INL/EXT-20-61079

Light Water Reactor Sustainability Program

Vendor-Independent Design Requirements for a Boiling Water Reactor Safety System Upgrade

May 2020

U.S. Department of Energy

Office of Nuclear Energy

INL/EXT-20-61079

Vendor-Independent Requirements for a Boiling Water Reactor Safety System Upgrade

Light Water Reactor Sustainability Program

Paul J. Hunton, Research Scientist, Principal Investigator
Robert T. England, Research Engineer

MPR Associates, Inc.

Paul Heaney
David Herrell
William Jessup

May 2020

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy

EXECUTIVE SUMMARY

The commercial nuclear sector faces unprecedented financial challenges driven by low natural gas prices and subsidized renewables in a marketplace that does not reward carbon-free baseload capacity. These circumstances, along with increasingly antiquated labor-centric operating models and analog technology, have forced the premature closure of multiple nuclear facilities and placed a much larger population of nuclear power stations at-risk. To enable nuclear plant economic survival in current and forecasted market conditions, an efficient and technology-centric operating model that harvests the native efficiencies of advanced technology is required. This is analogous to the transformation that has occurred in nearly every other industry.

Historical regulatory barriers have largely precluded the modernization of nuclear plant first-echelon safety systems to support this transformation. These barriers have now been largely addressed through collaboration between industry leaders and the Nuclear Regulatory Commission (NRC). These advances enable the modernization of key safety systems through the streamlined license amendment process reflected in Digital Instrumentation and Controls Interim Staff Guidance #06 (DI&C-ISG-06), Revision 2, "Licensing Process." While regulatory advances have improved the environment for modernizing safety systems, the industry has remained reluctant to perform such Instrumentation and Controls (I&C) upgrades because of perceived regulatory risks associated with being the first adopter of the DI&C-ISG-06, Revision 2 process for a major critical safety system.

This Light Water Reactor Sustainability Program (LWRS) research seeks to assist in breaking this impasse through the development of vendor-independent Boiling Water Reactor (BWR) I&C technical and licensing related documentation. These products are intended to support first-echelon safety-related (SR) upgrades for the industry. They include:

- A Plant Protection System (PPS) platform and application functional requirements baseline. The envisioned PPS design concept is a common, SR, replacement digital platform that implements the existing functions of the following BWR systems as applications:
  - Reactor Protection System (RPS)
  - Nuclear Steam Supply Shutoff System (N4S)
  - Emergency Core Cooling Systems (ECCS)*
    - Core Spray (CS)
    - High Pressure Coolant Injection (HPCI)
    - Reactor Core Isolation Cooling (RCIC)**
    - Low Pressure Coolant Injection (LPCI) mode of Residual Heat Removal (RHR)
    - Automatic Depressurization System (ADS)

  * ECCS represents the family of systems that provide core cooling. ECCS is not an individual system.

  ** RCIC provides an emergency core cooling capability. It is identified as a separate system in plant design documentation. It is grouped under ECCS for convenience.

  The PPS platform is expected to be expandable to support hosting most of the SR functions in a target BWR unit, within the hardware capabilities of the utility selected platform. This research presupposes that a utility will select a vendor with a SR platform prequalified by the NRC. Use of a NRC prequalified platform for the SR digital I&C design enables the use of the DI&C-ISG-06, Revision 2, Alternate Review (AR) process.

  The vendor-independent PPS platform and application functional requirements baseline is provided in Appendix A.

- A Non-Safety Related (NSR) platform requirements and application requirements baseline for the Redundant Reactivity Control System (RRCS). In accordance with Title 10 of the Code of Federal Regulations, Part 50, Energy, Section 62 (10 CFR 50.62), the RRCS must remain fully

independent of the PPS but need not be constructed of SR components. This research also presupposes a scenario where a Diversity and Defense-in-Depth (D3) analysis of the implementation of the NRC prequalified platform shows that Diverse Actuation System (DAS) functionality is required to address the potential for a common cause failure of the SR platform. This research proposes that DAS functionality (including the RRCS anticipated transients without scram [ATWS] function) be implemented using a NSR distributed control system (DCS).

The vendor-independent requirements baseline for the non-safety platform requirements and application requirements baseline for the RRCS is provided in Appendix B. These requirements form the basis of the DCS requirements for the DAS function in the DCS.

- A License Amendment Request (LAR) Framework Document. To implement the stated scope in a target BWR unit, a LAR must be submitted to the NRC. This research provides a vendor-independent LAR Framework Document created in a format consistent with the DI&C-ISG-06, Revision 2 AR process. Informed by the functional requirements baselines, the LAR Framework Document provides notional architectures and design attributes directed toward an advanced end-state. This provides a vehicle to communicate additional design information to vendors and streamlines the future generation of a complete, utility developed, vendor and unit-specific LAR which will be augmented to address plant-specific details, formatting, and the aspects of a complete LAR, as defined in guidance provided in Nuclear Energy Institute 06-02, "License Amendment Request Guidelines." The LAR Framework Document also provides the NRC an understanding of envisioned design concept attributes in a format that allows for early evaluation of their licensability.

  The vendor-independent LAR Framework Document is provided in Appendix C.

With the cooperation of Exelon Generation, the Limerick Generating Station (LGS) Units 1 and 2 were used as a basis for the creation of the research documents described above.

The vendor-independent functional requirements baselines and LAR Framework Document are written in a coordinated fashion to provide an aggregate solution that goes far beyond a like-for-like replacement. They describe capabilities and features enabled by digital technology to reduce acquisition, operating and maintenance (O&M), and lifecycle costs. The modernized requirements baselines and LAR Framework Document describe features that enable improved plant performance, improved data retention and analysis, and improved Human System Interfaces (HSIs). They enable a larger, plantwide digital transformation end-state that minimizes the plant total cost of ownership.

Utilities planning to perform BWR SR I&C upgrades and associated NSR DAS function installations on their plantwide NSR DCS would tailor information contained in the vendor-independent functional requirements baselines and LAR Framework Document produced by this research for use on their particular units. Utilities would then leverage this tailored information as a starting point for the collaborative development of SR digital I&C and NSR DAS requirements with their selected vendor(s). A utility and their selected vendor would collaboratively adapt and refine the tailored requirements baselines and LAR Framework Document to conform these documents to the utility's specific needs for a particular unit and the capabilities of the selected vendor's product lines.

The LWRS Program appreciates the research support provided by Exelon Generation. Exelon Generation is leveraging this research to support their in-progress LGS PPS upgrade and plans to leverage it for their RRCS replacement. This research report and the associated appendices make no commitments for Exelon Generation.

CONTENTS

FIGURES

ACRONYMS

10 CFR 50	Title 10 of the Code of Federal Regulations, Part 50, Energy
ABWR	Advanced Boiling Water Reactor
ADS	Automatic Depressurization System
AR	Alternate Review
ASAI	Application Specification Action Items
ATWS	Anticipated Transient Without Scram
BISI	Bypassed Indication and Status Indication
BWR	Boiling Water Reactor
BOP	Balance of Plant
CGD	Commercial Grade Dedication
CS	Core Spray
CBP	Computer Based Procedures
COSS	Computerized Operator Support System
CCF	Common Cause Failure
CFR	Code of Federal Regulations
CR	Control Room
D3	Diversity and Defense-in-Depth
DI&C-ISG-04	Digital Instrumentation and Controls Interim Staff Guidance #04
DI&C-ISG-06	Digital Instrumentation and Controls Interim Staff Guidance #06
DAS	Diverse Actuation System (function in a DCS)
DCS	Distributed Control System
DEG	Digital Engineering Guide
DKT	Display(s), Keyboard, and Trackball integrated Human System Interface
DR	Design Requirements
ECCS	Emergency Core Cooling Systems: Comprised of Core Spray, High Pressure Coolant Injection, the Low Pressure Coolant Injection mode of Residual Heat Removal, and Automatic Depressurization System. The Reactor Core Isolation Cooling System also provides emergency core cooling capability. It is identified as a separate system in plant design documentation. It is grouped under ECCS in this research document for convenience.
EIM	Equipment Interface Module
EMC	Electromagnetic Compatibility
EPRI	Electric Power Research Institute
FMEDA	Failure Modes, Effects, and Diagnostics Analysis
FR	Functional Requirements
GDC	General Design Criteria
GEH	General Electric - Hitachi
HFE	Human Factors Engineering

