approaches to addressing Digital I&C CCF is recommended based on the following:

1. *The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.*

   The approach described within this technical report leverages the STPA process to perform a Diversity and Defense-in-Depth (D3) analysis. STPA is used extensively in other safety industries (e.g. automotive and aviation) to perform hazard analyses as described in Section 3.5. This STPA process decomposes the system under analysis by function and control structure to identify actions and scenarios which may possibly lead to a loss. In accordance with BTP 7-19 [17], an alternative method may be utilized to eliminate/mitigate the potential for CCF identified in the D3 analysis.

2. *In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.*

   In lieu of analyzing each postulated common-mode failure for each event in the accident analysis section of the SAR, a risk-informed approach is taken to determine the consequence of failure. A PRA sensitivity study is performed to estimate the impact to Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) made by the proposed digital I&C system modification. This sensitivity study provides the impact of complete system failure and is utilized to determine the level of rigor applied during control method allocation. Additionally, if the impact of the sensitivity study is greater than the thresholds provided, then the proposed modification cannot be installed as designed (i.e. design change is required).

3. *If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.*

   The approach described herewith in does not prescribe diversity as a requirement for eliminating/mitigating a CCF; rather, ANY effective defensive measures (based upon level of rigor) may be applied to eliminate/mitigate the CCF. Diversity MAY be used as a defensive measure, but it is not prescribed in this approach. Due to the iterative nature of this process defensive measures are identified early in process and considered throughout the design process.

This approach conforms to NRC staff review guidance provided in BTP 7-19 [17] which provides acceptable paths for CCF elimination prior to implementation of diverse means. BTP 7-19, Section B.3.2, "Use of Diverse Means to Mitigate Common-Cause Failures," [17] states:

> *If a potential CCF vulnerability has not been eliminated from further consideration using the process in Section B.3.1 of this BTP, the reviewer should verify that the application's D3 assessment credits a diverse means to accomplish the same or different function than the safety function disabled by the postulated CCF or to mitigate spurious operations resulting from the postulated CCF.*

The NEI 20-07 approach aligns with BTP 7-19 Section B.3.1.3 [17] to utilize alternative methods to eliminate/mitigate CCF. Furthermore, acceptable means of applying diversity include crediting existing plant systems and manual operator action, both of which MAY be utilized as effective defensive (or control) measures in this process.

4. *A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.*

   Similar to Item 3, above, the approach described herewith in does not prescribe Human System Interface (HSI) for manual actuation and monitoring. Defensive measures MAY include manual actuation capabilities and critical parameter monitoring, as deemed necessary by the design to eliminate/mitigate a CCF.

3.2 Branch Technical Position (BTP) 7-19, Revision 8

BTP 7-19 [17] provides staff review guidance for I&C safety systems proposed in License Amendment Requests or in license applications (e.g. Design Certification, Combined Operating License, etc.) The guidance provides for three (3) acceptable methods for eliminating CCF vulnerabilities from HSSSR systems from further consideration: diversity, testing, and/or alternatives methods. The approach described herein provides an acceptable alternative method for eliminating CCF from further consideration.

BTP 7-19 [17] also provides staff review guidance for spurious operations. The method described herein requires consideration for control actions to be unsafe based on all states (i.e. control action applied, not applied, delayed, out of sequence, early, stopped too soon, and provided too long). Spurious operations are bounded by these control action considerations. Once identified as unsafe, defensive (or control) methods are applied to eliminate/mitigate the potential for CCF.

3.3 Regulatory Guide 1.174

NRC Regulatory Guide (RG) 1.174 [22] identifies a set of key principles to be addressed in risk-informed decision making (RIDM). 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 [4]).

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.

A change from an analog system to a DI&C system should meet 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.

The objective of the NEI 20-07 methodology is to identify hazards, unsafe control actions, and loss scenarios as part of a systems-oriented, integrated DI&C evaluation. By utilizing this methodology, the failures in design and operations can be identified by modeling the potential interactions between software errors, human errors, component failures, and component interaction.

By integrating hazard identification and PRA sensitivity analysis, risk reduction objectives 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 disposition the five principles for risk-informed decision-making process in RG 1.174 [20] using these concepts.

3.3.1 PRA Attributes

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. In regard to key assumptions and sources of uncertainty in the PRA models that can impact the bounding assessment, in the case of Step 1, assuming everything in the HSSSR system fails, is a way to address uncertainty (i.e., if it is unknown how likely the HSSSR system will be in terms of likelihood of failure, then the assumption is, it will all fail everything to determine the Risk Reduction Objective.

3.4 Other Regulatory Requirements

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

3.5 STPA Acceptance in Other Safety Industries

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

Table 1: Example STPA Users [16]

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

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

- The US Department of Transportation developed a STPA software tool, SafetyHAT, that is available for public use to facilitate use of STPA for analyzing advanced vehicle technology [23].
- General Motors has fully integrated STPA into system safety processes for human-system interface projects to prevent driver error in safety critical systems [28].
- Boeing has utilized STPA to evaluate potential conflicts between large commercial air traffic and small un-crewed aircraft systems to provide requirements/control measures for air traffic control systems [26].

- 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 [18] and approved by the NRC in the Final Safety Evaluation Report (FSER) [19]. 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.*

4 PROCESS

The process for identifying and eliminating HSSSR system CCF utilizes risk-informed, performance-based practices to decompose systems by function and structure to identify CCF vulnerabilities and apply defensive (or control) measures to eliminate/mitigate the potential for failure. EPRI HAZCADS [11] and DRAM [12] should be referenced by the practitioner for detailed implementation instruction. The STPA Handbook [27] also provides supplemental detail to aid the practitioner. The discussion provides sufficient description for NRC staff to reach a safety conclusion that the processes described herein are an acceptable alternative method for addressing CCF.

Part 1 of the process utilizes risk insights to perform a PRA sensitivity study to determine the level of rigor (Risk Reduction Objective) applicable to the system under analysis. Additionally, Part 1 describes the method for decomposing the system under analysis. Decomposition identifies Losses, Hazards, Control Actions, and Unsafe Control Actions as shown in Figure 1. This level of decomposition provides a traceable means of identifying all actions (including delayed, early, and no-action scenarios) that are possible for a given system. UCAs are re-stated as design requirements in the modification and/or system specifications. Section 4.1 provides further detail on Part I of the process. Section 4.1.3 provides a high-level example of the Part I methodology described.

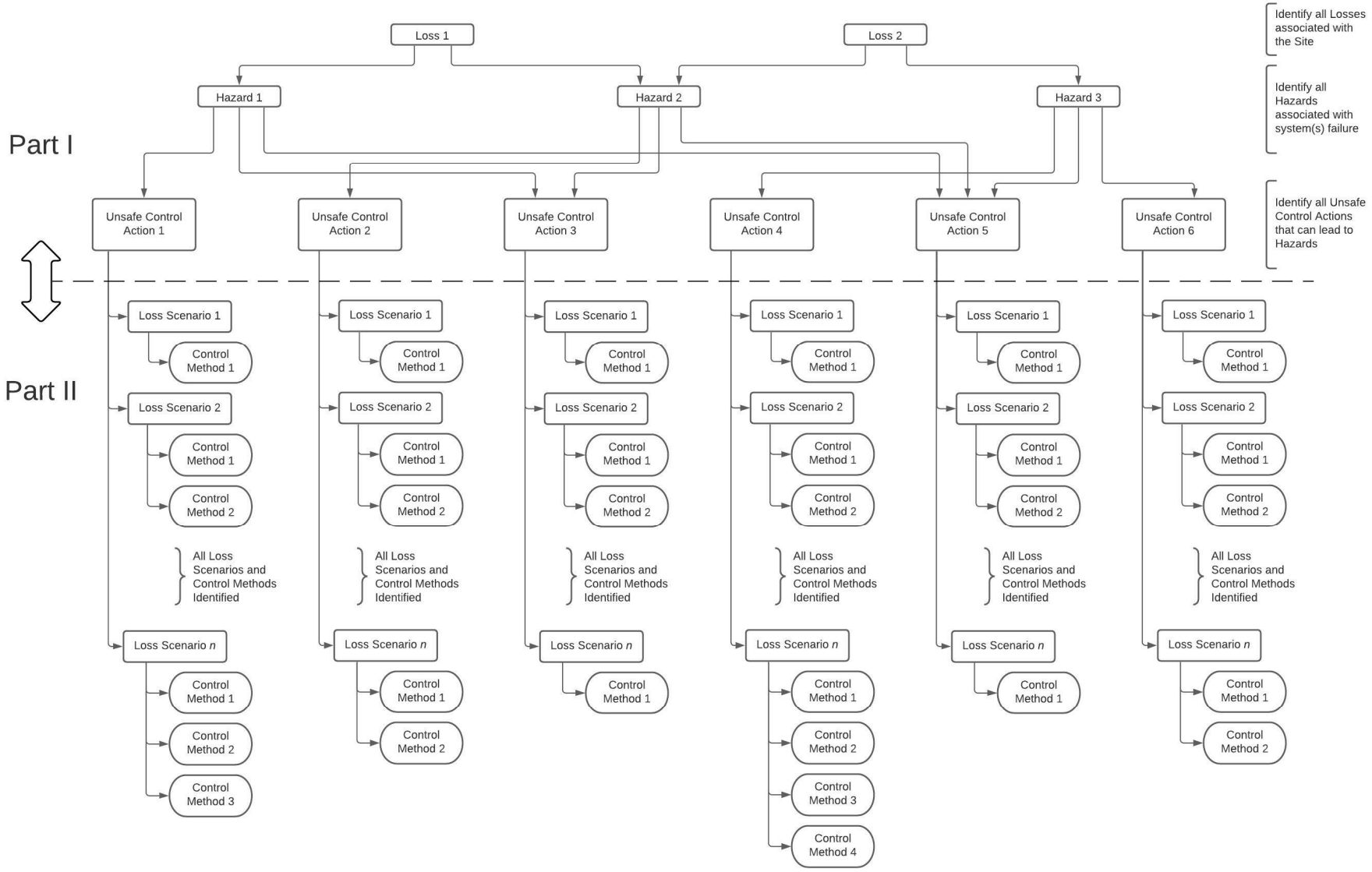

Figure 1: NEI 20-07 Process Overview

Part II of the process utilizes the results of Part I (i.e. Risk Reduction Objective and Unsafe Control Actions) to develop Loss Scenarios and apply Control Methods. For each Unsafe Control Action (UCA), Loss Scenarios are identified for all scenarios in which the UCA can occur. Once identified, the control method(s) is applied to prevent, detect, and/or respond and recover from the loss scenario commensurate with the level of rigor defined by the Risk Reduction Objective (RRO). Where necessary, multiple control methods may be utilized to achieve the RRO. Additionally, control methods MAY be applied to individual components OR groups of components. Section 4.2 provides further detail on Part II of the process. Section 4.2.6 provides a high-level example of the Part II methodology described.

