NEI and NRC Tabletop (PWR Modernization Example)

The following information is to support the ongoing review of NEI 20-07. The information within this report is hypothetical. The primary purpose of this report is to obtain feedback from NRC staff regarding the use of NEI 20-07 to implement the NRC policy on digital instrumentation and control (DI&C) Common Cause Failure (CCF), SRM-SECY-22-0076, using the risk-informed pathway.

NRC Tabletop (PWR Modernization Example)

1. Introduction

1.1. Purpose

The purpose of this document is to perform an analysis related to the Sample Plant (SP) Reactor Protection System (RPS) being implemented as part of the SP Modernization Project. The RPS will be implemented using the Sample Platform, which is a digital platform that has been reviewed and approved by the NRC for use for safety-related systems. The analyses are:

- Hazards and Consequence Analysis that evaluates plant and system losses, hazards, and Unsafe Control Actions (UCAs). This analysis will define the impacts of a potential Common Cause Failure (CCF) of the Sample Platform on the plant as measured by Core Damage Frequency (CDF) and Large Early Release Frequency (LERF). Refer to Section 3 for this analysis, which considered the guidelines of NEI 20-07 (Reference). This analysis identifies which portions of the architecture are risk significant. Refer to Section 2 for descriptions of the RPS architecture and its features.
- Digital Reliability Analysis identifies scenarios in which a systematic failure such as a CCF may lead to a plant loss and evaluates Control Methods that protect, detect and respond/recover to the identified scenarios. Refer to Section 4 for this analysis.

These analyses will identify digital system requirements that will be included in the overall design of the NSP Modernization Project as developed digital design guidance (EPRI Digital Engineering Guideline) and documented by the Standard Design Process (IP-ENG-001) and digital design procedure (NISP-EN-04).

1.2. Scope

This document addresses the expected analysis from the NRC Standard Review Plan (SRP), NUREG-0800, Chapter 7, Branch Technical Position (BTP) 7-19. The scope of the analysis is the RPS. The RPS monitors the plant for abnormal conditions and initiates reactor trip when predefined limits are exceeded.

2. Losses and Hazards

Section 2 identifies the scope of analysis, adequacy of the DI&C platform, stakeholder losses and system hazards associated with the sample RPS replacement project. As a result, the analysis has demonstrated that relevant Stakeholder Losses and System Hazards have been adequately identified to support a safety determination.

- Sections 2.1 through 2.4 provides system scope and design information that is needed to understand the system functions, platform compliance with requirements, and DI&C design. These sections demonstrate the full scope of the modification and system interactions that are relevant to the analysis.
- Section 2.5 identifies the key criteria needed for a safety determination. This analysis technique is consistent with the NRC accepted safety goals and existing safety criteria for risk-informed applications (Regulatory Guide 1.174). The SP Modernization Project has

identified many Stakeholder Losses; however, only Stakeholder Losses relevant to the safety criteria are identified within the scope of this analysis.

- Section 2.6 identifies System Hazards that may lead to the previously identified Stakeholder Losses. These System Hazards represent system states that in a worst-case scenario may adversely affect the plant.

As a result of the EPRI DEG and HAZCADS analysis documented in SP Modernization System Design Document and SP Modernization HAZCADS Worksheets, the project team has comprehensively analyzed all potential Stakeholder Losses and System Hazards relevant to the replacement of the Sample Plant RPS. The project team consists of subject matter experts in Probabilistic Risk Analysis (PRA), Engineering, Operations, Maintenance and Licensing. The analysis starts at a high level of abstraction that is intended to bound stakeholder losses and system hazards. The project team iterates through this diagnostic process as the design has progressed starting with an initial conceptual design and progressing through the design detailed in Section 2.3. The following sections identify key findings from these processes that are relevant to the safety determination for the SP Modernization Project.

2.1. System Scope and Interfaces

The Reactor Protection System automatically keeps the reactor operating within a safe region by shutting down the reactor whenever the limits of the region are approached. The safe operating region is defined by several considerations, such as mechanical/hydraulic limitations on equipment and heat transfer phenomena. Therefore, the RPS keeps surveillance on process variables that are directly related to equipment mechanical limitations, such as pressure and pressurizer water level (to prevent water discharge through safety valves and uncovering heaters), and on variables that directly affect the heat transfer capability of the reactor (e.g., flow and reactor coolant temperatures). Still other parameters utilized in the RPS are calculated from various process variables. In any event, whenever a direct process or calculated variable exceeds a setpoint, the reactor will be shut down to protect against either gross damage to fuel cladding or loss of system integrity which could lead to release of radioactive fission products into the containment.

The following systems make up the RPS:

- Process instrumentation and control system.
- Nuclear instrumentation system.
- Solid-state logic protection system.
- Reactor trip switchgear.
- Manual actuation circuit.

The RPS consists of sensors, which monitor various plant parameters when connected with analog circuitry consisting of four redundant channels, and of digital circuitry, consisting of two redundant logic trains, which receives inputs from the analog protection channels to complete the logic necessary to automatically open the reactor trip breakers.

Either of the two trains, A or B, can open a separate and independent reactor trip breaker, RTA and RTB, respectively. The two trip breakers, in series, connect three-phase ac power from the rod drive motor generator sets to the rod drive power cabinets. During plant power operation a dc undervoltage coil on each reactor trip breaker holds a trip plunger out against its spring, allowing the power to be available at the rod control power supply cabinets. For reactor trip, a loss of dc voltage to the undervoltage coil as well as energization of the shunt trip coils trips open the breaker. When either of the trip breakers opens, power is interrupted to the rod drive power supply, and the control and shutdown rods fall into the core. The rods cannot be withdrawn until the trip breakers are manually reset. The trip breakers cannot be reset until the abnormal condition which initiated the trip is corrected. Bypass breakers BYA and BYB are provided to permit testing of the trip breakers.