HPCI	High Pressure Coolant Injection
HSI	Human System Interface
I&C	Instrumentation and Control
LAR	License Amendment Request
LGS	Limerick Generating Station Units 1 and 2
LPCI	Low Pressure Coolant Injection (LPCI) - mode of RHR
LWRS	Light Water Reactor Sustainability (Program)
N4S	Nuclear Steam Supply Shutoff System
NRC	Nuclear Regulatory Commission (United States)
NSR	Non-Safety Related
O&M	Operating and Maintenance
PAMS	Post Accident Monitoring System
PPS	Plant Protection System
PSAI	Plant Specific Action Item
PWR	Pressurized Water Reactor
RCIC	Reactor Core Isolation Cooling
RHR	Residual Heat Removal
RISC	Risk-Informed Safety Class
RRCS	Redundant Reactivity Control System
RPS	Reactor Protection System
SCCF	Software Common Cause Failure
SE	Safety Evaluation
SOE	Sequence of Events
SLCS	Standby Liquid Control System
SPDS	Safety Parameter Display System
SR	Safety-Related
TBC	To Be Confirmed
TBD	To Be Determined
V&V	Verification and Validation
VOP	Vendor Oversight Plan
UFSAR	Updated Final Safety Analysis Report

VENDOR-INDEPENDENT DESIGN REQUIREMENTS FOR A BOILING WATER REACTOR SAFETY SYSTEM UPGRADE

1. Introduction and Scope

Currently installed Boiling Water Reactor (BWR) first-echelon safety systems have performed their function admirably. Most, however, are of the original plant vintage. As such, they are increasingly less supportable and more maintenance intensive. Parts are increasingly difficult and costly to obtain, and the expertise to maintain these older analog (and in some cases first generation digital) systems is waning. Making additional investments on these obsolete systems or providing like-for-like digital replacements that perform the same function as the original systems provides no opportunity for employing advanced digital technology capabilities to lower plant costs or improve plant performance. Costs associated with sustaining activities for older systems are rising rapidly. Like-for-like system replacement costs can rival those for digital systems which provide much more capability.

Up to now, there has been no road map for performing a large-scale digital transformation of currently operating nuclear plants to extend their technical longevity, while at the same time reducing their operating and maintenance (O&M) costs. The LWRS Plant Modernization Pathway, with input from Exelon Generation, has developed a design concept for first-echelon BWR safety system I&C upgrades as a key enabler for a larger Concept of Operations that moves an existing plant from a labor-centric analog domain to a technology-centric digital domain. This is illustrated in Figure 1 below.

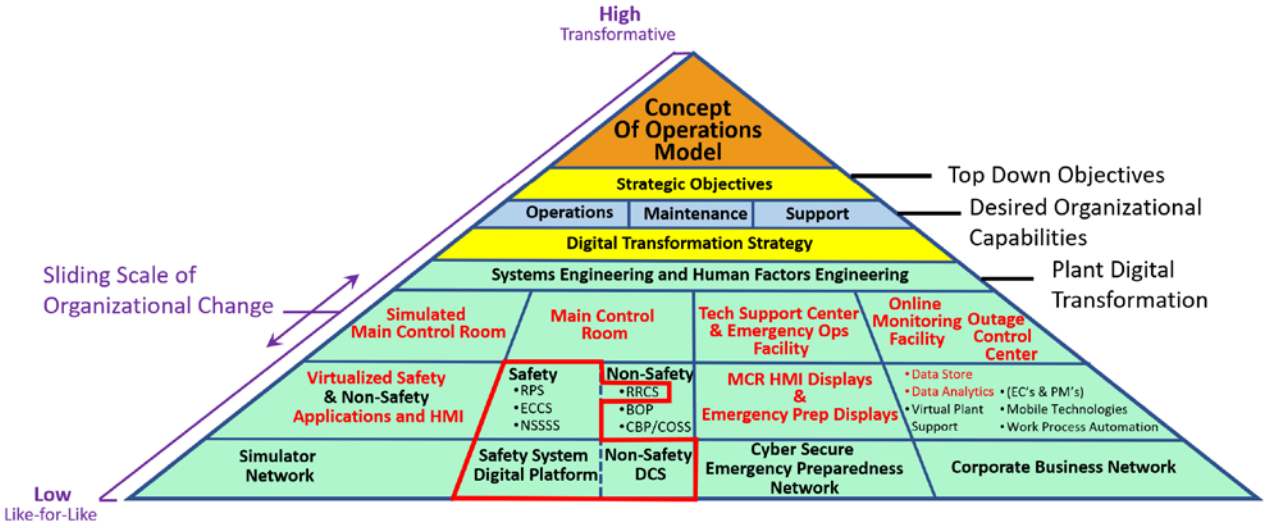

Figure 1. Safety-Related I&C Enables Advanced Concept of Operations Functions.

The Concept of Operations Model establishes strategic objectives and constraints for all plant protection, control, and business functions as an integrated set (shown in green above). This promotes a business-driven digital transformation strategy that reformulates the traditional labor-centric nuclear power plant operating model to one that is technology-centric. This supports a smaller on-site staff footprint, while increasing the safety, reliability, and situational awareness and improves focus on daily plant operations.

The research scope of this phase of the digital transformation strategy for a BWR is outlined in red in Figure 1 and includes:

- A Plant Protection System (PPS) platform and application functional requirements baseline. The envisioned PPS is a common, safety-related (SR) platform that will implement the functions of the following BWR systems as applications:

    - Reactor Protection System (RPS)
    - Nuclear Steam Supply Shutoff System (N4S)
    - Emergency Core Cooling Systems (ECCS)

  The PPS platform is expected to be expandable to potentially host most of SR functions in the unit, within the hardware capabilities of the utility selected, NRC prequalified platform.

- A Non-Safety Related (NSR) platform requirements and application requirements baseline for the existing SR Redundant Reactivity Control System (RRCS). In accordance with 10 CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants" [Reference 1], the RRCS must remain fully independent of the PPS but need not be constructed of SR components. Consequently, it is envisioned that the RRCS will be upgraded using a NSR distributed control system (DCS).

Developing a design concept for these first-echelon BWR safety system I&C upgrades is a key enabler for the holistic approach of the envisioned digital transformation. This holistic approach positively impacts business and operational needs that are beyond the scope of the identified systems themselves. As a representative example, consider online performance monitoring. Digital systems are inherently capable of collecting and disseminating large volumes of process and plant performance data. This research eliminates the manual recording of system data. It significantly increases the amount of outbound information that is available from the SR systems for remote monitoring and data analytics, which enables condition-based maintenance. These opportunities are reflected in red text items in Figure 1.

To implement the stated scope, a complete License Amendment Request (LAR) must be submitted to the NRC. This research also provides the digital portion of a complete LAR as a vendor-independent LAR Framework Document created in a format consistent with Digital Instrumentation and Controls Interim Staff Guidance #06, Revision 2, "Licensing Process" (DI&C-ISG-06) [Reference 2] to aid this effort. The LAR Framework Document is informed by the above functional requirements baseline and also contains other necessary information such as notional architectures. The LAR Framework Document also provides guidance for incorporating vendor-specific information for designs prequalified by the NRC to streamline the process of generating a complete, utility directed, vendor and unit-specific LAR. The LAR Framework Document also affords the NRC an early opportunity to understand envisioned design attributes and research direction in a format which allows for the early evaluation of their licensability.

Initial related economic research evaluations of implementing the PPS along with its associated applications as well as migrating the RRCS to a NSR DCS provide a compelling justification to support these upgrades. This initial related research will more closely relate the vendor-independent functional requirements in Appendices A and B to identified economic benefits of digital modernization. This related economic research is being documented in a separate report.