The overall process is iterative in nature and is adjusted throughout the design process to accommodate the available level of detail. For example, during the conceptual design phase, high levels of abstraction are utilized to identify initial sets of UCAs, loss scenarios and control methods. As the design progresses into detailed design, the analysis is modified to refine the analysis results. The initial analysis is performed after a conceptual design has been established. The results of this process (i.e. systematic control methods) are then incorporated into the design (or plant operating policies, in non-technical control methods are deemed acceptable). As the design matures into the detailed design, the process is repeated to reflect greater levels of detail. The results are continuously fed back into the design process to ensure applied control methods are adequately documented, evaluated, tested and maintained.

4.1 Part I: Establish Risk Reduction Objective and Unsafe Control Actions

Part I of this process is to establish the RRO and perform the hazard analysis using STPA to define the Unsafe Control Actions for the HSSSR system. The first step in Part I establishes the Risk Reduction Objective (RRO) for the system under analysis which informs the level of rigor required to satisfactorily apply Control Measures based upon risk significance. Subsequent steps of Part I provide a process for decomposing Losses, Hazards, Control Actions and Unsafe Control Actions (UCAs). The resulting UCAs are actions that if taken (or delayed, too early, or not taken) would result in system-level Hazards and potentially plant Losses. Design requirements are derived from UCAs that provide traceable evaluation, testing, etc. through the design process.

4.1.1 Establish Risk Reduction Objective

Establishing the RRO is accomplished by performing a PRA sensitivity study in which the HSSSR system is assumed to completely fail. If the HSSSR system is an integrated RPS and ESFAS, then it is the combined failure of both that is postulated in the PRA sensitivity study. The result would be a change in Core Damage Frequency (CDF) and Large Early Release Frequency (LERF). The ΔCDF and ΔLERF are then mapped to the regions in Figures 2 and 3 (RG 1.174 Figures 4 and 5 [20]) and used to determine the RRO.

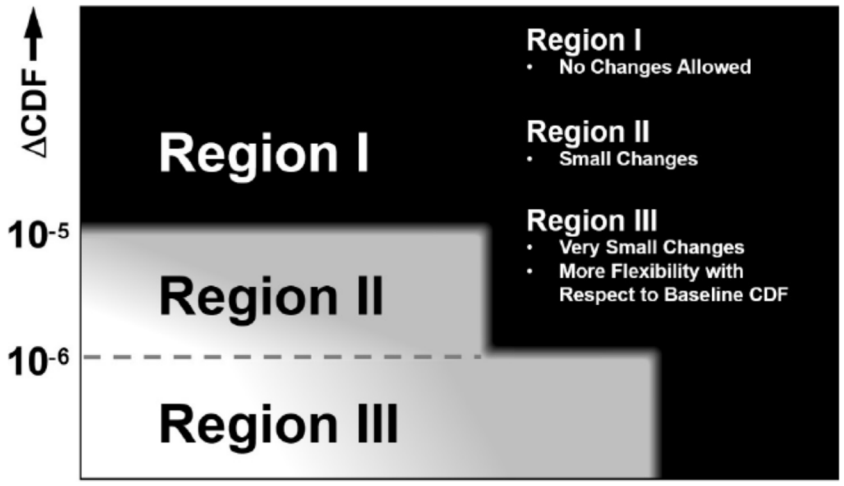

Figure 2: PRA Sensitivity Study to Establish Δ CDF

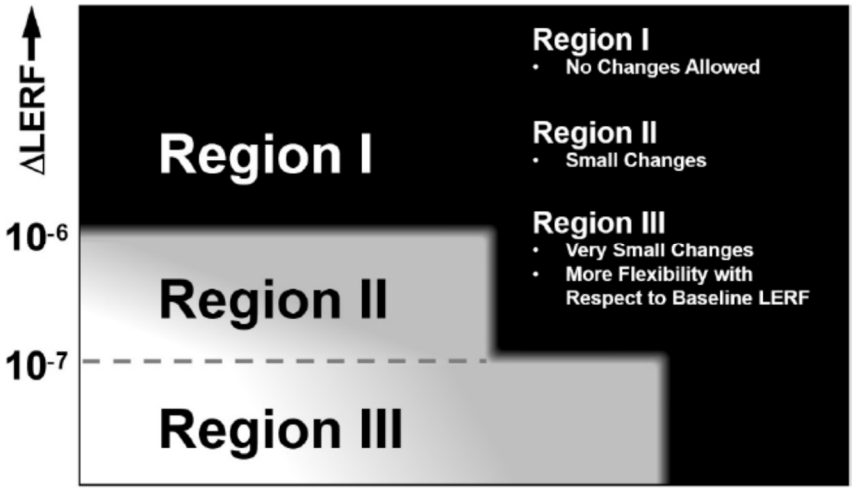

Figure 3: PRA Sensitivity Study to Establish Δ LERF

Once the ΔCDF and ΔLERF are calculated for the system(s) under analysis, Table 2 is utilized to determine the RRO. 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 RRO would be A in Table 2. If ΔCDF and ΔLERF results provide different RRO results, then the most conservative RRO result is applied throughout the remaining process steps. The RRO impacts the type, strength and, possibly, quantity of control methods that will be applied for each Loss Scenario in subsequent steps. RRO 'A' requires the most rigorous control method types and strengths (or strongest combinations thereof). If the ΔCDF result is 1E-2, then the RRO is not attainable and thus a new design needs to be created. Note that the changes in CDF and LERF as used in Table 2 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 purposes of providing a mechanism for risk-informing decisions about the I&C design.

Table 2: Establish RRO base on ΔCDF and ΔLERF

RRO	Change in Core Damage Frequency – CDF (per year)	Change in Large Early Release Frequency – LERF (per year)
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

Figure 4 combines these concepts to display how the RRO is used to inform application of control methods to qualitatively reduce the change introduced by the modification/upgrade.

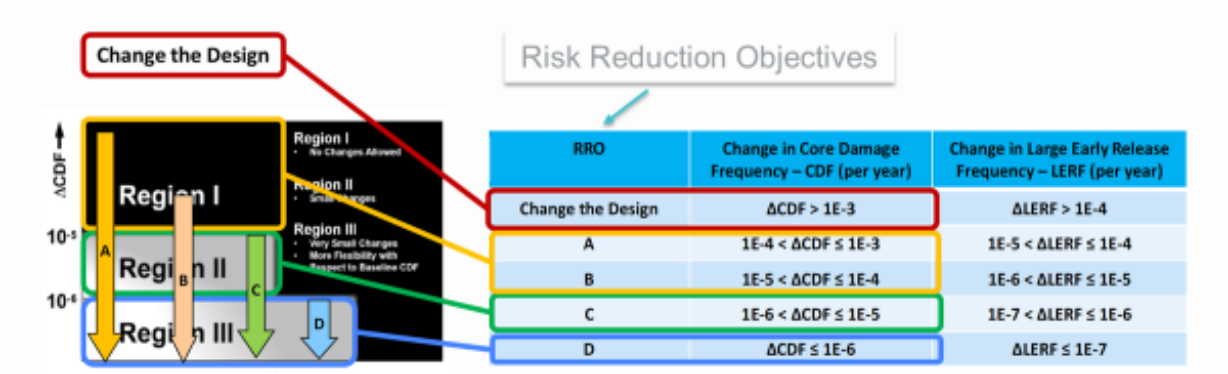

Figure 4: RRO Mapped to RG 1.174 Table [20]

4.1.2 Establish Unsafe Control Actions

This process utilizes the first three (3) parts of the STPA method to decompose plant level Losses to UCAs.

4.1.2.1 Identify Losses

Losses should be identified at a high level of abstraction and are typically limited to five, so they are relatively simple and bounding. Losses are listed categorically and are labeled L1, L2, etc. for traceability. The list of Losses can be standardized and used as a starting point for all assessments, recognizing that new losses may be identified for a particular assessment. For example, the following Losses are possible for unmitigated hazards in many systems (but should not be considered a complete or representative list):

- L-1 Human injury or loss of life

- L-2 Radiological impact
- L-3 Environmental damage
- L-4 Significant loss of revenue
- L-5 Reputational harm

These unacceptable Losses then serve to benchmark descriptions of unacceptable behavior within the HSSSR system. Some precautions in identifying Losses include:

- Losses should not reference individual components or specific causes.
- Losses may involve aspects of the environment that are not directly controlled by the system designer.
- Document any special considerations or assumptions made, such as losses that are explicitly excluded.