The scope of the SP Modernization Project is to replace the solid-state logic protection system with a new digital platform. Other RPS sub-systems maintain their existing interfaces will continue to provide input/output (I/O) interface with the new digital Sample Platform control system. The new digital Sample Platform control system is compatible with the existing RPS sub-systems as demonstrated in the SP Modernization Project System Design Document and SP Modernization License Amendment Request Package.

2.2. DI&C Platform Adequacy

The Sample Platform has been reviewed and accepted by the NRC as a qualified digital safety system as documented in Sample Platform Topical Report which affirms the digital systems compliance with regulatory requirements. The Sample Platform incorporates key features that support defense-in-depth requirements:

- Deterministic logic: The platform uses deterministic algorithms, which limits the possibility of unpredictable behavior.
- Redundancy: Channels are designed to operate independently, enhancing system resilience to faults.
- Extensive self-diagnostics: The system continuously monitors its own performance and can alert operators to anomalies.
- *[Insert any other platform level capabilities that support system-level defense-in-depth. Examples include:*
    - *Built-in platform diversity*
    - *Architecture]*

The Sample Platform Topical Report demonstrates compliance with applicable criteria within IEEE 603-1991. Application-Specific Action Items (ASAI) are addressed in the License Amendment Request (LAR) submittal. The Sample Plant License Amendment Request Package provides additional information demonstrating the Sample Platform's compliance in IEEE 603-1991 and IEEE 7-4.3.2 2016 for this unique application.

2.3. DI&C Design

For the purposes of this analysis, Figure 1 is used to analyze potential vulnerabilities to CCF in the RPS architecture. The architecture is made up of two channels of redundant sensors for each division and two divisions labeled A and B.

- Division A with Channels A1X and A1Y
- Division B with Channels B1X and B1Y

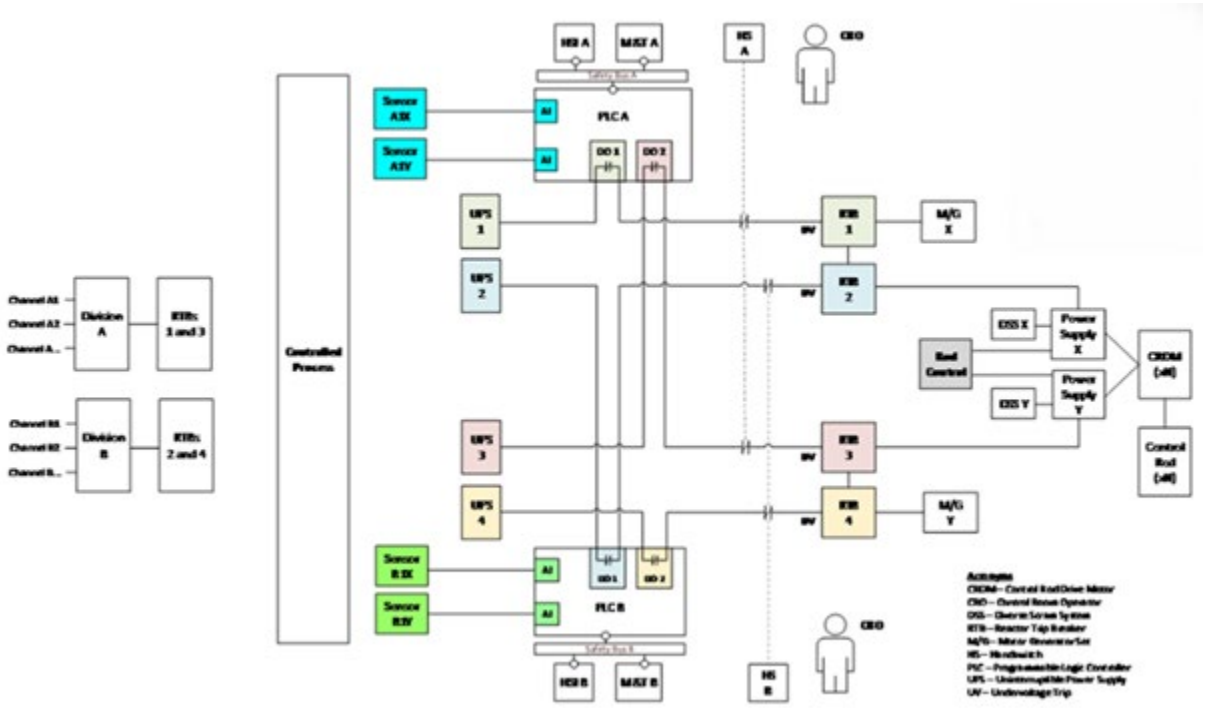

Figure 1: Sample Platform Architecture

The sample plant is designed to initiate a trip command for the following scenarios:

- High reactor power
- High reactor power flux rate
- High RCS pressure
- Low RCS pressure
- Overtemperature ΔT
- High RCS temperature
- High Reactor Building pressure
- Loss of both Main Feedwater pumps
- Main Turbine trip
- Loss of any Reactor Coolant pump

Refer to the SP Modernization System Design Document and License Amendment Request Package for additional detail regarding the DI&C design.