The remaining sections of this research report provide the following information:

- Section 2 describes the process used to develop the two vendor-independent functional requirements baselines (Appendices A and B) as described above.
- Section 3 describes the process used to develop the vendor-independent LAR Framework Document (Appendix C) as described above. It also provides an overview of key digital upgrade design concepts as captured for both the SR PPS and the NSR DAS functions.
- Section 4 describes how the vendor-independent functional requirements baselines and LAR Framework Document are to be used by the utility and their selected vendor.

The research team has endeavored to ensure that all documents that make up this research report are technically consistent. Due to the complex nature of this activity and the use of multiple authors, however, some deviations may exist. Any such deviations are unintended and are most likely at a level of detail that would not impact the overarching objectives of this research report.

The LWRS Program appreciates the research support provided by Exelon Generation. Exelon Generation is leveraging this research to support their in-progress LGS PPS upgrade and plans to leverage it for their RRCS replacement. This research report and the associated appendices make no commitments for Exelon Generation.

2. Vendor-Independent Functional Requirements Baselines

MPR Associates, Inc. was subcontracted by the LWRS Program to lead the authoring of the two vendor-independent functional requirements baselines described below. MPR coordinated extensively with personnel from the Exelon LGS and LWRS in the creation of the functional requirements baselines.

These products are intended to support first-echelon BWR SR upgrades for the industry. With the cooperation of Exelon Generation, the LGS was selected as a basis for creation of the following:

- A PPS platform and application functional requirements baseline. The envisioned PPS is a common, SR, replacement digital platform that will implement the existing functions of the following BWR systems as applications:
  - RPS
  - N4S
  - The family of systems that together are referred to as the ECCS

  The vendor-independent PPS platform and application functional requirements baseline is provided in Appendix A.

- A NSR platform requirements and application requirements baseline for the RRCS.

  The vendor-independent requirements baseline for the non-safety platform and RRCS application is provided in Appendix B.

The subsections below provide details as to how the functional requirements baselines were created.

The "requirements" in Appendices A and B are, in fact, only a baseline. Appendices A and B are intended to provide specific information regarding desired attributes of the envisioned end-state when the scoped systems are replaced with new digital technology. Appendices A and B have been developed as tools for the nuclear industry to engage vendors in a collaborative effort to adapt and conform them with the needs of a particular unit and to the capabilities of the selected vendor's product line. To provide a firm foundation for Appendices A and B, LGS was selected as the reference facility for this effort. Because of this, the research information contained therein is tailored to the LGS plant design and reflects design concept decisions made by research participants to achieve objectives associated with LGS digital transformation plans. Exelon is leveraging Appendices A and B as part of an effort to perform first-echelon SR I&C upgrades at LGS. From an industry perspective, these requirements baselines contain design concepts based on an actual reference plant. Section 4 presents how the functional requirements baseline information is being used by utilities and by their selected vendors in conjunction with the LAR Framework Document (Appendix C) to create a final, unit-specific set of functional requirements.

2.1 Functional Requirement Baseline Development Process

2.1.1 Guiding Principles

Guiding principles were established at the onset of this research activity to frame the approach for developing the platform and application functional requirements baselines. While these were primarily generated with a focus on SR applications, the principles can be generally applied for NSR applications as well with minimal adjustments. A list of these principles is provided below:

- There are multiple vendors who provide SR systems that have received a Safety Evaluation (SE) Report from the NRC (e.g. Westinghouse Common Qualified [Common Q] Platform, Areva Teleperm XS, Radiy RadICS). Based upon a general understanding of these systems from publicly

available data, a generic superset of features that they offer was drawn upon to enable a best aggregate solution, while keeping the research design concept bounded in the "art-of-the-possible."

- To reduce overall design and implementation risks, requirements should maximize the use of off-the-shelf technologies and features rather than driving first-of-a-kind development efforts.
- Overall licensing risk should be minimized, while at the same time introducing the use of existing technologies in ways novel to nuclear that can provide clear operational/economic benefits.
- Field devices that provide inputs to the systems and field devices that are driven by outputs from the systems are to be retained, to the extent practical. Requirements shall not be developed with the intent to require the installation and use of new or additional field devices.
- Requirements shall encourage the consolidation and reduction of field devices (e.g. transmitters) to the extent practical.
- Some requirements will be constrained by the physical configuration of retained field devices and wiring outside of the I&C cabinets. Design bases and licensing constraints for such equipment will not be altered by the upgrade effort.
- Current industry standards and licensing requirements will be invoked, where appropriate, for new digital equipment (primarily within and between cabinets where new digital equipment will be installed).
- In general, all the functions of the existing systems intended to be migrated to the new digital platforms are to be provided as applications. Any additions, omissions, or deviations (e.g. a change in voting scheme) within the new digital platforms and hosted functional requirements are to be clearly identified.
- Design attributes of the new digital platforms should support the elimination of Technical Specification surveillances, calibrations, time response testing, etc. to reduce labor and other O&M costs.

2.1.2 Decisions for the Design Concept

In some cases, the guiding principles listed above may conflict. In others, the guiding principles did not by themselves provide sufficient guidance to establish a particular design concept direction. In order to keep the design concept moving forward, it was necessary to coordinate with Exelon as a research team participant to make design concept decisions. As the need for these decisions were identified, they were captured in a Research Decision Matrix for tracking and disposition. These items were discussed during meetings, with the resulting dispositions documented to support the direction to be pursued by this research activity. Appendix D captures the Research Decision Matrix that supported the development of the functional requirements baseline for each of the applications as well as the PPS and NSR platforms. These research decisions may be revisited as the design progresses and based upon selected vendor platform capabilities. Section 4 presents in more detail how the Research Decision Matrix may be used by utilities and by their selected vendors in conjunction with the functional requirements baselines (Appendices A and B) and the LAR Framework Document (Appendix C) to create a final, unit-specific set of functional requirements.

2.1.3 Stakeholder Needs

Using the systems engineering guidance contained in the Electric Power Research Institute (EPRI) report 3002011816, Digital Engineering Guide [Reference 3], several stakeholder organizations (e.g. engineering, maintenance, operations, etc.) within Exelon were solicited to provide input to the development of the baseline platform and functional requirements. The objective was to elicit a set of clear and concise needs related to the digital modernization effort and to transform these stakeholder needs into verifiable stakeholder requirements. Multiple workshops were conducted with research

participants, which resulted in a number of requirements being revised to reflect stakeholder needs or resulted in the creation of new standalone requirements.

2.1.4 Requirements Baseline Document Road Map

A Microsoft Excel workbook was chosen as the mechanism to document the requirements. Each existing system being upgraded was assigned a spreadsheet for design requirements (DR) and another for functional requirements (FR). The spreadsheets were initially populated with requirements information applicable to the existing system design and licensing basis. Each of the requirements was assessed to determine the degree to which it was impacted by the transition to a digital platform. The impact may be an update to a source/basis entry, an elimination of a requirement, the creation of a new requirement, the revision of a requirement, or no impact. The impact assessment was documented in the spreadsheet. Any changes from the existing system requirements were captured using additional columns to retain the history associated with the evolution of the requirement. The spreadsheets were used as a tool to arrive at the final version of the requirements that reflect the intended FR and DR for each current system to be hosted on a digital platform as an application.

The Excel workbook includes two additional spreadsheets that document the creation and evolution of the digital platform requirements for the replacement SR and NSR digital platforms. The new platform requirements define the functional and performance framework that envelope the DR of the existing platforms. This is necessary to satisfactorily host the system applications described in the FR that are to be migrated to the respective replacement SR and NSR digital platforms. The SR and NSR platforms must demonstrate that they satisfy the DR of each of the current systems, while hosting the respective applications that meet the FR that have been created for those same systems. In this way, the replacement platforms and hosted applications can be shown to meet the requirements that the current systems satisfy.