The STPA Handbook [27] provides additional guidance in developing Losses. For the purposes of the applicant, the analysis provided for regulatory review should focus on Losses that are relevant to the safety determination.

4.1.2.2 Identify Hazards

After identifying Losses, system level Hazards that contribute to these Losses are created. Potential system level Hazards are identified that are precursors to these Losses. Note that a hazardous condition by itself may or may not directly lead to a Loss. In many cases, other hazardous conditions are necessary before a Loss will occur.

To identify the system level Hazards, the HSSSR system boundary to be analyzed needs to be identified. The most useful way to define the system boundary for analysis purposes is to include the parts of the system over which the system designers have some design control. This is the primary reason for distinguishing between Hazards and Losses—Losses may involve aspects of the environment over which the system designer or operator has only partial or no design control at all. The goal is to eliminate or mitigate the effects of Hazards in the system under analysis, so some level of design control is necessary. Figure 5, from the STPA Handbook [27], illustrates the system boundary as an abstraction that separates a system from its environment.

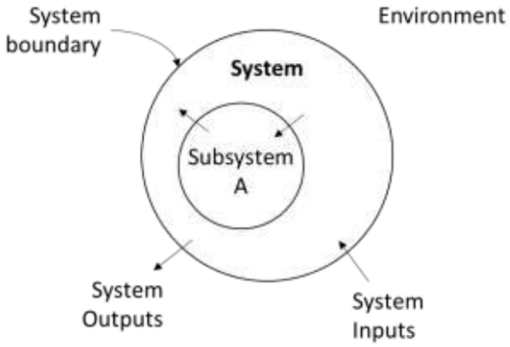

Figure 5: Relationship between the HSSSR System, Its Boundary, and the Environment [27]

Like Losses, the system Hazards are listed and labeled, but in this case the Hazards are labeled H1, H2, etc. so they can be linked and traced to the resulting losses. Note the list of system Hazards is typically not any longer than the list of losses, and in some cases the list is shorter.

The STPA handbook [27] identifies three basic criteria for defining system-level Hazards:

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

   Hazards are states or conditions, not external environmental states that are outside the designer's control. In addition, Hazards should not describe detailed component-level causes like a physical component failure. Referencing component-level causes during this step will overly restrict the analysis, making it easy to overlook other less obvious causes during later steps. Instead, identify the states or conditions to be prevented (the Hazards) and allow the later STPA steps to systematically identify component-level causes of the Hazards.

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

   There must be a worst-case environment in which Hazards will lead to a Loss. This requirement does not necessarily guarantee that a Hazard will always result in a Loss. For example, NPP physical damage may allow the NPP to release toxic levels of radiation, but wind and weather conditions prevent the toxic radiation from impacting nearby personnel and populated regions. However, in a worst-case environment, the toxic radiation can be carried to populated areas and lead to Losses.

3. Hazards must describe states or conditions to be prevented

   Hazards are states or conditions to be prevented. "The RPS scrams the reactor" is a system state that could arguably lead to a Loss in a worst-case environment, but it is not a condition to be eliminated or prevented (otherwise there would be no HSSSR system). Hazards should be states to be prevented — not states that the system must normally be in to accomplish its goals.

From the STPA handbook [27], some precautions in identifying hazards (hazardous system states) include:

- Confusing hazards with causes of hazards

A common mistake in defining Hazards is to confuse Hazards with causes of Hazards. For example, “processor failure” and “processor failure not annunciated” are not hazards but potential causes of hazards. To avoid this mistake, make sure the identified hazards do not refer to individual components of the HSSSR system, like CPU or I/O module.

In other words, check that each hazard contains:

<Hazard ID> = <System> & <Unsafe Condition> & <Link to Losses>

Hazards define exactly what “unsafe” means. The STPA Handbook [27] cautions using the word “unsafe” in the Hazards themselves. Doing so creates a recursive definition and does not add information or value to the analysis; and does not help specify the actual condition that is unsafe. The recommendation then is to avoid using the word “unsafe” in the Hazard itself and instead specify exactly what is meant by “unsafe” (i.e. define what states or conditions would be unsafe).

Hazard identification in STPA identifies conditions that are inherently unsafe— regardless of the cause. The 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 following recommendations are made in the STPA Handbook [27] to assist in creating good Hazard statements:

- Hazards should not refer to individual components of the system.
- All Hazards should refer to a condition to be prevented.
- Hazards should refer to factors that can be controlled or managed by the system designers and operators.
- The number of Hazards should be relatively small.
- Hazards should not include ambiguous or recursive words like “unsafe”, “unintended”, “accidental”, etc.

The STPA Handbook [27] suggests beginning with a more abstract and manageable set of Hazards and refine them into sub-hazards later, if needed.

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 the list of system-level Hazards has been identified and reviewed, these Hazards can be refined into sub-hazards. Sub-hazards are typically derived from states or conditions that are required to be controlled to prevent a Hazard. Sub-hazards can be useful for large analysis efforts and complex applications because they can guide future steps like modeling the control.

4.1.2.3 Model Control Structure

Once Hazards are created, a control structure is developed to model the HSSSR system. A hierarchical control structure is composed of control loops like the one shown in Figure 6 from the STPA Handbook [27]. 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.

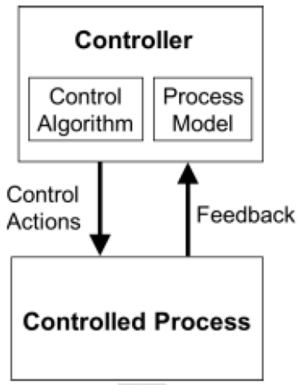

Figure 6: Elements of a Control Structure [27]

Most HSSSR systems typically have several overlapping and interacting control loops. Multiple interacting control loops can be modeled in a hierarchical control structure, as shown in Figure 7.

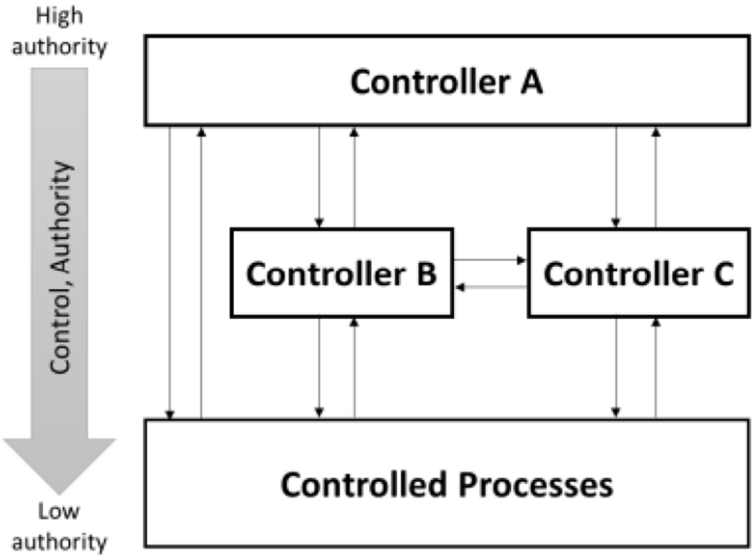

Figure 7: Hierarchical Control Structure [27]

In general, a hierarchical control structure contains at least five types of elements:

- Controllers
- Control Actions

- Feedback
- Other inputs to and outputs from components (neither control nor feedback)
- Controlled processes

The vertical axis in a hierarchical control structure is meaningful because it indicates control and authority within the system. The vertical placement represents the hierarchy of control from high-level controllers at the top to the lowest-level entities at the bottom. Each entity has control and authority over the entities immediately below it, and each entity is likewise subject to control and authority from the entities immediately above. For example, the HSSSR system in Figure 8 (adapted from the STPA Handbook [27]) can act as a controller by sending control actions to physical NPP components and monitoring feedback. At the same time, the HSSSR system is also a controlled process that receives and executes control actions from the Main Control Room (MCR) Operator and sends feedback to the MCR.

All downward arrows represent control actions (commands) while the upward arrows represent feedback. These conventions help to manage complexity and make control relationships and feedback loops easier to recognize.

According to the STPA Handbook [27] failures can occur at any point in Figure 7. For example, a process model that is not consistent with reality (e.g. a controller believes an NPP is performing normally when it is really approaching plant design limits) can lead to control actions that are unsafe. A sensor failure may cause incorrect feedback and lead to unsafe behavior. A design may be missing the necessary feedback or may provide delayed feedback that results in a process model flaw and unsafe behavior. STPA provides a way to systematically identify these and other scenarios that can lead to a loss.

The generic control loop in Figure 7 can be used to explain and anticipate complex software and human interactions that can lead to losses—two of the biggest challenges in modern engineering. For humans, the process model is usually called a mental model and the control algorithms may be called operating procedures or decision-making rules, but the basic concept is the same.

Most HSSSR systems typically have several overlapping and interacting control loops. Multiple interacting control loops can be modeled in a hierarchical control structure.

The STPA Handbook [27] provides the following cautions when developing the HSSSR system control structure:

- A control structure is not a physical model

  The hierarchical control structure used in STPA is a functional model, not a physical model like a physical block diagram, a schematic, or a piping and instrumentation diagram. The connections show information that can be sent, such as commands and feedback—they do not necessarily correspond to physical connections. For example, the interactions between the Operators and NPP Management are not of a physical nature, but they are modeled in a functional control structure.