2.4. Control Structure Hierarchy

Figure 2 provides a control structure hierarchy for the Sample Plant RPS. The following description provides the system elements relevant to the digital platform. SP Modernization HAZCADS Worksheets provide a complete description of the Control Structure Hierarchy. To address digital CCF, the following system elements are considered:

- Feedback
  - Reactor Power
  - RCS Flow
  - RCS Pressure
  - RCS Temperature
  - Reactor Building Pressure
  - Main Turbine Trip
  - Main Feedwater Pump Trip
  - Reactor Coolant Pump Status
- Controllers
  - RPS Division 1 (RPS1)
  - RPS Division 2 (RPS2)
- Control Actions
  - Automatic Trip Division 1 (AT1)
  - Automatic Trip Division 2 (AT2)
- Controlled Process
  - Reactor Trip Relay 1
  - Reactor Trip Relay 2
  - Reactor Trip Relay 3
  - Reactor Trip Relay 4
- Control Actions from other Controllers
  - Channel Trip (Operator)
  - Test (Operator)
  - Bypass (Operator)
  - Setpoints (Engineer)
- Feedback to other Controllers
  - Trip Status (Operator)
  - Fault Alarms (Operator)
  - Bypass Status (Operator)
  - Logs (Engineer)

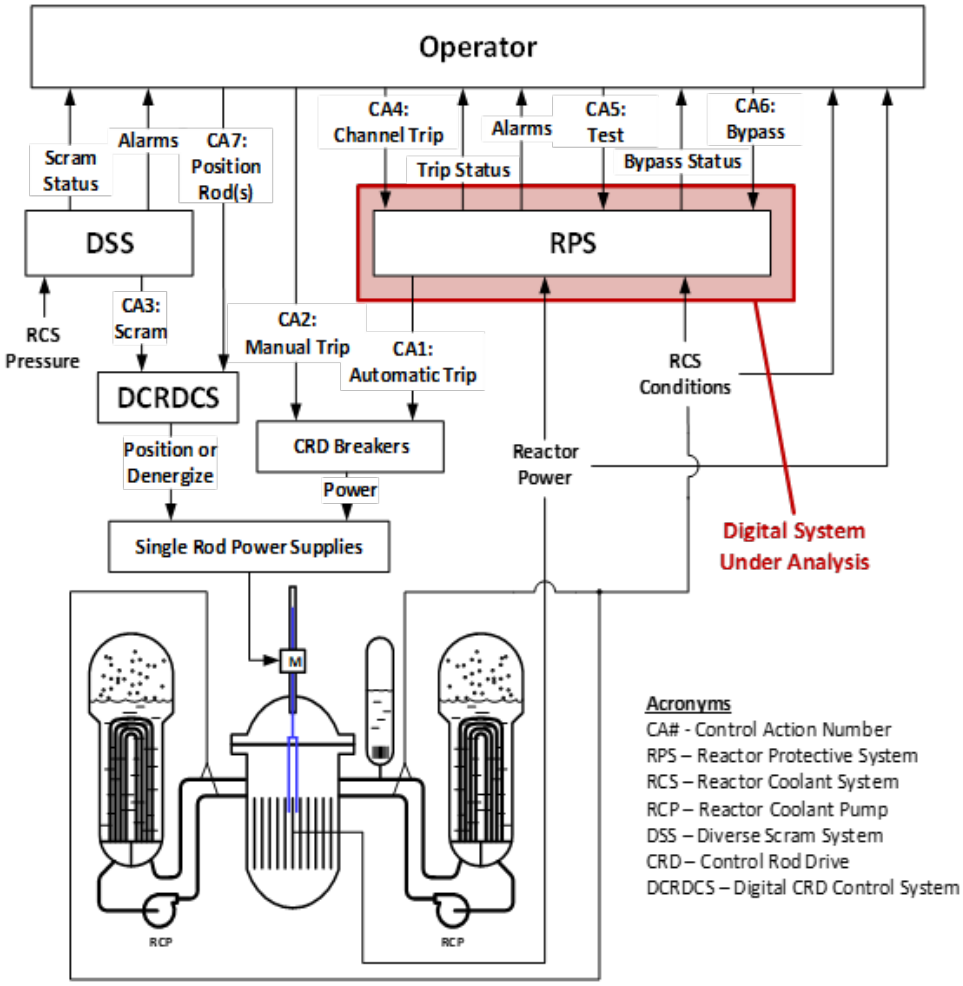

Figure 2: Sample Plant RPS Control Structure Hierarchy

2.5. Stakeholder Losses

SP Modernization HAZCADS Worksheets document all stakeholder losses addressed by the analysis which include stakeholder losses not relevant the NRC accepted safety goals (e.g., loss of revenue). This analysis is focused on the Stakeholder Losses "L1: Core Damage" and "L3 Containment Damage" which is consistent with Regulatory Guide 1.174 metrics for risk-informed decision-making. This analysis utilizes Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) as risk metrics associated with "radiological impact." Refer to Section 3.2 and 3.3 for additional risk metric information.

The SP Modernization HAZCADS Worksheets addresses other stakeholder losses that are not relevant to a safety determination (e.g., loss of revenue). Associated hazards, unsafe control actions, loss scenarios, and applied control methods that are not associated with L1 or L3 are excluded from the results documented within this report; however, these have been addressed commensurate with their risk. All hazards and unsafe control actions associated with L1 and L3 are evaluated to determine the impact of a potential CCF.