All the requirements documented in the Excel workbook have been intentionally tailored so that they are vendor-independent. The final version of this collective set of requirements represents a bounding framework specific to LGS (as the research basis units) to support the transition to digital platforms. This has been defined as the functional requirements baseline. Microsoft Word documents have been developed to communicate the functional requirements baselines to utility selected prospective candidate vendors; one for the SR requirements (Appendix A) and another for the NSR requirements (Appendix B). Both Appendix A and Appendix B provide a narrative to explain the purpose, background, scope, and approach for this endeavor and provide a listing of all the references used to develop the FR and DR. The final versions of the vendor-independent SR and NSR platform and application requirements were exported from the Excel workbooks into Word tables, which are included in Appendices A and B. It is intended that utilities and their selected vendors will leverage these research products (Excel workbooks and Appendices A and B) as an input to collaboratively conform them to the vendor’s product line. This will result in the creation of unit- and vendor-specific functional requirements that meet both the utility’s need and all applicable design and regulatory requirements.

The native Excel workbook files contain additional information that goes well beyond what is contained in Appendices A and B. This additional information is critical to understanding how both appendices were produced, starting from source design and licensing basis documentation for the current systems and how these were leveraged in the process to create Appendices A and B. The native files are a roadmap that captures the thought process to create the functional requirements baseline deliverables. The native files also show the delta between the source design and its licensing basis as compared to the new requirements. Showing this transition is necessary when the final replacement system requirements are used as supporting documentation for NRC review of the complete LAR submittal. Having this information in a Microsoft Excel workbook format lends itself to incorporation into a requirements management tool to support future requirements traceability. For these reasons, the separate Microsoft Excel workbook native files from which Appendices A and B were drawn are also available for general industry use.

2.1.5 Identification of Design and Functional Requirements Derived from Existing Systems

The identification of the applicable design and functional requirements for the existing systems to be migrated to the digital platforms begins with a review of relevant documents. The types of documents to be reviewed include, but are not limited to, the Updated Final Safety Analysis Report (UFSAR), plant drawings, plant procedures, Design Basis Documents, specifications, calculations, system descriptions, etc. The lists of LGS documentation used in the development of the respective DR and FR for the existing systems are identified in Section 5 (references) of Appendices A and B.

Each existing system is assigned two Excel spreadsheets; one for DR and one for FR. The baseline requirements that establish the licensing and design basis for a system have been drawn from various codes, criteria, and regulatory requirements. For the I&C portions of the existing systems (hardware, relays, etc.), the regulatory guides, 10 CFR 50 Appendix A "General Design Criteria" (GDC) [Reference 4], and industry codes and standards that are applicable are listed in the respective DR spreadsheet.

For each DR spreadsheet, their structure is as follows:

- Each row of the spreadsheet is associated with a specific DR.
- Columns A and B: Used to assign a unique ID to each DR.
- Column C: Provides a description of the DR.
- Column D: Identifies the existing source/basis for the DR.
- Column E: Identifies the new source/basis for the DR. If there is no change, the same source/basis applies.
- Column F: Identifies how the existing system complies with the design requirement.
- Column G: Identifies what the impact will be to the DR source/basis or the ability of the design to comply with the requirement based on the transition to the digital platform.
- Column H: Provides the reference that identifies how the existing system complies with the design requirement.

Columns A, B, C, and E from each DR spreadsheet are exported for use in the vendor-independent functional requirement baseline deliverables as provided in Appendices A and B.

The baseline requirements for the instrumentation and control portions of the system that describe the application functionality are listed in the respective FR spreadsheet. The FR also incorporate elements that reflect design constraints, physical constraints, licensing commitments, system interfaces, system boundaries, control philosophy, controlling parameters, etc.

For each FR spreadsheet, their structure is as follows:

- Each row of the spreadsheet is associated with a specific FR.
- Columns A and B: Used to assign a unique ID to each FR.
- Column C: Provides a description of the FR for the existing system.
- Column D: Provides a description of the initial iteration of the FR for the new platform.
- Column E: Provides a description of the final iteration of the FR for the new platform.
- Column F: Identifies the existing source/basis for the FR.
- Column G: Identifies the new source/basis for the FR. If there is no change, the same source/basis applies.

- Column H: Provides additional information deemed necessary to further explain/clarify a requirement entry.
- Column I: Identifies what the impact will be to the FR source/basis or the FR as initially described, based on the transition to the digital platform.

The evolution of an FR can be seen by comparing the content across columns C, D and E. Based on the iterations that occurred for some of the individual requirements captured in the FR, this may have resulted in the elimination of a requirement, the creation of a new requirement, the expanding of a requirement into multiple requirements, or the revision of a requirement. Empty cells designated as "Not Used" are a clear indication that a requirement evolved.

Columns A, B, E, G, and H from each FR spreadsheet are exported for use in the vendor-independent functional requirement baseline deliverables as provided in Appendices A and B. Cells/rows designated as "Not Used" are not included in the FR contained in Appendices A and B.

2.1.6 Identification of Replacement Digital Platform Functional Requirements

The identification of the applicable FR for the replacement SR and NSR platforms was based on the authors' familiarity with features and capabilities that are available with and unique to digital platform designs. Many of these FRs reflect typical architecture, HSI, communication and other related capabilities prevalent in the industry. There are a number of FR identified that that are unique to the needs of the LGS.

The SR and NSR platforms are each assigned one FR Excel spreadsheet.

Each SR and NSR platform spreadsheet structure is as follows:

- Each row of the spreadsheet is associated with a specific FR.
- Columns A and B: These columns are used to assign a unique ID to each FR.
- Column C: This column provides a description of the initial iteration of the FR.
- Column D: This column provides a description of the final iteration of the FR.
- Column E: This column identifies the source/basis for the FR.

The evolution of an FR can be seen by comparing the content across columns C and D. Based on the iterations that occurred for some of the FR, this may have resulted in the elimination of a requirement, the creation of a new requirement, the expanding of a requirement into multiple requirements or the revision of a requirement. Empty cells designated as "Not Used" are a clear indication that a requirement evolved.

Columns A, B, D, and E from each FR spreadsheet are exported for use in the vendor-independent functional requirement baseline deliverables as provided in Appendices A and B. Cells/rows designated as "Not Used" are not included in the FR contained in the baseline deliverable.

2.2 Vendor-Independent Functional Requirements Baseline Review

Exelon Generation personnel at LGS reviewed and provided comments to Appendix A. All comments to this research product were dispositioned and appropriate changes incorporated.

Exelon Generation has chosen to separately pursue the implementation of the RRCS upgrade. At such time when Exelon pursues a project to replace RRCS, a LGS personnel review and comment disposition cycle will need to be performed on Appendix B in order to ensure that the research contained therein is reflective of the LGS RRCS.

The entire content of the native Excel workbook files, including the information provided in Appendices A and B, represents an interim state in the design concept of these systems and has been reviewed by technical personnel and administrative editors at MPR Associates Inc.

Exelon also contributed to and reviewed the Research Decision Matrix provided in Appendix D.

3. Vendor-Independent License Amendment Framework Document

MPR Associates, Inc. was subcontracted by the LWRS Program to lead the authoring of the vendor-independent LAR Framework Document. MPR worked with personnel from the Exelon LGS and LWRS to generate much of the technical content contained in the LAR Framework Document presented in Appendix C. This section describes the process by which Appendix C as was developed. This section also provides an executive summary of the key digital upgrade design concepts as captured for both the SR PPS and the NSR DAS and their respective functions.

A complete LAR must be submitted to the NRC and approved to enable implementation of first-echelon safety system upgrades in the target unit or units. This research provides a vendor-independent LAR Framework Document created in a format consistent with the DI&C-ISG-06, Revision 2, AR process. Plant-specific details, formatting, and many of the aspects of a complete LAR, as defined in guidance provided in Nuclear Energy Institute 06-02, "License Amendment Request Guidelines" (NEI 06-02) [Reference 5], are not incorporated in the LAR Framework Document. The LAR Framework Document focuses on the LAR aspects that are different for digital content, leaving the established LAR details to the utility to add and generate the complete LAR. The decision to focus only on the digital aspects in this research ensures that the digital detail is not obscured by the content required in the complete LAR.