- A control structure is not an executable model

The control structure is not an executable model or a simulation model. Control structures often include components for which executable models do not exist (such as humans). Instead, STPA can be used to carefully derive the necessary behavioral constraints, requirements, and specifications needed to enforce the desired system properties.

- A control structure does not assume obedience

  The control actions and feedback in a control structure simply indicate that a mechanism will be created to send this information (i.e. it will be in the system design or plant policies/procedures). It does not imply or assume anything about how controllers and processes will actually behave in practice. In fact, a major goal of STPA is to analyze the control structure and anticipate how each element might behave in unsafe and potentially unexpected ways.

- Use abstraction to manage complexity

  One of the biggest challenges in any hazard analysis is managing system complexity. Control structures use abstraction in several ways to help manage complexity. For example, instead of explicitly listing every individual HSSSR subsystem, begin with a more abstract level by modeling HSSSR system automation and the physical processes they control as two levels in the control hierarchy.

  The principle of abstraction can also be applied to the command and feedback paths in the control structure. This principle is especially useful during early development phases when individual commands and sensors are not yet known.

  The control action path may contain mechanisms by which the controller acts upon a controlled process (referred to as actuators) and mechanisms by which the controller senses feedback from a controlled process (referred to as sensors). These details are usually abstracted away when initially creating the control structure, but the control structure will be refined to include actuators and sensors later during the scenario creation step.

  The abstract control structure can be used to begin STPA and identify the requirements and constraints for the communication path and other parts of the system. Then, STPA results can be used to drive the architecture, preliminary and detailed design, make implementation decisions, and refine the control structure. Even if details are known and design decisions have been made, it can be helpful to first apply STPA at a higher abstract level first to provide quicker results and identify broader issues before analyzing more detailed control structure models.

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

The control actions identified during the control structure modelling will be the basis for establishing unsafe control actions (UCAs).

4.1.2.4 Identify Unsafe Control Actions

Once the control structure has been modeled, the next step is to identify Unsafe Control Actions (UCAs).

The STPA Handbook [27] states that there are four ways a control action can be unsafe:

1. Control action not provided when _____.
2. Control action provided when _____.
3. Control action provided too early, provided too late, or provided in the wrong order when _____.
4. Control action stopped too soon or provided too long when _____.

The structure of the UCA has 4 elements:

<controller> <type of UCA> <control action> <context>

Developing the fourth element (context) of a UCA statement is more involved because it requires knowledge and evaluation of the system and its purpose or goals.

4.1.2.5 Translate Unsafe Control Actions to Requirements

Each UCA is inverted so it is restated in the form of a requirement, which is then included in the requirements documentation for the HSSSR system. Restating each UCA as a design requirement provides traceability throughout the design process to ensure resulting analysis/evaluation, system testing, and lifecycle maintenance considerations are incorporated into the system design lifecycle. Additionally, incorporation into requirements documentation provides legacy requirements to be considered during future plant changes.

4.1.3 Reactor Protection System Example

To demonstrate the process of identifying UCAs and resulting requirements, the following high-level example of a Pressurized Water Reactor (PWR) Reactor Protection System (RPS) is provided from the EPRI HAZCADS implementation guide [11]. Note this example is high-level and intended to provide contextual support of the process described herein. Actual implementation requires greater design detail, multidisciplinary team engagement, etc.

4.1.3.1 Identify Losses

The following losses are typical plant-level losses for an NPP.

- L-1 Human injury or loss of life
- L-2 Radiological impact
- L-3 Environmental damage

- L-4 Significant loss of revenue
- L-5 Reputational harm

4.1.3.2 Identify Hazards

An example list of Hazards for a PWR RPS is provided below, linked to the previous Losses (but should not be considered a complete or representative list):

- H1: Plant is physically damaged (L2, L3, L5)
- H2: Plant releases radioactive materials (L2, L3, L5)
- H3: Plant is shut down (L4)

For H-1, the Hazard can be a contributor to loss L-2, “Radiological impact”. It is possible that loss L-1 does not occur, but it needs to be assumed that the worst-case conditions occur such that it contributes to large radiological release that leads to the potential loss [L-1]. There may be defense-in-depth systems in the nuclear power plant that the HSSSR system does not control that may mitigate the potential loss, but the HSSSR system can control the scram of the reactor so as not to contribute to the potential loss. Hazard [H-1] can be linked to losses [L-2], [L-3] and [L-5].

4.1.3.3 Model Control Structure

Creation of a control structure is an iterative process. The following figures provide an example of how a PWR RPS control structure can be modeled at a conceptual level.

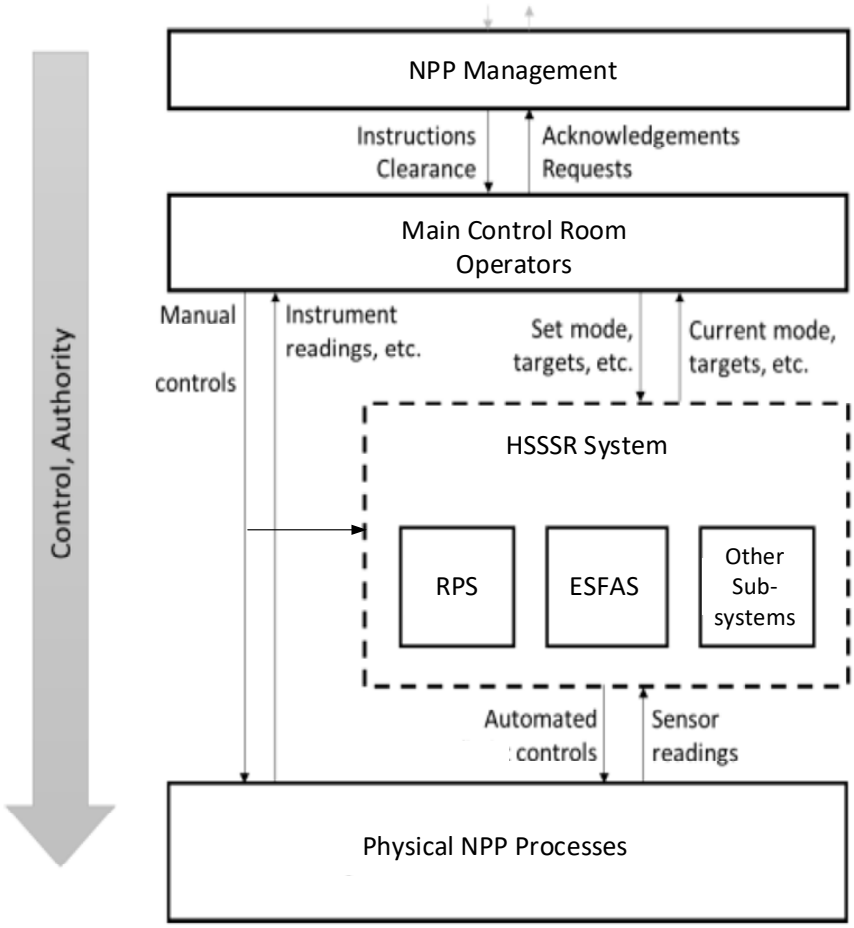

Figure 8: Simple Example of Hierarchical Control Structure – Adapted from STPA Handbook [27]

The control structure can be refined by defining how each subsystem will be controlled. Figure 9 shows how the RPS subsystem can be refined.

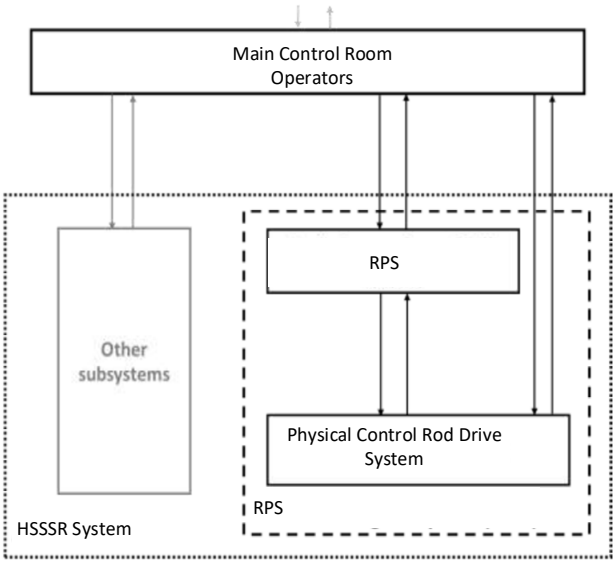

Figure 9: Refined Hierarchical Control Structure – Adapted from STPA Handbook [27]

The control structure can then be further refined to provide even greater detail as shown in Figure 10. The control structure includes three controllers (an operator, Diverse Scram System (DSS), and RPS) to show how they all influence the positions of the control rods, but the scope of this example as it is developed further in HAZCADS [11] is only about the RPS. The red box in Figure 10 indicates a proposed digital RPS that is completely independent of the DSS and the Operator when it comes to tripping the reactor. The Operator and DSS both receive information and can execute their control actions without relying on the RPS.