2.6. System Hazards

[Applicant] identified two (2) hazards associated with the SP Modernization Project:

- RPS-H1: RPS does not initiate reactor trip
- RPS-H2: RPS initiates reactor trip

RPS has two primary states: no reactor trip and reactor trip. Each of these states can present hazardous conditions in a worse case environment. For example, if the Reactor Coolant System (RCS) is unable to sufficiently remove heat and the RPS does not initiate a reactor trip, then the plant is in a potentially hazardous state. Likewise, if the RCS is sufficiently removing heat and the RPS initiates a reactor trip, then the plant is also in a potentially hazardous state. These conditions may present themselves in any mode of operation. The table below displays the identified hazards and their potential stakeholder losses. As discussed in Section 2.5, L1 and L3 (highlighted in the table below) are the Stakeholder Losses associated with nuclear safety.

Table 1: Sample Plant RPS Stakeholder Losses and System Hazards

System Under Analysis		Losses				
Reactor Protection System		L1: Core Damage	L2: RCS Damage	L3: Containment Damage	L4: Loss of Revenue	L5: Reputational Damage
System Hazards	H1: RPS does not initiate reactor trip	X	X	X	X	X
	H2: RPS initiates reactor trip				X	X

The SP Modernization Project replaces the RPS; therefore, only system hazards associated with the RPS are applicable. The hazards identified above represent the two system states that could create a stakeholder loss. Refer to the SP Modernization HAZCADS Worksheets for additional information.

3. Common Cause Failure Analysis

Section 3 identifies Unsafe Control Actions, identifies PRA model characteristics needed for risk-informed decision-making, and evaluates the risk-significance of a postulated CCF to the Sample Plant. As a result, the analysis has demonstrated that UCAs deemed postulated CCF have been

adequately identified and their risk-significance to the plant has been determined to support a safety determination.

- Section 3.1 identifies RPS UCAs consistent with the scope of the SP Modernization Project and evaluates each to determine whether it is considered a postulated CCF. The UCAs deemed postulated CCFs are the focus of the remaining sections of analysis.
- Section 3.2 evaluates key characteristics of the PRA model to determine it's acceptability for risk-informed decision-making. The information evaluated within this section is consistent with the NRC accepted safety goals and existing safety criteria for risk-informed applications (Regulatory Guide 1.174).
- Section 3.3 provides the results of the PRA sensitivity analysis used to determine the risk-significance of the RPS. These results inform the Control Effectiveness Profile used to determine the sufficiency of applied Control Methods.

As a result of the EPRI DEG and HAZCADS analysis documented in SP Modernization System Design Document and SP Modernization HAZCADS Worksheets, the project team has comprehensively analyzed postulated CCFs relevant to the replacement of the Sample Plant RPS. The project team consists of subject matter experts in Probabilistic Risk Analysis (PRA), Engineering, Operations, Maintenance and Licensing. The analysis identifies all potential control actions and identifies unsafe states for each that may lead to a System Hazard. The project team iterates through this diagnostic process as the design has progressed starting with an initial conceptual design and progressing through the design detailed in Section 2.3. The following sections identify key findings from these processes that are relevant to the safety determination for the SP Modernization Project.

3.1. Unsafe Control Actions Deemed Postulated CCFs

The Control Structure Hierarchy described in Section 2.4 provides the control actions (as indicated by downward arrows) associated with the sample RPS modification. Each control action has been evaluated to determine if it leads to a system hazard in the following potentially unsafe states:

- Control Action is not provided when necessary.
- Control Action is provided when not necessary.
- Control Action is provided too early / too late / out of order
- Control Action is stopped too soon or applied too long

The results of this analysis are documented in SP Modernization HAZCADS Worksheets. The Automatic Trip control action is the only control action associated with the digital controllers impacted by the sample RPS replacement project. All other Control Actions are associated with a human controller (i.e., Engineer or Operator) or interfacing system (e.g., Diverse SCRAM System). As such, the following four (4) Unsafe Control Actions (UCAs) are identified to evaluate as a postulated CCF:

RPS-UCA1: RPS does not provide an automatic reactor trip when there is an initiating event.

RPS-UCA2: RPS provides an automatic reactor trip when there is not an initiating event.

RPS-UCA3: RPS provides an automatic reactor trip too late, after there is an initiating event.

RPS-UCA4: RPS stops providing an automatic reactor trip too soon - before the reactor trip breakers can detect and respond - when there is an initiating event.

RPS-UCA1, UCA3, and UCA4 are postulated CCFs that would result in the loss of a safety function. If one of these UCAs were to occur within both RPS divisions (RPS1 and RPS2), the RPS would not be able to perform its safety function as intended. RPS-UCA2 is a spurious operation resulting from a postulated CCF. If this UCA were to occur within both RPS divisions (RPS1 and RPS 2), the RPS would initiate a reactor trip unnecessarily. This UCA is not associated with L1: Core Damage or L3: Containment Damage. RPS-UCA2 is evaluated in the complete analysis; however, it is not within the scope of regulatory review.

The scope of this modification is limited to the Reactor Protection System which only consists of one (1) control action from the DI&C system; therefore, the selection of RPS-UCA1, UCA3, and UCA4 as postulated CCFs is complete. No other control actions are initiated from the DI&C system. Other control actions from humans or systems that interface with the DI&C system are evaluated as potential loss scenarios that can lead to unsafe conditions for the Automatic Trip control action (e.g., an Operator may set a Bypass that leads to a UCA). These control actions are also evaluated as UCAs but are not within the scope of the digital CCF analysis. The analysis accounts for all control actions within the scope of the modification and the identified potential interfaces.

[Applicant] identified all UCAs associated with the SP Modernization Project in the SP Modernization HAZCADS Data Sheets.