The subsections below provide details on the creation of and an executive summary for the LAR Framework Document. The rest of this section provides reasoning for creating this Framework Document so early in the design process.

At this point in design concept development, the LAR Framework Document supports two separate but related purposes. First and foremost, the LAR Framework Document provides a mechanism for the research team to capture and communicate a comprehensive, top-down description of the systems being replaced, along with a description of the replacement systems and their overall function in one place. Secondly, the LAR Framework Document provides a foundation on which to generate a LAR consistent with NRC expectations for a digital system.

This upgrade effort does far more than provide like-for-like functional replacements of the current systems. The new systems leverage current state-of-the-industry digital technology not only to implement the functions of the original systems, but also to leverage that technology to:

- Drastically reduce equipment part counts, thus increasing reliability while lowering acquisition, installation, and lifecycle support costs
- Enable mass data capture for historical and data analytics purposes
- Implement advanced diagnostics to detect system faults and failures
- Eliminate most of technical specifications surveillance tests, calibrations, and operational checks by either the inherent nature of the design or by automated diagnostic processes
- Eliminate the potential for human error by eliminating the need to lift and re-land field leads at the logic solver and by providing test aids (e.g., test jacks, signal disconnect switches) where testing or troubleshooting is required
- Eliminate some potential human performance error traps by automating parts of the RHR
- Provide previously unavailable plant data to the Operations staff in the Control Room (CR)

- Improve plant operational performance, while at the same time drastically reducing O&M workload and the potential for human performance error
- Support the implementation of an end-state CR modernization that is predominately digital, minimizing the manual switches and meters in the CR.

In the aggregate, these features are intended to support the overarching objective of economical and sustainable nuclear plant operation, including a path to address digital equipment obsolescence through lifecycle management. While informed by and consistent with the "bottom-up" view of the proposed replacement systems provided by the functional requirements baselines developed, as described in Section 2, the LAR Framework Document provides a "top-down" view of overall system architecture and features, which cannot be easily gleaned from the functional requirements by themselves. Eventually, design documentation will be created by the implementing utility and their vendor in later project phases that will govern the design, as described in the actual, complete LAR document created by the utility, as described in Section 4. But at this phase of the design process, the LAR Framework Document focusses on, captures, and communicates this information.

The second purpose of the vendor-independent LAR Framework Document is to provide a mechanism for the NRC staff to obtain an early understanding of envisioned safety system digital replacement design attributes identified in this research in a format which allows for an early evaluation of their licensability. By providing the draft technical information as described above as early as possible in the design process in a format consistent with that identified in DI&C-ISG-06, Revision 2 for the AR process, the NRC staff can provide early feedback on both the technical content and the format in which an implementing utility may communicate that information. The intent of early communication is to reduce implementing utility licensing risk.

The vendor-independent LAR Framework Document is in fact, only a framework. The LAR Framework Document provides top-down information with regard to notional architectures and attributes of the end-state when the scoped systems are replaced with new technology. The rest of the industry guidance regarding the content of a complete LAR, as provided in NEI 06-02, needs to be added to this LAR Framework Document and applied to the Technical Specification changes, along with utility-specific formatting of the complete LAR. The LAR Framework Document provided in Appendix C will never be submitted formally to the NRC, although the NRC may choose to read this research report. How Appendix C could be used by a utility and their selected vendor in conjunction with the vendor-independent functional requirements baselines to create a final, unit specific LAR is presented in Section 4.

3.1 License Amendment Request Framework Document Development Process

The LAR Framework Document development process considered the digital I&C guidance provided in both the D&IC-ISG-06, Revision 2 and in the digital-specific appendices to the NEI 06-02 guidance developed for the digital LAR author. The LAR Framework Document provided in Appendix C focuses on the digital aspects, leaving the other, proven mechanics of writing a complete LAR for the utility, as defined in the remainder of NEI 06-02. Rather than diluting the digital I&C message with the required LAR mechanics, which are familiar to utilities, the LAR Framework Document provided in Appendix C focuses on the digital aspects in D&IC-ISG-06, Revision 2.

Research decisions were incorporated into the Research Decision Matrix. An abbreviated, revised version of the Research Decision Matrix is provided in Appendix D, incorporating editorial revisions for reading and comprehension. The Research Decision Matrix was used to document design choices that were then implemented in the design concept captured in the functional requirements baselines and in the LAR Framework Document. Note that the Research Decision Matrix for the most part documents decisions necessary to implement the systems, since the existing reference plant architecture and plant safety

requirements are considered design constraints for which no decision is required. In a small number of cases, it was decided to modify existing architectures and design constraints as part of this research to obtain functional benefits and/or reduce cost without negatively impacting safety (e.g. changes to voting logic, the removal of redundant sensors). Such decisions were also captured in the Research Decision Matrix. The Research Decision Matrix, the functional requirements baselines, and LAR Framework Document should be retained as retrievable design input records, as the record of decisions, requirements, and system descriptions will assist implementations performed on any unit.

3.2 Guiding Principles for Licensing

The development considered the current regulatory environment, including software and hardware guidance. The LAR Framework Document is based on complying with current guidance and on an architecture that provides a more computer-based monitoring and control system for the plant, minimizing the number of hardwired switches, meters, and recorders, while maximizing the ability of the operator to understand plant state through computer-driven displays.

The list of references used during development of the vendor-independent LAR Framework Document is provided in Appendix C, Section 10. These references include regulatory documents, industry standards, vendor and NRC documents (e.g., vendor's Licensing Topical Report, NRC SE Report, vendor's Failure Modes, Effects, and Diagnostics Analysis), and Limerick-specific documents (e.g., UFSAR, drawings, D3 Analyses, Functional Requirements for the PPS as a system and the DAS function in the DCS, Vendor Oversight Plans [VOPs] for the PPS and DAS function, and Project Plans). Many of these references are common to the Vendor-Independent PPS Functional Requirements Baseline.

In addition to the guiding principles defined in Section 2.1.1, the LAR Framework Document also considered the following guiding principles:

- Consider and incorporate the guidance provided in current regulation, consistent with the regulation used by the NRC to evaluate the prequalified platform.
- Consider and incorporate, where possible, the approach taken in the nonproprietary architecture and licensing aspects of safety systems in current plants accepted by the NRC. The LAR Framework Document considered publicly available information on the I&C systems in several modern plants, including the Westinghouse AP1000 pressurized water reactor (PWR), General Electric-Hitachi (GEH) Advanced Boiling Water Reactor (ABWR), and Korean APR1400 PWR. The approach is restricted by limitations placed on the architecture by the existing field sensing and actuation equipment.
- Consider current proven-in-use approaches used by safety critical industries outside nuclear power and determine where those approaches could be applied or applied with modifications appropriate for nuclear power plants.
- Consider the use of a single, expandable platform having the capability to meet the needs of this and future modernizations of nonspecialized monitoring and control (i.e., not radiation monitoring, LPRM/APRM/OPRM, HVAC, or Emergency Diesel Generator (EDG) controls), thus minimizing the number of SR platforms in use.

3.3 Design Concept Decisions for Licensing

Several system architecture and requirements design concept decisions were made to reduce licensing risk. These include the following:

- As defined in LAR Framework Document Section 3.1.1, the licensing basis for the PPS logic solvers is also to be modernized. Within the limitations imposed by the existing field wiring at the input and output terminations within the existing RPS, N4S, ECCS, and RRCS cabinets, the PPS complies with current as-endorsed Institute of Electrical and Electronics (IEEE) standards and

considers the clarifications in more modern IEEE standards not yet endorsed. The PPS is implemented in compliance with endorsed IEEE standards, but the design process also considers guidance from current IEEE standards in the design.