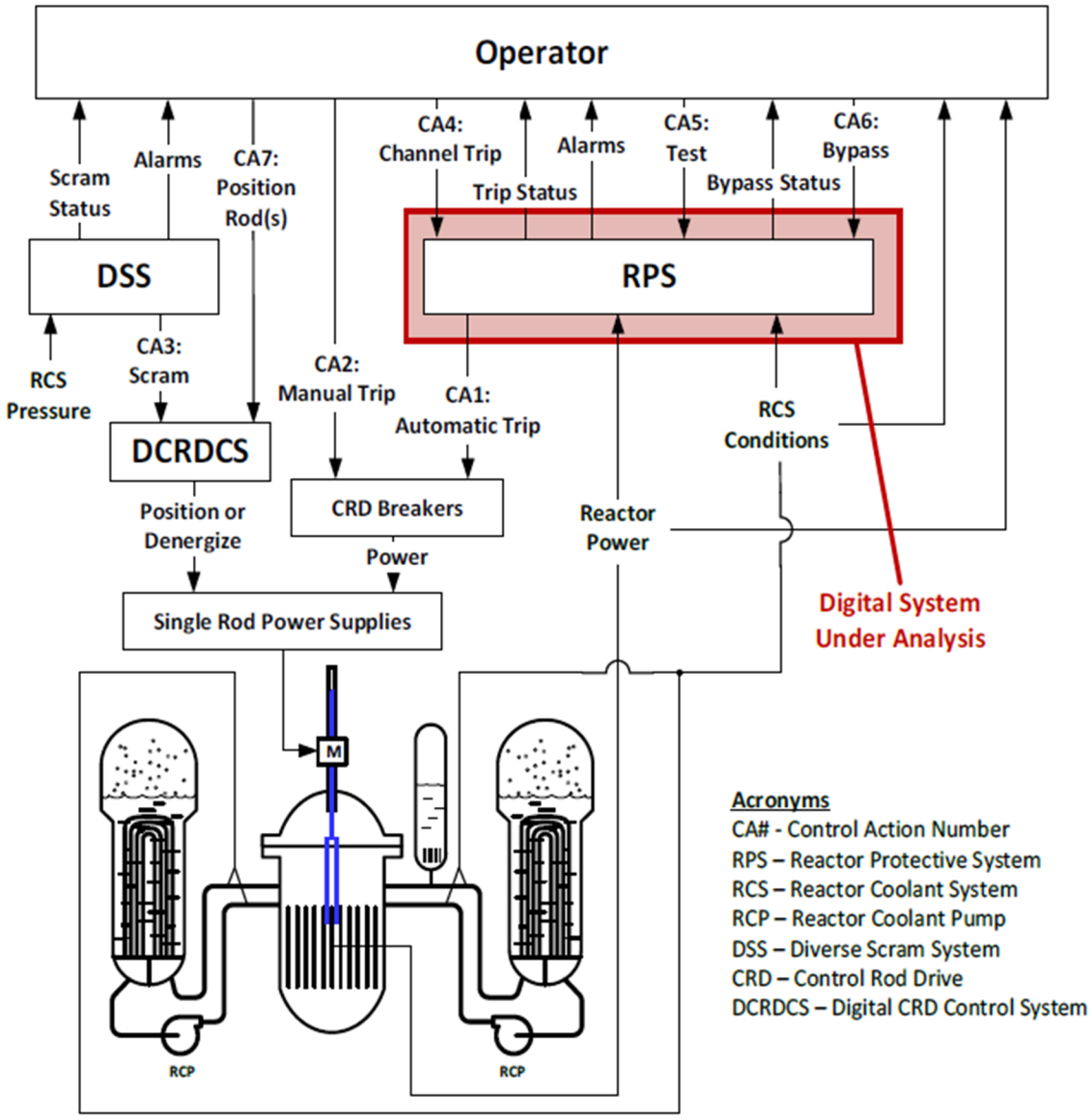

Figure 10: Refined Hierarchical Control Structure for an RPS [11]

The controlled process would be the Control Rods and RCS (i.e., limiting RCS pressure by tripping the reactor when pressure is increasing beyond normal conditions).

Seven high level control actions are identified in Figure 10 as follows:

- CA1: Automatic trip (via RPS)
- CA2: Manual trip (via human operator)
- CA3: Scram (via DSS)
- CA4: RPS Channel Trip (via human operator)

- CA5: RPS Test (via human operator)
- CA6: RPS Bypass (via human operator)
- CA7: Position Control Rod(s)

4.1.3.4 Identify Unsafe Control Actions

At the highest level, the RPS has one simple control action - automatically trip the reactor. An example of a high-level unsafe control action (UCA) would then be as follows:

RPS does not provide automatic reactor trip when neutron flux exceeds safety limit.

Where,

<controller>	=	RPS
<type of UCA>	=	does not provide
<control action>	=	automatic reactor trip
<context>	=	when neutron flux exceeds safety limit

Every UCA must be traceable to one or more Hazards. If UCA is identified that does not relate to one of the identified Hazards, a Hazard may be missing, and it may be necessary to add a new Hazard or revise an existing Hazard.

Table 3 is an example set of UCAs for CA1: Automatic Trip in Figure 10. Note – Table 3 is incomplete because it does not include ALL control actions that an operator can provide to the RPS as shown in Figure 10. For the analysis to be complete, development of UCAs for the operator control actions is necessary.

Table 3: Examples of Unsafe Control Actions for the RPS [11]

	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Order	Stopped Too Soon/ Applied Too Long
Controller: RPS Control Action: CA-1 Automatic Trip	RPS-UCA1 RPS does not provide automatic reactor trip when heat addition (reactor power) exceeds heat removal capability (RCS conditions), leading to a fuel damage safety limit or a pressure integrity safety limit [H-1, H-2]	RPS-UCA2 RPS provides automatic reactor trip when heat addition (reactor power) does not exceed heat removal capability (RCS conditions) [H-3]	RPS-UCA3 RPS provides automatic reactor trip too late - after heat addition (reactor power) exceeds heat removal capability (RCS conditions), leading to a fuel damage safety limit or a pressure integrity safety limit [H-1, H-2]	RPS-UCA4 RPS stops providing an automatic reactor trip too soon - before the CRD breakers can detect and respond - when heat addition (reactor power) exceeds heat removal capability (RCS conditions), leading to a fuel damage safety limit or a pressure integrity safety limit [H-1, H-2]

The first column indicates the “automatic reactor trip” control action by RPS. The second column RPS-UCA1 is the first of four UCAs for this control action. RPS-UCA1 can lead to hazards H-1 and H-2. RPS-UCA2, 3 and 4 are in the remaining columns.

4.1.3.5 Translate Unsafe Control Actions to Requirements

Each UCA in Section 4.1.3.4 will be converted to a design requirement included in the associated design package. As an example, UCA2 states:

> *RPS provides automatic reactor trip when heat addition (reactor power) does not exceed heat removal capability (RCS conditions) [H-3].*

Can be converted to the requirement:

> *RPS SHALL NOT initiate a reactor trip when heat addition (reactor power) does not exceed heat removal capability (RCS conditions).*

4.2 Part II: Develop Loss Scenarios and Identify, Allocate and Score Systematic Control Methods

There are 3 processes involved for Part II of this process:

1. Develop Loss Scenarios – utilizing UCAs developed from Part 1, Loss Scenarios are developed to further decompose Losses into unique scenarios that may result in a UCA.

2. Develop Systematic Control Methods – systematic control methods to eliminate or mitigate loss scenarios are created and allocated to the HSSSR system architecture, plant policies, plant procedures, etc.

3. Score Control Methods – each systematic control method to eliminate or mitigate a loss scenario is scored and benchmarked against the scoring requirements commensurate with the RRO.

4.2.1 Develop Loss Scenarios

Loss Scenarios are developed such that specific causes of UCAs are identified that can be prevented and/or detected. The STPA Handbook [27] defines two (2) types of Loss Scenarios:

1. Scenarios that drive the execution of UCAs (or "Why would Unsafe Control Actions occur?")

2. Scenarios that improperly execute, or prevent execution of, control actions (or "Why would control actions be improperly executed or not executed?")

Figure 11 displays these two types of Loss Scenarios mapped on a generic control structure to display where they primarily present themselves.

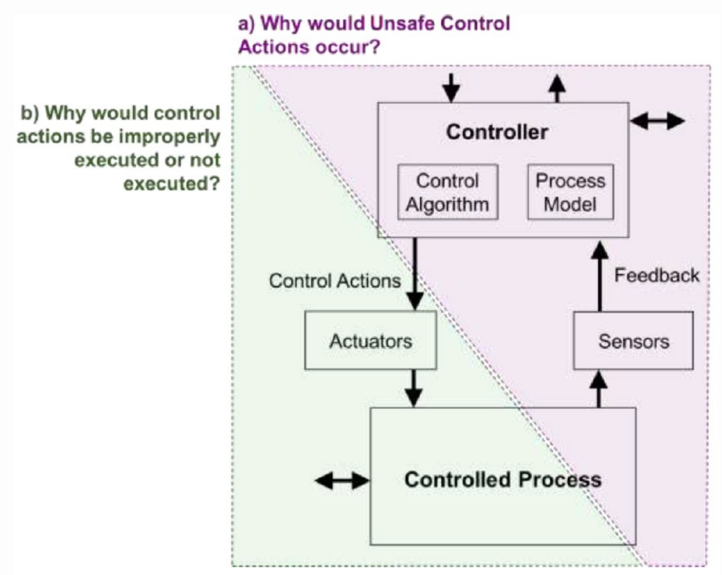

Figure 11 - Two Types of Loss Scenarios [27]

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

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

Figure 12 maps these sources for loss scenarios to show the relationship between the two types of loss scenarios with the four sources of loss scenarios:

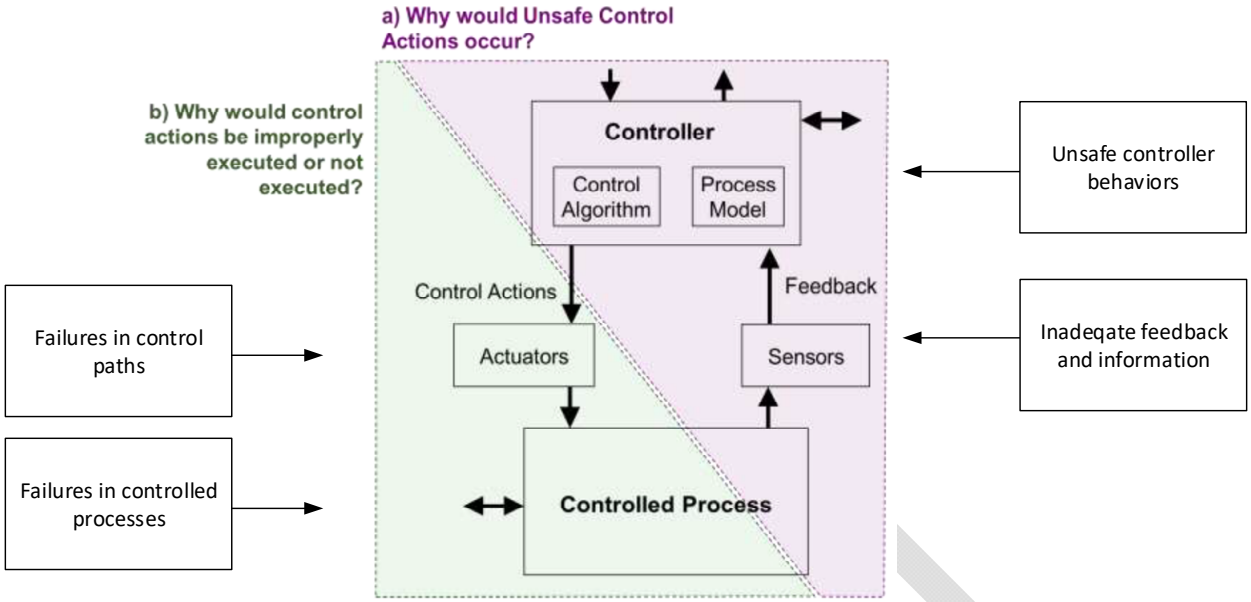

Figure 12: Four Sources for Loss Scenarios Mapped to Two Types of Loss Scenarios

The STPA Handbook [27] cautions to avoid identifying individual causal factors rather than a scenario. The problem with listing individual factors outside the context of a scenario is that it is easy to overlook how several factors interact with each other. It can lead to overlooking non-trivial and non-obvious factors that indirectly lead to UCAs and hazards and considering how combinations of factors can lead to a hazard. Considering single factors essentially reduces the analysis to a Failure Modes and Effects Analysis (FMEA) where only single component failures are considered.

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.

4.2.1.1 UCA Drivers

Unsafe Control Actions are primarily driven from two considerations:

1. Unsafe Controller Behavior

2. Inadequate Feedback and Information

The STPA Handbook [27] and EPRI DRAM [12] describes three types of loss scenarios related to unsafe controller behavior as shown in Table 4 below. The table also provides examples of Loss Scenario causes that can be considered. This table is NOT a complete list of Loss Scenario causes and should NOT be utilized in that manner.

Table 4 – Unsafe Controller Behavior Loss Scenario Types [12, 27]

Unsafe Controller Behavior Loss Scenario Types	Example Loss Scenario Causes
Controller failure	Physical controller failure Power failure
Inadequate control algorithm	Flawed implementation Flawed specification Algorithm degrades over time due to external change
Unsafe control input	UCA received from another controller Inadequate process model Controller receives incorrect feedback/information Controller receives correct feedback/information but interprets it incorrectly or ignores it Controller does not receive feedback/information when needed (delayed or never received) Necessary controller feedback/information does not exist

An additional source of UCAs if from inadequate sensors and elements that provide feedback or data pathway between a controlled process and processor. This information can be provided from a variety of sources such as analog components, digital components, scaled signals, binary signals, etc. Table 5 provides Loss Scenario types and examples related to inadequate feedback or information. This table is NOT a complete list of Loss Scenario causes and should NOT be utilized in that manner.

Table 5 – Inadequate Feedback or Information Loss Scenario Types [12, 27]

Inadequate Feedback/Information Loss Scenario Types	Example Loss Scenario Causes
Sensor(s) information/feedback sent but not received by controller	An element in the feedback or information pathway is exposed to environmental conditions beyond its capabilities. A sneak circuit or race condition results in a discontinuity, block, or incorrect route in the feedback or information pathway.

Inadequate Feedback/Information Loss Scenario Types	Example Loss Scenario Causes
Sensor(s) information/feedback not sent by sensor(s)	Sensor output terminations are incorrect or blocked. Sensor configuration is incorrect.
Sensor(s) information/feedback is inadequate upon receipt	The duration of the feedback or information is not long enough to be acquired by the controller. The feedback or information is aliased by a pathway element. Cable insulation resistance is degraded, causing an error. Noise is induced in feedback or information pathway elements, causing an error.
Feedback/information is not received by or applied to sensor(s)	Sensing lines for fluid process sensors (water, steam, air, hydrogen, nitrogen, oil, chemical, etc.) are blocked, filled, drained, or fouled. Sensors that rely on proximity, touch, clamping, or physical bond are masked, fouled, loose, or not in the correct position. Sensor is in the wrong location in the controlled process.
Sensor(s) respond adequately but is inadequately sent	Sensor exposed to environmental conditions beyond its specifications, causing a delay or error. Environmental conditions can include vibration, temperature, humidity, particulates, radiation, etc. Sensor is degraded, causing a delay or error beyond specifications. Sensing element lifetime is shorter than assumed (e.g., incore detector burnup is faster than expected). Sensor calibration interval is too long.

Inadequate Feedback/Information Loss Scenario Types	Example Loss Scenario Causes
Sensor(s) receive inadequate feedback/information	Sensor is in the wrong location in the controlled process. Maximum or minimum process conditions are masked by conditions at or near the sensing element. Masking may be caused by fouling, corrosion, thermal layering, poor mixing, cavitation, two-phase flow, freezing, etc.
Feedback pathway is inadequate for necessary feedback/information.	One or more feedback/information pathway elements is exposed to environmental conditions beyond its specifications. One or more feedback/information pathway elements does not meet its specified environmental capability. The sensitivity capability of sensors and related signal processing equipment is insufficient. The accuracy capability of sensors and related signal processing equipment is insufficient.

4.2.1.2 Improperly Executed Control Action

A control action may be improperly executed, or not executed, due to:

1. Failure in the control path
2. Failure in the control process

Control path failures occur between the controller and controlled process. These types of failures are typically due to elements in the pathway or the actuators themselves. For this discussion, an actuator is any component that can receive a control action and respond by directly or indirectly influencing the controlled process. Table 6 provides example loss scenarios incurred due to failures in the control path. This table is NOT a complete list of Loss Scenario causes and should NOT be utilized in that manner.

Table 6 – Inadequate Control Path Loss Scenario Types [12,27]

Failure in Control Path Loss Scenario Types	**Example Loss Scenario Causes**
Control action sent but not received	An element in the control action pathway is exposed to environmental conditions beyond its capabilities. A sneak circuit or race condition results in a discontinuity, block, or incorrect route in the control action pathway.
Control action correct but not sent to actuation	Controller output terminations are incorrect or blocked. Controller output configuration is incorrect.
Control action correctly sent but is inadequate upon receipt at the actuator	A feedback or information lag or delay. The duration of the control action is not long enough to be acquired by the actuator(s). Cable insulation resistance is degraded, causing an error. Where multiple actuators are used to complete a control action, terminations are incorrect.
Control action correctly sent and received, but actuator(s) does not respond	Mechanical elements in the actuator(s) are blocked, fouled, frozen, not latched, or disconnected. Motive force is insufficient, blocked, or not available (e.g., pneumatic pressure, or hydraulic pressure). Electric power is insufficient, blocked, or not available. Electrical elements in the actuator(s) are open or shorted to ground, or power is not applied.
Actuator(s) respond but control action is not applied to or received by the controlled process	The actuator(s) is disconnected or isolated from the actuated process element. The actuated process element is isolated or blocked.

Failure in Control Path Loss Scenario Types	Example Loss Scenario Causes
Control action is correctly received, but the actuator(s) response is inadequate	Mechanical elements in the actuator(s) are stuck, loose, or worn (e.g., excessive backlash). Hydraulic or pneumatic elements in the actuator(s) are stuck, leaking, or leaking by. Electrical elements in the actuator(s) are aged and are not capable of providing sufficient electromagnetic or electromechanical force.
Actuator(s) respond but control action is not adequately applied to or received by the controlled process	When actuation depends on a timed sequence of actuator responses, the responses are applied out of order or the timing is incorrect. The actuator(s) response is too slow, causing inadequate controlled process performance. The actuator(s) response is too fast, causing damage to controlled process elements (e.g., water hammer). The actuator(s) motive force is too high, causing damage to actuated process elements. The actuator(s) motive force is too low, causing insufficient actuation of actuated process elements. The actuator(s) is not configured to actuate the full range of the actuated element.
Control action is not sent, but actuator(s) act as if it had been sent	Another controller sends or provides its own control action (e.g., a human at the actuator).

Failure in Control Path Loss Scenario Types	Example Loss Scenario Causes
Actuator or control pathway element is not capable of providing an adequate response	Actuator or control pathway element is exposed to environmental conditions beyond its specifications. Actuator or control pathway element does not meet its specified environmental capability. Actuator mechanical, electrohydraulic, or electromechanical capability is insufficient. Actuator frequency response is insufficient. The actuator(s) is not capable of actuating the full range of the actuated element.