3.2. PRA Information

[Applicant] evaluated the impact of the digital modernization project within the PRA to determine the impact of a postulated CCF. The PRA model used by [applicant], PRA Version 3.4A, has been reviewed and accepted by the NRC to be compliant with Regulatory Guide 1.200 as documented in Sample Plant PRA Acceptance. PRA Version 3.4A represents the current, as-built configuration of the plant. No revisions to the PRA model are required for the sensitivity analysis to be performed. The sensitivity analysis uses a surrogate event, Failure of Automatic Rx Trip Signal (x2), which represents a complete failure of the RPS. Since no event trees or fault trees have been added or modified, there are no changes or additions to uncertainties modeled in the PRA. Two other control actions are modeled in the PRA that impact this modification: Anticipated Trip Without SCRAM (ATWS) and a manual operator reactor trip. These control actions are not impacted by this modification; therefore, no changes to these elements of the PRA have been made.

The Sample Plant License Amendment Request Package demonstrates the SP Modernization Project complies with regulatory requirements. Additionally, the SP Modernization Project

conforms to the [applicant] defense-in-depth philosophy. The project does not reduce nor adversely affect any defense-in-depth layers (e.g., Engineered Safety Features Actuation System, Anticipated Transient Without SCRAM, etc.). Any impacts to safety margin have been evaluated within their associated calculations and addressed within the Sample Plant License Amendment Request Package. [Applicant] strategic engineering will perform system health monitoring on the new digital system in accordance with the Maintenance Rule and as appropriate to detect and respond and recover to Loss Scenarios as determined by the Control Methods described in Section 5.1. Section 3.3 provides the results of the sensitivity analysis performed in support of this modification.

The Failure of Automatic Rx Trip Signal (x2) basic event adequately bounds the impact of the RPS failure. The Automatic Rx Trip Signal is the only control action associated with the SP Digital Modernization Project. This basic event bounds both random and systematic failures (including CCF) in the RPS including control actions from other interfacing systems (e.g., Operator action). System Hazards and UCAs associated with RPS are bounded by the results of this sensitivity analysis.

3.3. Risk Reduction Targets and Control Effectiveness Profiles

Using PRA Version 3.4A, [applicant] performed a sensitivity study to demonstrate the impact of the basic event: Failure of Automatic Rx Trip Signal (x2). The results produced the following results:

- CDF: 1.9×10^{-4}
- LERF: 4.09×10^{-7}

In accordance with NEI 20-07, the follow Risk Reduction Target (RRT) and Control Effectiveness Profile (CEP) are used to evaluate Loss Scenarios and their Control Methods.

Table 2: Sample Plant RPS Risk Sensitivity Analysis

UCA	CDF	LERF	RRT	CEP
RPS-UCA1, UCA3, UCA4	1.9×10^{-4} RRT – A	4.09×10^{-7} RRT – C	A	A

Each UCA listed in the table above inherits the RRT – A and requires Control Methods that meet the CEP - A threshold. These classifications are the most conservative classes within the EPRI DEG, HAZCADS, and DRAM framework. Systematic Loss Scenarios associated with RPS-UCA1, UCA3, or UCA4 inherit these classifications. Refer to SP Modernization Project HAZCAD Data Sheets for additional information.

4. Systematic Loss Scenarios

Section 4 identifies Systematic Loss Scenarios associated with the postulated CCFs (i.e., RPS-UCA1, UCA3, and UCA4). The Systematic Loss Scenarios are categorized as follows:

- Section 4.1 addresses Class 1 Loss Scenarios related to the RPS controller(s)
- Section 4.2 addresses Class 2 Loss Scenarios related to the process feedback
- Section 4.3 addresses Class 3 Loss Scenarios related to the RPS control action
- Section 4.4 addresses Class 4 Loss Scenarios related to the controlled process

Random Loss Scenarios are not addressed within the scope of the CCF analysis; however, Random Loss Scenarios are addressed within the SP Modernization Project Loss Scenario Data Sheets.

As a result of the EPRI DEG, HAZCADS, and DRAM analysis documented in SP Modernization Project System Design Document, SP Modernization Project HAZCADS Worksheets, and SP Modernization Loss Scenario Data Sheets the project team has comprehensively analyzed loss scenarios associated with postulated CCFs relevant to the replacement of the Sample Plant RPS. The project team consists of subject matter experts in Probabilistic Risk Analysis (PRA), Engineering, Operations, Maintenance and Licensing. The Systematic Loss Scenarios identified within this section represent a full control loop and bound potential scenarios that may lead to a postulated CCF. These Systematic Loss Scenarios also identify system interactions with other controllers that may impact a postulated CCF. The project team iterates through this diagnostic process as the design has progressed starting with an initial conceptual design and progressing through the design detailed in Section 2.3. The following sections identify key findings from these processes that are relevant to the safety determination for the SP Modernization Project.

4.1. Class 1 Loss Scenarios

Class 1 Loss Scenarios are indicative of a postulated CCF that occurs within the digital controller itself. As defined, Class 1 Loss Scenarios occur when the required feedback is correct; however, the controller issues a UCA. These Loss Scenarios evaluate specific situations that would drive the UCA. The following high-level class 1 Loss Scenarios were identified in the SP Modernization HAZCADS Data Sheets.

Table 3: Sample Plant RPS High Level Class 1 Loss Scenarios

UCA	Part A	Part B
RPS-UCA1	RPS does not provide an automatic reactor trip when there is an initiating event.	Feedback to RPS correctly indicates there is an initiating event.
RPS-UCA3	RPS provides an automatic reactor trip too late after there is an initiating event.	RPS received feedback that indicates there is an initiating event on time.
RPS-UCA4	RPS stops providing an automatic reactor trip too soon before the reactor trip breakers can detect and respond when there is an initiating event.	RPS received feedback that indicates there is an initiating event on time.