- To provide enhanced failure tolerance and to eliminate issues with one-out-of-two taken twice voting, all PPS inputs are processed by PPS channels. The PPS channels provide only the votes (i.e., results of bi-stable evaluations and discrete input states) to the PPS divisions, which usually perform a two-out-of-four vote on each one of the redundant field process values, requiring two of the four channels to provide votes to not scram, scram, not actuate, or actuate on the same sensor before implementing the required protective action. The existing system could take protective action based on one process sensor in the first division and a different process sensor in the second division. By forcing evaluations of all parameters individually, the PPS design concept eliminates noncoincident scrams or actuations. The PPS design concept also should minimize, if not eliminate, half scrams and half actuations, where one division decides to scram or actuate and the other division does not. For plant scrams, both divisions of the existing design have to actuate, so a half scram did nothing more than heighten tension in the CR. For existing system actuations, a half actuation could isolate the inboard or outboard isolation valve or start one of the ECCS. Closing both isolation valves in a pathway provides a much larger potential for actually isolating the pathway.
- To provide equivalent or better fault tolerance for failed discrete outputs, the PPS as well as DAS functions executed in the DCS both provide diagnosed single-failure tolerant discrete outputs. The use of single-failure tolerant discrete outputs ensures that no single failure of an electronic output switch can result in blocking a required protective action or falsely initiating an unrequired protective action. The requirement for diagnostics on those outputs ensures that output switch failures are detected and alarmed in the CR.
- The existing system provided little information to the CR operator concerning the plant state being evaluated by the RPS, N4S, and ECCS analog trip modules. If operators needed data, the operators dispatched staff to the Auxiliary Equipment Room, where the analog trip modules were installed, to read and record data values. These values would then be provided to plant watchstanding operators. The modernized system displays that data on video displays in the CR.

3.4 Stakeholder Needs that Affect Licensing

Some of the stakeholder needs, as discussed in Section 2.1.3, also affected the LAR Framework Document. Stakeholder requests were considered and implemented in the LAR Framework Document where appropriate. If implementation would require additional field sensors or actuators, that stakeholder need was retained for a potential future modification. If the implementation could be accomplished using existing field equipment and additional application software in the logic solver, that need was further evaluated to see if the implementation could be licensed. Several stakeholder requests could be met without licensing considerations. However, some of the requests changed the way design functions are documented in the UFSAR and would be implemented as part of this modernization. Since the request changes the UFSAR and will be implemented in this modernization, the change has to be discussed in the LAR Framework Document for incorporation into the complete LAR.

In one example, the Operations staff asked if the NSR RHR modes could be automated, such that a soft control on a video display could be used to check appropriate interlocks and set the appropriate valve and pump configuration, ensuring that a single operator mistake could not have large consequences. Automation of the NSR RHR modes requires an evaluation and discussion in the LAR Framework Document. The automation provided supports the operator, in that the operator uses soft controls on video displays to initiate functions. The automation does not replace the operator, who is still required to initiate an operator-defined function. Since this automation does help eliminate human performance errors, this

automation of NSR aspects of the SR RHR system should be acceptable and should be considered in advancing from primitive analog to modernized digital systems.

In another example, concerns over the adverse effects on the plant on actuation of the Standby Liquid Control System (SLCS) led to the research decision to provide a means of inhibiting automatic SLCS actuation. In the modernized system, concerns about maintenance error falsely initiating SLCS led to the addition of the SLCS Inhibit capability. This capability would allow the RO to inhibit SLCS initiation at the direction of the SRO while work proceeds on RRCS, along with the capability of bypassing channels within ATWS for testing. This is consistent with the ADS, which also provides an inhibit capability in the CR.

The lesson learned from this evaluation is that the industry should consider modern methods and not feel constrained by the design choices made in the existing analog design. The existing analog design is definitely a compromise, based on what could be reasonably achieved with limited functionality components and minimized complexity. The modernized system should not be constrained by the design choices made based on the capabilities of analog trip modules, pneumatic time delay relays, and relay logic. The modernized design should eliminate or at least minimize Operations and Maintenance staff workload. This can reduce the total cost the plant ownership over time to assist in keeping the unit economically viable, while at the same time improving safety by reducing human performance errors. It is also especially important to improve performance during accident and transient plant conditions, even if the plant license does have to be changed to incorporate the modernization.

3.5 LAR Framework Document Development and Use

3.5.1 Initial Development and Use

The vendor-independent LAR Framework Document is written in a format and at a level of detail to satisfy the DI&C-ISG-06, Revision 2 AR process. The LAR Framework Document was developed in parallel with the vendor-independent PPS and NSR Platform and RRCS functional requirement baselines (Appendices A and B, respectively). This was done to maintain consistency between the top-down (LAR Framework Document) and bottom-up (requirements baseline) viewpoints provided by each. The guiding principles used in the development of the functional requirements baselines as described in Section 2.1.1 were also applied to the LAR Framework Document. In order to move the design concept forward, the research effort coordinated the development of the LAR Framework Document and the functional requirements baselines with Exelon as a research contributor to make design concept decisions. These research decisions are also reflected in the requirements baselines and LAR Framework Document. Appendix D captures the Research Decision Matrix that also supported the development of the LAR Framework Document contained in Appendix C.

The LAR Framework Document describes the original system and the modernized system concepts, providing a discussion of those items that are changed from the original licensed analog RPS, N4S, and ECCS. The LAR Framework Document also describes the existing hybrid analog and digital RRCS and the modernization of the SR RRCS into the NSR ATWS function (the diversity for the RPS) in the context of the DAS functions in the NSR DCS, along with the selected portions of the N4S and ECCS required for diversity, also installed as DAS functions in the NSR DCS.

The LAR Framework Document provides a vehicle for early communication of design concepts from the utility to the platform vendor and to the reviewers at the NRC. Between text and pictures, the intent for the LAR Framework Document is to explain the top-down systems in a holistic view to complement the bottom-up view defined by the functional requirements baselines, which define the detailed requirements for PPS and DAS function in the DCS.

The LAR Framework Document provided in this research report reflects the pre-vendor-selection state, which is viewed as the most useful to assist a utility to make decisions about generic architecture and vendor selection, as none of the vendor-specific decisions are incorporated in the document.

Exelon has reviewed and provided comments on the LAR Framework Document. These comments were reviewed and dispositioned as part of this research. The LAR Framework Document provided in Appendix C captures the results of this effort.

3.5.2 Future Development and Use

In order to use the AR process in DI&C-ISG-06, one of the NRC's prequalified platforms must be used. The NRC process for approving platforms also uses DI&C-ISG-06 to evaluate the platform Licensing Topical Report and supporting documentation generated by the platform vendor. The result of the process is a SE Report defining the boundaries established by the NRC for the now prequalified platform and open issues to be resolved by the utility in the design process that applies to the selected platform. The open issues, referred to as either Plant Specific Action Items (PSAIs) or Application Specification Action Items (ASAIs) have not been resolved in the LAR Framework Document, since a vendor had not been chosen when this report was written.

The AR process assumes that the utility and selected vendor have completed the PPS Conceptual Design and have proceeded far enough into the Software Requirements Specification to minimize the errors in the Conceptual Design. The LAR Framework Document was written in part to provide top-down design information to assist the utility and selected vendor in creating future conceptual designs for the SR PPS and DAS functions in the NSR DCS that can be implemented, licensed, maintained, and surveillance tested, while minimizing the scope of surveillance testing and calibration.

The LAR Framework Document (Appendix C) and the PPS functional requirements baseline (Appendix A) provide a starting point for the PPS Conceptual Design, to be jointly developed by a utility and their selected vendor. During the PPS Conceptual Design, information in the LAR Framework Document and the PPS requirements baseline are intended to be collaboratively conformed to the selected vendor's platform by a tradeoff analysis to achieve the best aggregate solution, based upon maintaining safety while providing improved performance as well as implementation and lifecycle cost reductions. Modifications will be driven by the selected vendor and the finalized architecture, the vendor's existing application software program, the scope of the DAS, the interface between the SR platform vendor and the DAS vendor, and final utility decisions. LAR Framework Document information will be extended by incorporating vendor-specific detail and the traditional LAR content, which the LAR Framework Document, provided herein, does not include. The LAR Framework Document thus provides a digital-centric basis using DI&C-ISG-06 to build a licensable system as well as providing a top-down view of the system to ensure that the utility, platform vendor, and Regulator all have a common picture of the PPS and the DAS functions to be implemented on a NSR DCS.