A controlled process is any plant system, plant subsystem, or set of plant systems that can be influenced by a controller (automated or human). 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 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. Table 7 provides example loss scenarios incurred due to failures in the control path. This table is NOT a complete list of Loss Scenario causes and should NOT be utilized in that manner.

Table 7 – Inadequate Controlled Process Loss Scenario Types [12, 27]

Failures in Controlled Process Loss Scenario Types	Example Loss Scenario Causes
Assumptions about the controlled process are inadequate	The controlled process variables (e.g., flow, level, pressure, temperature, reactor power, electrical power, chemistry, etc.) are outside the range of conditions assumed in the controller process model design. The controlled process is not available, or its operating mode is different than assumed. The controlled process is being adversely influenced by another process.

Failures in Controlled Process Loss Scenario Types	Example Loss Scenario Causes
Equipment under control is faulted	Mechanical process element is disconnected, loose, fouled, frozen, worn, broken, or slow to respond. Actuated element is physically locked in one position, blocked, stuck, or separated from its actuator. Actuated element is disconnected or isolated from the controlled process. Actuated element is worn, fouled, or degraded.
Equipment under control is not capable or designed for necessary response	Fluid elements (e.g., pumps, valves) have insufficient or ineffective flow characteristics. Electromechanical elements have insufficient capacity or motive force. Isolation elements have insufficient capability. Equipment under control has insufficient time or frequency response.

4.2.2 Identify Systematic Control Methods

A systematic control method is a method that can be implemented to eliminate or mitigate a loss scenario. For each HSSSR system loss scenario, systematic control methods are created to eliminate or mitigate the loss scenario.

The identification of 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 particular controller) or it can span multiple elements in the HSSSR system (e.g., multiple controllers or controller and equipment under control). This is established by identifying Relationship Sets in accordance with Section 4.2.3.

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 as described in Section 4.2.3.

4.2.3 Score Systematic Control Methods

A scoring method is used as a tool to perform a qualitative assessment of the control method effectiveness. A scoring method removes potential bias in the qualitative assessment. Each control method is evaluated separately for its control method effectiveness and in combination when more than one control method is applied to an I&C element or relationship set of I&C elements.

There are two parts to the scoring control method effectiveness:

1. Pre-scored systematic control methods for the control algorithm commensurate with the Risk Reduction Objective.

2. Score each control method individually to determine if its effectiveness and compare the score to the benchmark set for the Risk Reduction Objective.

This document is intended to provide the acceptable criteria for a scoring system to evaluate systematic control methods to allocate to loss scenarios. Actual control method scoring attributes, baseline values, and RRO thresholds shall be defined by implementing procedures (i.e. EPRI HAZCADS [11] and DRAM [12]).

4.2.3.1 Pre-scored Systematic Control Methods

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 [13]. Similar to how IEC 61508-3, Annex A [13] is formatted in which a given technique or measure listed in the Annex is designated has Highly Recommended (HR), Recommended (R), No Recommendation (-), or Not Recommended (NR) 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 Objective.

For each systematic control method synthesized from IEC 61508-3, Annex A [13], designated as HR for a given Risk Reduction Objective, 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.

The disposition of these control methods would be documented and provided as part of a LAR submittal.

4.2.3.2 Control Method Scoring Process

The control method scoring 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 and provides the relative effectiveness of a control measure at eliminating/mitigating CCF.

For each systematic loss scenario, potential control measures are identified, each control measure is evaluated individually using a scoring process to determine the relative effectiveness, then control measures can be applied individually (or in combination) to match the level of rigor dictated by the RRO. One control method (or combination of control methods) can mitigate multiple loss scenarios.

Control method effectiveness 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 control method effectiveness 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 control method effectiveness is suitable for this process because it allows for the establishment of a reasonable scale for control method effectiveness when combining the attributes. Using a scientific scoring process for this qualitative assessment of control method effectiveness reduces the potential for human bias that may enter into the assessment.

It is the combining of the control method attributes (e.g. type and strength) that assesses the control method effectiveness. A set of attributes are used to objectively define critical characteristics of a control method. For example, control method attributes of type and strength may be utilized to calculate control method effectiveness. 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 measure 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 a Risk Reduction Objective.

These baseline scores for control method attribute describe the level of effectiveness of each. However, the overall control method effectiveness is the combination of ALL attributes. The algorithm that is used to combine these control method attribute scores to assess the control method effectiveness is:

$$CME = Log_2(Att_1 * Att_2 * ..... Att_n * Constant)$$

Where:

CME is control method effectiveness

Att_1 is Attribute 1 baseline score

Att_2 is Attribute 2 baseline score

Att_n is Attribute *n* baseline score

Constant is used as a scaling factor that provides consistent boundaries and forces a lower CME to 0.10 (to avoid a result of 0).

A CME score is not probabilistic. It is a deterministic measure that simply bounds the qualitative space of control method effectiveness on a preferred scale starting at 0.1.

For each systematic loss scenario, the analysis team decides what systematic control method or methods to apply. For each loss scenario, the control method effectiveness for each individual control method identified to eliminate or mitigate that loss scenario is calculated. The result is then compared to the requisite control method effectiveness for the Risk Reduction Objective.

If all individual control method effectiveness scores meet or exceed the requisite control method effectiveness for the Risk Reduction Objective, then the risk reduction objective is achieved for the system.

If an individual control method effectiveness score does not meet or exceed the requisite control method effectiveness for the Risk Reduction Objective, then additional control methods are added and combined in attempt to achieve the requisite control method effectiveness.

4.2.4 Create Relationship Sets

An identified Relationship Set provides an opportunity to apply the same control methods to multiple components. The same opportunity arises when one or more control methods can mitigate multiple loss scenarios (which, in turn, can affect multiple components).

The identification of relationship sets should improve the efficiency of control method allocation and scoring. There can be many-to-many (as opposed to one-to-one, many-to-one, etc.) associations of I&C components, loss scenarios, and relationship sets.

A relationship set can be composed of I&C elements that share certain characteristics. Each subsystem can be a relationship set because the elements in each subsystem are identical, have identical failure rates, and can have identical diagnostic test coverage, diagnostic test intervals, periodic test coverage, periodic test intervals, etc.

4.2.5 Allocate Systematic Control Methods

For each systematic loss scenario, the analysis team decides what systematic control method or methods to apply to eliminate or mitigate the loss scenario. One control method can mitigate multiple loss scenarios. A control method is allocated to an I&C element or a relationship set of I&C elements to eliminate or mitigate the loss scenario. A systematic control method is allocated through the design process as part of the design or plant operational policies (if non-technical control methods are utilized). Systematic control methods utilized shall be commensurate with the Risk Reduction Objective established in Section 4.1.1. HSSSR systems with RRO A should utilize systematic control methods with high effectiveness scores. If a single systematic control method does not match the level of rigor established by the RRO threshold, multiple control methods can be allocated to a loss scenario or relationship set that do match the RRO threshold.

A combined control method effectiveness 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 RRO threshold.

The equation for combining the effectiveness of control methods is:

$$CCME = \sum_{i=1}^{n} CME_{(i)} * \left(\frac{2}{3}\right)^{i-1}$$

Where:

CCME = Resulting control method effectiveness when the effectiveness of multiple control methods is combined.

CME_i = the i^{th} control measure effectiveness being combined in a series starting with the highest score and working down to the lowest effectiveness score

n = the number of control methods, each with its own control method effectiveness score, applied to an I&C element or relationship set of I&C elements.

$(2/3)^{i-1}$ = the geometrical weighting factor

When a combined control method effectiveness score meets or exceeds the requisite threshold for the Risk Reduction Objective, then the risk reduction objective is achieved. If the combined control method effectiveness score does not meet or exceed the requisite RRO benchmark for the HSSSR system or subsystem under analysis, the risk due to one or more UCAs related to that system or subsystem is not mitigated, and the result is a set of residual loss scenarios. and related UCAs that must be evaluated for potential design changes.

4.2.6 RPS Example

The following sections continue the RPS example from Section 4.1.3 utilizing UCAs, Hazards, and Losses identified in that example. Note this example is high-level and intended to provide contextual support of the process described herein. Actual implementation requires greater design detail, multidisciplinary team engagement, etc.

4.2.6.1 Develop Loss Scenarios

The following tables provides example Loss Scenarios for RPS-UCA1 through RPS-UCA3.

Table 8: RPS-UCA1 Loss Scenario Examples [12]

RPS-UCA1: RPS does not provide automatic reactor trip when heat addition (reactor power) exceeds heat removal capability (RCS conditions), leading to a fuel damage safety limit or a pressure integrity safety limit **[RPS-H1, RPS-H2]**	
LS-1	A random hardware failure of the RPS controller inhibits a trip condition when heat addition (reactor power) exceeds heat removal capability (RCS conditions),leading to a fuel damage safety limit or a pressure integrity safety limit.
LS-2	RPS controller believes heat addition (reactor power) is less than heat removal capability (RCS conditions) when the opposite is true.

LS-2.1	Reactor power or RCS conditions feedback is bypassed by operator and control algorithm continues reading last known good values.
LS-2.2	The sensed reactor power is accurate but not sent to the RPS controller, and reactor power is greater than the heat removal capability of the RCS.
LS-2.2.1	The reactor power sensing equipment is configured for a test or maintenance activity that locally blocks its output.
LS-3	The RPS controller input module for acquiring reactor power feedback or information is dead, disabled, or configured incorrectly.
LS-4	Reactor power feedback pathway terminations are incorrect or blocked.
LS-5	Reactor power is not sensed, and reactor power is greater than the heat removal capability of the RCS.
LS-6	RCS conditions are not sensed, and RCS heat removal capability is less than reactor power.