These high-level Loss Scenarios are used to initiate the Loss Scenario analysis. The SP Modernization Loss Scenario Data Sheets detail the full analysis of Class 1 Loss Scenarios identified. The SP Modernization Loss Scenario Data Sheets demonstrate [applicant] has evaluated refined Loss Scenarios associated with:

- Function allocation
- Control algorithm*
- System state*
- Process model
- Interpretation
- Feedback and other information (including other control actions)*

**Loss Scenarios included as an example for the NEI/NRC tabletop*

These refined Class 1 Loss Scenarios provide a bounding set of loss scenarios that consider systematic failures introduced during design engineering and system development that may lead to a postulated CCF during system operations. The scope of this analysis covers the Sample Platform system (hardware and software elements). The following table provides a summary of the refined Loss Scenarios associated with postulated CCFs identified in the SP Modernization Loss Scenario Data Sheets.

Table 4: Sample Plant RPS Refined Class 1 Loss Scenarios

LSDS #	Refined Loss Scenario
LS-1-1	RPS cabinet air temperatures exceed equipment rating by an unspecified amount (fan failure, equipment overheating, blocked vents, insufficient HVAC,…)
LS-1-2	RPS control algorithm provides inadequate control logic.
LS-1-3	RPS receives a Manual Operator Bypass control action from the Control Room Operator (CRO) when RPS is needed.
LS-1-4	*[Left black for NEI/NRC tabletop]*
[…]	*[…]*
LS-1-xx	*[Left black for NEI/NRC tabletop]*

These refined Class 1 Loss Scenarios demonstrated the breadth and depth of the evaluation performed by [applicant]. Refer to the SP Modernization Project Loss Scenario Data Sheets for full details on each of the refined Class 1 Loss Scenarios. An interdisciplinary project evaluated the system elements for Loss Scenarios associated with the Sample Platform.

4.2. Class 2 Loss Scenarios

Class 2 Loss Scenarios are indicative of a postulated CCF that occurs within the plant sensors and their feedback signals. Class 2 Loss Scenarios occur when the required feedback is incorrect

resulting in the controller issuing a UCA. Loss scenarios associated with termination issues are considered random loss scenarios which are not within the scope of the digital CCF analysis.

[Class 2 Loss Scenarios are not included for the tabletop].

4.3. Class 3 Loss Scenarios

Class 3 Loss Scenarios are indicative of a postulated CCF that occurs within the actuators and command signals. Class 3 Loss Scenarios occur when the controller issues the correct control action; however, the control action is received incorrectly resulting in a UCA. Loss scenarios associated with termination issues are considered random loss scenarios which are not within the scope of this analysis.

[Class 3 Loss Scenarios are not included for the tabletop].

4.4. Class 4 Loss Scenarios

Class 4 Loss Scenarios are indicative of a postulated CCF that occurs with the controlled plant equipment. Class 4 Loss Scenarios occur when process feedback is correct, the controller interprets feedback and issues commands correctly, the control action is received correctly; however, the controlled plant equipment still results in a failure.

[Class 4 Loss Scenarios are not included in the tabletop].

5. Control Methods

Section 5 identifies the Control Methods applied to each Systematic Loss Scenario associated with postulated CCFs. Each Control Method is identified as either 'Protect,' Detect,' or 'Respond and Recover.' Additionally, this section describes how the applied Control Methods have adequately addressed the Systematic Loss Scenarios associated with postulated CCFs. No deviations from the EPRI DRAM scoring methodology were used in this application. Lastly, this section demonstrates how Control Methods will be implemented in the design.

5.1. Allocated Control Methods

Attachment 1 demonstrates the systematic control methods allocated to the SP Modernization project. These systematic control methods indicate reliability type (protect, detect, and respond and recover) and demonstrate the evaluated reliability metrics as follows:

- Control Method Strength (CMS)
- Control Method Type (CMT)
- Control Method Configurability (CMC)
- Control Method Verifiability (CMV)

Each Loss Scenario inherited an RRT – A, CEP – A threshold; therefore, the following EPRI DRAM threshold values were used:

Table 5: Sample Plant RPS CEP Thresholds

RRT / CEP	Target CEP Threshold
A	CME ≥ 2.25
B	CME ≥ 1.50

In accordance with EPRI DRAM, if the 'Protect' CME score exceeds the target CEP threshold (i.e., RRT / CEP – A), then the 'Detect' and 'Respond and Recover' CME scores may use the target CEP threshold lower (i.e., RRT / CEP – B). Likewise, if the 'Detect' and 'Respond and Recover' CME scores exceed the target CEP threshold (i.e., RRT / CEP – A), then the 'Protect' CME score may use the target CEP threshold lower (i.e., RRT / CEP – B). Attachment 1 demonstrates:

- Each Loss Scenario
- Protect, Detect and Respond & Recover Control Methods
- Control Method Effectiveness (CME) Score
- Control Method scoring attributes
- Reference to how the control method was implemented

Each Loss Scenario has been adequately addressed in accordance with EPRI DRAM guidance commensurate with the risk of the SP Modernization Project. [Applicant] used Control Method scoring practices defined in EPRI DRAM with no deviations. All scoring calculations, constants and threshold values are consistent with the EPRI approach. The control methods were scored by the design engineering team and reviewed by an interdisciplinary team composed of subject matter experts in Engineering, Operations, and Maintenance.