Since responsibility for oversight of the vendor implementing the PPS is transferred to the utility by use of the AR process in DI&C-ISG-06, the LAR Framework Document summarizes the expectations for the utility's SR VOP. The PPS VOP will be evaluated by the NRC and will be the basis for ensuring that the vendor processes are implemented and that the resulting PPS is of high quality and as free of design errors as possible. The VOP for the DAS function may be evaluated by the NRC. The utility should generate and implement strong VOPs and processes to ensure that the vendor follows the plans, procedures, processes, and instructions in the SE Report for the SR PPS and as accepted by the utility for the DAS functions in the DCS.

Without a selected platform, many decisions could not be made and incorporated in the LAR Framework, including any improvements or platform requirements provided by the selected vendor. In order to track the locations of those needed decisions, a list of items that are To Be Determined (TBD) or To Be Confirmed (TBC) with the selection of a vendor was added to the LAR Framework Document. Including the TBD and TBC as identified locations, with an automatically generated table of contents for the TBD/TBC items ensures that the items are identified and resolved prior to the submission of the completed LAR to the NRC for acceptance review. The expectation is that the TBD/TBC entries and their table of contents will be deleted after the items are resolved. In many cases the TBD/TBC entries will be

addressed by reference to the selected vendor's prequalified design documentation. The TBD/TBC list also includes the utility's required VOP for the PPS. The TBD/TBC list also includes the utility's required VOP for the DAS function vendor, which will include the implementing utility's definition of the features of an augmented quality software lifecycle.

3.6 Overview of the Safety-Related Technical Information Contained in the LAR Framework Document

The vendor-independent LAR Framework Document provided in Appendix C is written at a level of detail to satisfy the DI&C-ISG-06, Revision 2 AR process. Given the expectations of this guidance and the scope of the envisioned SR upgrade, the LAR Framework Document is lengthy (approximately 250 pages). This section provides a summary of key design concept attributes of the envisioned replacement systems and associated applications that will envelope the current functions of the RPS, N4S, ECCS, and RRCS. Additionally, the LAR Framework Document describes advanced features that are made available through the use of digital technology. This summary is provided as an aid to promote a more general understanding of the top-down design technical information contained in Appendix C. Any potential discrepancies between the information contained in this section as compared to Appendix C (or Appendices A, B, and D by extension) is unintentional. If any discrepancies should be identified, the information in the appendices is overriding.

3.6.1 Plant Protection System Architecture

The PPS design concept architecture is discussed in LAR Framework Document Sections 3.4.1 through 3.4.4. The modernized PPS as shown on the left side of Figure 2 below retains most of the enveloping platform characteristics as the existing RPS, N4S, and ECCS systems. The existing RPS, N4S, and ECCS system functions will become segmented applications running on the PPS. The modernized design concept will retain the four channel architecture common to the RPS, N4S, and ECCS but replaces the hardwired implementations of the analog trip units (i.e., channels) in the RPS, N4S, and ECCS with four separate instantiations of the common PPS platform, implementing the separate, independent channel functions. Each of the channels provides unidirectional serial data transfer to the four divisions over redundant fiber optic cables. By design, independence is maintained between PPS channels as well as between PPS divisions by having no communication links between the channels or between the divisions. Similarly, channels do not provide engineering unit data to divisions, thus ensuring that application programs in divisions use the vote data provided by channels. Like the existing system, electrical signal isolation is maintained between all channels and all divisions. Physical separation is required by strict separation of each of the four channels and by strict separation of each of the two divisions.

The modernized PPS design concept retains the two division architecture in the RPS and the four division design in most of the N4S and ECCS. The divisions will also be separate, segmented, independent applications/functions operating in separate instantiations of the PPS platform. Existing N4S and ECCS requirements necessitate some customization to the generic two division architecture. Each division will perform the RPS, N4S, and ECCS voting, operational bypass, and maintenance bypass functions in separate, segmented applications. The existing scram, bypass, inhibit, permissive, and similar manual CR capabilities will be included in the PPS functions. While manual controls required by regulation or industry standard are retained, most of the existing manual controls are modernized to soft controls, and all of the manual controls are duplicated as soft controls through the PPS and DAS function application software.

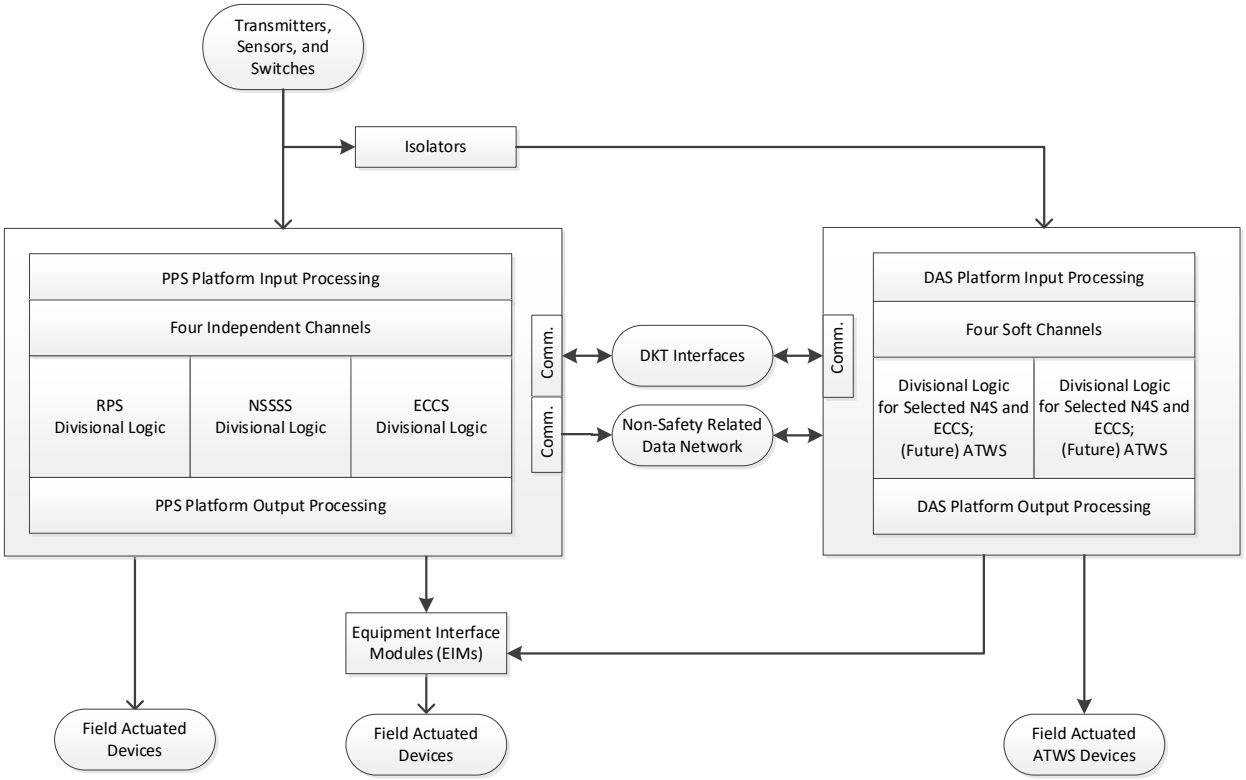

Figure 2. Plant Protection System Notional Architecture.