Table 9: RPS-UCA2 Loss Scenario Examples [12]

RPS-UCA2: RPS provides automatic reactor trip when heat addition (reactor power) does not exceed heat removal capability (RCS conditions) **[RPS-H3]**	
LS-7	A random hardware failure of the RPS controller causes a trip condition when heat addition (reactor power) does not exceed heat removal capability (RCS conditions).

Table 10: RPS-UCA3 Loss Scenario Examples

RPS-UCA3: RPS provides automatic reactor trip too late - after heat addition (reactor power) exceeds heat removal capability (RCS conditions), leading to a fuel damage safety limit or a pressure integrity safety limit **[RPS-H1, RPS-H2]**	
LS-8	RPS controller provides trip command more than 100 msec after heat addition (reactor power) exceeds heat removal capability (RCS conditions)**.**
LS-8.1	The controller scan time is set to a value greater than 100 msec.
LS-8.2	A flawed control algorithm is uploaded to the RPS controller.

LS-9	Reactor power information is delayed beyond 150 msec, and reactor power is greater than the heat removal capability of the RCS

There can also be loss scenarios that address multiple UCAs. Table 11 provides examples of these types of Loss Scenarios with the applicable UCAs in bracketed text.

Table 11: Multiple UCAs Loss Scenarios Examples [12]

LS-10	Power supply voltage, current or frequency conditions outside the ranges specified for the RPS controller equipment result in any of the RPS UCAs. **[RPS- UCA1, RPS-UCA2, RPS-UCA3, RPS-UCA4]**
LS-11	An HVAC failure or failure of a local fan causes temperature and/or humidity conditions outside the ranges specified for the RPS controller equipment that result in any of the RPS UCAs. **[RPS-UCA1, RPS-UCA2, RPS-UCA3, RPS- UCA4]**
LS-12	A failure in a human system interface (HSI) causes an erroneous command that results in any of the RPS UCAs. **[RPS-UCA1, RPS-UCA2, RPS-UCA3, RPS- UCA4]**

4.2.6.2 Identify Control Methods

Table 12 shows RPS-UCA1, Loss Scenario 2.1, with possible control methods. These control methods can be evaluated for strength to determine effective methods (single or combined) to eliminate/mitigate the potential for the loss scenario.

Table 12: Control Method Examples [12]

RPS-UCA1: RPS does not provide automatic reactor trip when heat addition (reactor power) exceeds heat removal capability (RCS conditions), leading to a fuel damage safety limit or a pressure integrity safety limit **[RPS-H1, RPS-H2]**	
LS-2.1 Reactor power or RCS conditions feedback is bypassed by operator and control algorithm continues reading last known good values	
CM1-LS-2.1	The RPS shall have sufficient redundancy (channels) to provide automatic reactor trip when heat addition (reactor power) exceeds heat removal capability (RCS conditions), to allow the operator to bypass RCS conditions in one channel and still meet the single failure criterion in IEEE Std 603.
CM2-LS-2.1	By administrative control, only one RPS channel shall be bypassed for RCS conditions.

CM3-LS-2.1	The RPS shall perform coincidence logic on redundant channels providing automatic reactor trip signals when heat addition (reactor power) exceeds heat removal capability (RCS conditions).
CM4-LS-2.1	The RPS shall initiate an automatic reactor trip when the minimum number of operable channels provide a reactor trip signal when heat addition (reactor power) exceeds heat removal capability (RCS conditions).
CM5-LS-2.1	The RPS shall read the bypass status of RCS conditions.
CM6-LS-2.1	The RPS shall remove from coincidence logic the reactor trip signal, when heat addition (reactor power) exceeds heat removal capability (RCS conditions), bypassed in one redundancy by the operator.

5 LICENSE AMENDMENT CONSIDERATIONS

The licensee will need to demonstrate the adequacy of the systematic hazard analysis based on STPA and demonstrate the plant-specific PRA meets the prerequisites in Section 3.3.1.

The licensee's LAR would need to address the five guiding principles for risk-informed decision taking into consideration the discussion in Section 3.3. The licensee's responsibility for meeting NRC regulatory criteria for an HSSSR system are unchanged when using this process.

The licensee will need to summarize the approach and results of the NEI 20-07 process in the LAR. The HSSSR System architecture submitted with the LAR would reflect the results of the NEI 20-07 process. The detailed NEI 20-07 PRA and STPA analyses would be made available to the NRC for audit as part of the LAR review. The STPA analyses need to document traceability from STPA losses, hazards, and unsafe control actions (Part I) to STPA loss scenarios and control methods (Part II).

The analyses produced by the NEI 20-07 process for the HSSSR system needs to meet the quality requirements of 10 CFR 50 Appendix B [3]:

- Criteria III, Design Control,
- Criteria VI, Document Control
- Criteria XVII, Quality Assurance Records

If the DI&C-ISG-06 Alternate Review Process [9] is used for the LAR, then there will be restrictions to the HSSSR System Design Changes as defined in that process.

6 RECOMMENDATIONS AND CONCLUSIONS

This approach to addressing HSSSR systematic failures including CCF begins by establishing a Risk Reduction Objective for the HSSSR system. To assess if the HSSSR system Risk Reduction Objective is

achieved, a hazard analysis process developed by MIT, STPA, is used to identify HSSSR system losses, hazards, unsafe control actions, and loss scenarios. Control measures are then established to eliminate or mitigate the loss scenarios. Using an established scoring methodology, the effectiveness of these control measures is assessed and compared to a benchmark established for the Risk Reduction Objective. Once these control measures reach that benchmark then these control measures (depending on the type) become requirements for implementation in the HSSSR system.

This approach is a risk-informed, performance-based approach to assessing the control measures in place to protect the HSSSR system from systematic failure including CCF. The underlying STPA process has been adopted in many other safety industries such as automotive, aviation, and defense and proven effective at identifying and eliminating/mitigating hazards to prevent losses.

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, USNRC ADAMS Accession # ML18269A259
10. EPRI Report 3002011816, Digital Engineering Guide - Decision Making Using Systems Engineering
11. EPRI Report 3002016698, HAZCADS: Hazards and Consequences Analysis for Digital Systems, Revision 1, July 2021
12. EPRI Report 3002018387, DRAM: Digital Reliability Analysis Methodology, Revision 0, July 2021
13. IEC 61508, Edition 2.0, 2010-04, Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems
14. IEEE 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations”
15. IEEE 603-1991, “Criteria for Safety Systems for Nuclear Power Generating Stations”

16. MIT Partnership for Systems Approaches to Safety and Security (PSASS), 2021 STAMP Workshop General Information (http://psas.scripts.mit.edu/home/2021-stamp-workshop-information/)

17. 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

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

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

20. Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Rev. 2, May 2011

21. Regulatory Guide 1.200, "Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities," Rev. 3, Dec. 2020

22. Regulatory Guide 1.201, "Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance," Rev. 1, May 2006

23. 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)

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

25. SRM/SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," July 21, 1993

26. 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)

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

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

APPENDIX A. RELEVANT NRC REGULATORY FRAMEWORK

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

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

A.1. 10 CFR 50.54(jj) [5], 10 CFR 50.55a(h) [6]

IEEE 603-1991 [15] or IEEE 279 -1971 [14] as incorporated by reference requires, in part, that components and modules shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program.

It is assumed in this document that the HSSSR system is developed in accordance with these regulatory criteria. Section 4.2.5.1, “Pre-scored Systematic Control Methods” are techniques and measures that may, in some cases, exceed the current regulatory guidance for meeting these regulatory criteria.

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

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

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

Since HSSSR systems are considered of high significance regarding the importance of safety functions to be performed, this GDC applies. It is assumed in this document that the HSSSR system is developed in accordance with these regulatory criteria. Section 4.2.5.1, “Pre-scored Systematic Control Methods” are techniques and measures that may, in some cases, exceed the current regulatory guidance for meeting these regulatory criteria.

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

It is assumed in this document that the HSSSR system is developed in accordance with the recognized industry codes and standard in 10 CFR 50.54(jj) [5], 10 CFR 50.55a(h) [6] - IEEE 603-1991 [15] or IEEE 279 -1971 [14]. Section 4.2.5.1, “Pre-scored Systematic Control Methods” are techniques and measures that may, synthesized from the industry standard IEC 61508 Part 3, normative Annex A which is a recognized safety standard in the petrochemical industry.

GDC 1 also states, in part, “A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of

structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit."

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

A.2.2. GDC 13, "Instrumentation and Control"

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

The HSSSR system requirements development needs to address the functional requirements stated in this GDC. The control measures generated from the STPA hazard analysis process ensures that HSSSR systematic failures like CCF do not prevent the HSSSR system from performing its safety function.

A.2.3. GDC 19, "Control Room"

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

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

A.2.4. GDC 20, "Protection System Functions"

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

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

A.2.5. GDC 21, "Protection System Reliability and Testability"

GDC 21, “Protection System Reliability and Testability” states, “The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.”

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

A.2.6. GDC 22, “Protective System Independence”

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

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

A.2.7. GDC 23, “Protective System Failure Modes”

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

The scope of NEI 20-07 is HSSSR DI&C systems and these systems need to meet this GDC. The STPA process described in this document identifies the potential unsafe control actions and the loss scenarios that can cause these unsafe control actions. Failing in the safe state is a consideration in the STPA process.

A.2.8. GDC 24, “Separation of Protection and Control”

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

It is assumed in this document that the HSSSR system must meet this regulation. The STPA process described in this document takes into account all interfaces to the HSSSR system to effectively evaluate the potential systematic failures including CCF.

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

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

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

A.2.10. GDC 28, "Reactivity Limits"

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

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