6. Conclusions

The SP Modernization Project replaces the existing analog RPS solid-state logic system with a new digital Sample Platform control system. As demonstrated in this analysis, the SP Modernization Project team has:

1. Identified relevant Stakeholder Losses and System Hazards
2. Identified and analyzed Unsafe Control Actions to determine postulated CCFs and their risk to the Sample Plant
3. Identified systematic Loss Scenarios that may lead to each postulated CCF
4. Applied Control Methods to protect, detect, and respond & recover from systematic loss scenarios commensurate with the risk significance

The enclosed analysis complies with the guidance provided in Regulatory Guide 1.174, NUREG-0800, Chapter 7, BTP-7-19 and the NRC CCF policy, SRM-SECY-22-0076. As such, [applicant] has demonstrated that the SP Modernization Project has adequately assessed the defense in depth and diversity of the Sample Plant. Vulnerabilities to digital CCF have been adequately identified and addressed commensurate with the risk significance of the RPS Sample Platform control system.

7. References

[Include references to design documents, licensing documents, EPRI data sheets, etc. as necessary to provide evidence.]

NRC Tabletop (PWR Modernization Example)
Attachment 1: Systematic Control Methods

LSDS #	Refined Loss Scenario	Applied Control Methods	Control Method Score	Implementation
LS-1-1	RPS cabinet air temperatures exceed equipment rating by an unspecified amount (fan failure, equipment overheating, blocked vents, insufficient HVAC,...)	(Protect) Specify equipment temperature rating of 120°F to allow for the maximum MCR design basis temperature of 104°F, plus 15°F for local temperature rise, plus 1°F margin; credit qualified, independent and redundant MCR HVAC divisions to maintain MCR temperature <= 104°F; provide a cabinet fan/filter; procedure requires periodic inspection/cleaning of fan/filter.	**CME - 3.00** CMS – High CMT – Technical CMC – Low CMV – High	SP Modernization Project System Design Document, Section xx
		(Detect) Cabinet air temperature is indicated locally. A loss of trip function or a spurious trip may occur in the affected cabinet.	**CME - 1.24**	SP Modernization Project System Design Document, Section xx
		(Respond) Equipment in the affected cabinet is promptly provided with sufficient temporary cooling. A procedure requires response and recovery within the lowest mean time to restoration limit assumed in the PFD calculations. If the MTTR limit is exceeded, the plant is shut down or remains shut down until the system is restored.	**CME - 2.68**	SP Modernization Project System Design Document, Section xx

NRC Tabletop (PWR Modernization Example)
Attachment 1: Systematic Control Methods

LSDS #	Refined Loss Scenario	Applied Control Methods	Control Method Score	Implementation
LS-1-2	RPS control algorithm provides inadequate control logic.	Refer to Appendix B	Refer to Appendix B	Refer to Appendix B
LS-1-3	RPS receives a Manual Operator Bypass control action from the Control Room Operator (CRO) when RPS is needed.	(Protect) Interdivisional, one-way communication between RPS divisions that provides bypass status. Bypass status is also provided via I/O modules between divisions. Include requirements to block Manual Operator Bypass and alert the Operator if another division is already in Manual Operator Bypass when.	**CME - 2.76** CMS – High CMT – Technical CMC – High CMV - Medium	SP Modernization Project System Design Document, Section xx
		(Detect) Main Control Room indication of Manual Operator Bypass status is provided for both divisions. Main Control Room alarm indicates if both divisions are in Manual Operator Bypass.	**CME - 2.76** CMS – High CMT – Technical CMC – High CMV - Medium	SP Modernization Project System Design Document, Section xx

NRC Tabletop (PWR Modernization Example)
Attachment 1: Systematic Control Methods

LSDS #	Refined Loss Scenario	Applied Control Methods	Control Method Score	Implementation
		(Respond and Recover) Manual Operator Bypass is removed upon notification. A procedure requires response and recovery within the lowest time to restoration. If one division of RPS cannot be restored, the plant is shut down or remains shut down until the system is restored.	**CME - 1.90** CMS – Moderate CMT – Procedure CMC – High CMV - Medium	SP Modernization Project System Design Document, Section xx
LS-1-4	*[Left blank for NEI/NRC tabletop]*	*[Left blank for NEI/NRC tabletop]*	*[Left blank for NEI/NRC tabletop]*	*[Left blank for NEI/NRC tabletop]*
[…]	*[…]*	*[…]*	*[…]*	*[…]*
LS-1-xx	*[Left blank for NEI/NRC tabletop]*	*[Left blank for NEI/NRC tabletop]*	*[Left blank for NEI/NRC tabletop]*	*[Left blank for NEI/NRC tabletop]*

NRC Tabletop (PWR Modernization Example)
Attachment 2: Pre-Scored Control Methods

CM #	Control Method	CEP – A Applicability	Implementation
CM-1	In addition to natural language text, semi-formal methods are used to specify control algorithm requirements. Semi-formal methods include logic or function block diagrams, sequence diagrams, data flow diagrams, finite state machine or state transition diagrams, and decision or truth tables.	HR	SP Modernization Project System Requirements, Section xx
CM-2	Control algorithm requirements are backward traceable to the functional and performance requirements of the affected plant systems and their design and licensing bases.	HR	SP Modernization Project System Requirements, Section xx
CM-3	Computer aided tools are used to support CM-1 and/or CM-2.	HR	SP Modernization Project System Requirements, Section xx
CM-4	The control algorithm includes features for detecting and responding to loss scenarios (and their causes) when they are detectable. When a loss scenario is detected, the control algorithm response is to provide an alarm and put the system in a safe state.	HR	SP Modernization Project System Requirements, Section xx
CM-5	Control algorithm software architecture is stateless or a limited state design.	R	SP Modernization Project System Requirements, Section xx
CM-6	Control algorithm software architecture and design is modular.	HR	SP Modernization Project System Requirements, Section xx
CM-7	Control algorithm software module size is limited.	HR	SP Modernization Project System Requirements, Section xx

NRC Tabletop (PWR Modernization Example)
Attachment 2: Pre-Scored Control Methods

CM #	Control Method	CEP – A Applicability	Implementation
CM-8	Control algorithm software modules use information hiding or encapsulation.	HR	SP Modernization Project System Requirements, Section xx
CM-9	Control algorithm software modules have a limited or fixed number of parameters.	R	SP Modernization Project System Requirements, Section xx
CM-10	Control algorithm software modules have one entry point and one exit point.	HR	SP Modernization Project System Requirements, Section xx
CM-11	Control algorithm software modules have fully defined interfaces.	HR	SP Modernization Project System Requirements, Section xx
CM-12	Control algorithm software modules use trusted and verified elements if available.	HR	SP Modernization Project System Requirements, Section xx
CM-13	Control algorithm architecture and design are backward traceable to control algorithm requirements.	HR	SP Modernization Project System Requirements, Section xx
CM-14	Control algorithm architecture and design is 1) cyclic, with a set maximum cycle time, 2) time-triggered, or 3) event-driven with a set maximum response time.	HR	SP Modernization Project System Requirements, Section xx
CM-15	Static resources are allocated for resources required by the control algorithm.	HR	SP Modernization Project System Requirements, Section xx
CM-16	Static synchronization of access is used when the control algorithm needs access to shared resources.	HR	SP Modernization Project System Requirements, Section xx

NRC Tabletop (PWR Modernization Example)
Attachment 2: Pre-Scored Control Methods

CM #	Control Method	CEP – A Applicability	Implementation
CM-17	Type 2 and Type 3 tools used in control algorithm software development and maintenance are certified or demonstrate confidence in use as described in IEC Std. 61508 (2010).	HR	SP Modernization Project System Requirements, Section xx
CM-18	Control algorithm implementation includes defensive programming methods, such as range checking of variables; checking plausibility of values where possible; checking of parameters for type, dimension, and range; checking of output variables by observing associated changes in system states; checking for accessibility of expected hardware; and checking that control algorithm software configuration is complete.	HR	SP Modernization Project System Requirements, Section xx
CM-19	Design and coding standards are used in control algorithm implementation, including no dynamic objects; no dynamic variables; limited use of interrupts, limited use of pointers; limited use of recursion; no unstructured control flow; and no automatic type conversion.	HR	SP Modernization Project System Requirements, Section xx
CM-20	Structured programming is used in control algorithm implementation.	HR	SP Modernization Project System Requirements, Section xx

NRC Tabletop (PWR Modernization Example)
Attachment 2: Pre-Scored Control Methods

CM #	Control Method	CEP – A Applicability	Implementation
CM-21	Control algorithm software modules are tested using dynamic analysis and test methods, including avalanche/stress test cases and response times subject to system performance requirements.	HR	SP Modernization Project System Requirements, Section xx
CM-22	Control algorithm software modules are subjected to functional testing.	HR	SP Modernization Project System Requirements, Section xx
CM-23	Performance testing of control algorithm software modules includes data recording and analysis.	HR	SP Modernization Project System Requirements, Section xx
CM-24	Control algorithm software modules are subjected to interface testing.	HR	SP Modernization Project System Requirements, Section xx
CM-25	Testing of control algorithm software modules is supported by test management and automation tools.	HR	SP Modernization Project System Requirements, Section xx
CM-26	Control algorithm software module test cases cover the boundaries and extremes of input classes determined via boundary value analysis, such as zero divisors, blank characters, empty list elements, full matrices, or zero table entries.	HR	SP Modernization Project System Requirements, Section xx
CM-27	Control algorithm software module entry points are subjected to 100% structural test coverage. If 100% coverage cannot be achieved, justification is provided.	HR	SP Modernization Project System Requirements, Section xx

NRC Tabletop (PWR Modernization Example)
Attachment 2: Pre-Scored Control Methods

CM #	Control Method	CEP – A Applicability	Implementation
CM-28	Control algorithm software module statements are subjected to 100% structural test coverage. If 100% coverage cannot be achieved, justification is provided.	HR	SP Modernization Project System Requirements, Section xx
CM-29	Control algorithm software module branches are subjected to 100% structural test coverage. If 100% coverage cannot be achieved, justification is provided.	HR	SP Modernization Project System Requirements, Section xx
CM-30	Control algorithm test cases are backward traceable to a control algorithm software design description.	HR	SP Modernization Project System Requirements, Section xx
CM-31	Control algorithm software integration with hardware is performed via CM-21, CM-22, and CM-23.	HR	SP Modernization Project System Requirements, Section xx
CM-32	Control algorithm aspects of system validation are subjected to test cases that include simulation of the controlled process.	HR	SP Modernization Project System Requirements, Section xx
CM-33	Control algorithm software aspects of system validation are subjected CM-22.	HR	SP Modernization Project System Requirements, Section xx
CM-34	The control algorithm software validation plan is backward traceable to the control algorithm requirements.	HR	SP Modernization Project System Requirements, Section xx

NRC Tabletop (PWR Modernization Example)
Attachment 2: Pre-Scored Control Methods

CM #	Control Method	CEP – A Applicability	Implementation
CM-35	When system failure detection is allocated to automation, and response and recovery functions are allocated to humans, the control algorithm software provides the necessary alarm functions.	HR	SP Modernization Project System Requirements, Section xx
CM-36	When system failure response and recovery functions are allocated to humans, the control algorithm (allocated to the human) is implemented by a procedure that provides the necessary steps.	HR	SP Modernization Project System Requirements, Section xx