The DAS function's architecture is discussed in LAR Framework Document Section 3.4.6. DAS functions in this design concept will be hosted on a NSR DCS as shown on the right side of Figure 2. For appropriate interface of the N4S and ECCS portions of the DAS function, an Equipment Interface Module (EIM) is required. The EIM provides the priority logic defined in Digital Instrumentation and Controls Interim Staff Guidance #04 (DI&C-ISG-04), Revision 1, "Highly Integrated Control Rooms & Digital Communication Systems" [Reference 6], Section 2, "Command Prioritization." The logic in the EIM is required to be sufficiently simple, subjected to equipment qualification tests, and completely testable, thus avoiding issues with common cause failure (CCF). More summary detail on the DAS function's architecture is provided in Section 3.6.2 below.

The modernized HSI architecture design concept is discussed in LAR Framework Document Section 3.4.5. This architecture sets precedent in the nuclear industry. In the PPS System Architecture, the standard HSI device is identified as a DKT (which provides display(s), a keyboard, and a trackball [or touchscreen functionality]), To provide data to the operator, each channel and division provides data to redundant PPS video generators (identified as DKT Interfaces), which are then connected using fiber optic links to a SR switched network consisting of DKT Switches to drive DKTs. DKTs are used by Operations staff in the CR and for Maintenance and Engineering staff when required in the Auxiliary Equipment Room, where the logic solvers are installed.

PPS CR indication is provided on the DKTs, except in rare instances where a diverse distinct physical display is required. The SR DKTs are connected to the SR DKT Interfaces through SR Switches to allow the operators to connect any DKT to any digital plant system (e.g. the PPS, NSR DCS, or the corporate business network, etc.) in such a way that no cross-talk between these digital plant systems is possible. The DKTs also provide soft control capabilities for the watchstanding Reactor Operator. The DKTs also provide navigation for the screens generated in separate DKT Interfaces assigned to channels and divisions. Manual SR controls (physical switches and pushbuttons) are retained where necessary to meet regulatory requirements. Most of the existing CR manual switches migrated to soft controls provided on

the DKTs, which feed either PPS application logic or DAS application logic. More summary detail on the HSI architecture is provided in Section 1 below.

A second path also exists for data display. Each PPS channel transmits engineering unit, status, and vote input data to the DCS independently. Each PPS division also transmits status and actuation status data to the DCS. This data can be used to replicate PPS displays on the DCS as well as to create additional displays on the DCS using multiple channels and divisions of PPS data. The DCS also provides NSR functions, including alarming, PPS interface to the annunciators, trending, long-term data storage, and the comparison and recording of the PPS and DAS data to replace the operator's manual channel checks.

By use of redundant fiber optic connections from channels to divisions, from channels to the DCS, from divisions to the DCS, between single channels and DKT Switches, between single divisions and DKT Switches, and between DKT Switches and DKTs, separation and isolation are maintained. By using fiber optic links, issues with electrical isolation and EMC are reduced. By requiring compliance with DI&C-ISG-04, Revision 1, Section 1, "Interdivisional Communications," independence and messaging reliability are assured. Redundancy is provided for reliability and availability, as well as providing a means of ensuring that a failed transmitter or receiver does not reduce the PPS reliability. Redundancy also provides additional protection against multiple bit errors, since bit errors are not likely to occur in both redundant links simultaneously.

One major change incorporated in the PPS architecture deals with the voting scheme. The existing design is shown in Figure 3 below, using the RPS as an example. In this figure, the outputs of the existing RPS trip modules are shown as inputs to the two divisions. Any parameter in either channel within a division and any parameter in either channel within the other division can together generate a scram.

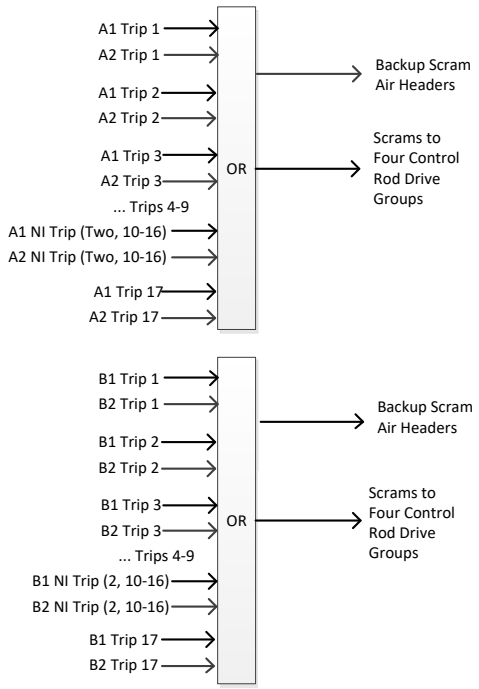

Figure 3. Existing RPS Plant Scram Logic.

The plant parameters do not have to match in any way, and two single failures in separate channels can generate a scram or a half scram. The existing RPS seventeen trip numbers, shown in Figure 3 for the existing RPS, reference a list in the LAR Framework Document that is not repeated here. The only significant change in the voting for any of these in the new design concept is to Trip 1, the manual scram pushbuttons in the CR. With the change from relay logic to digital logic, the manual scram pushbuttons

are now required to function independently of the PPS logic, such that a PPS software common cause failure (SCCF) would not prevent the operator from initiating a scram.

Figure 4 below shows the modernized PPS voting scheme. In this figure, the digital PPS channel data is shown as inputs to the two RPS divisions. The four votes from each input parameter are evaluated in the two-out-of-four voter logic in each division. Any two-out-of-four condition causes a voter in each division to initiate a scram in that division. Since both divisions receive the same information from the channels and both divisions implement the same logic, this eliminates the condition in the existing RPS where only one division can generate a half scram based upon inputs unique to that division. Also, if the two channels in a single division in the current RPS detect a plant condition requiring a scram and no channels in the other division detect the condition, the plant will only initiate a half scram. In the modernized PPS, both divisions are provided with the information and both divisions appropriately initiate a scram when required by the voting function.

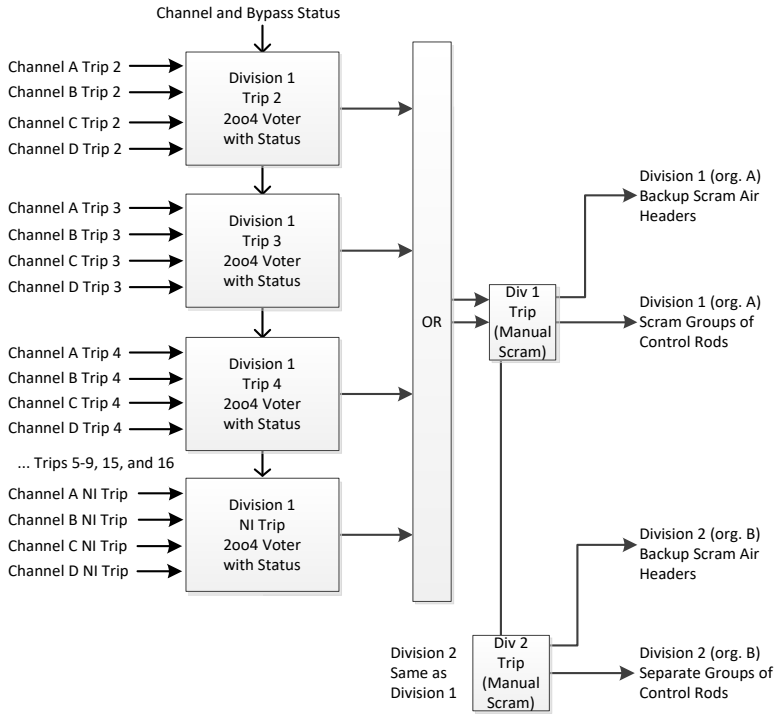

Figure 4. Modernized RPS Plant Scram Logic.

Each PPS channel within a PPS division is intended to consist of one or more (if necessary) totally independent copies of the PPS standard platform. Portions of the PPS channels supporting the N4S and ECCS are different, to accommodate the provision of only two field sensors or a single train system (e.g. HPCI and RCIC). Each PPS channel independently samples the required PPS channel-specific analog and discrete inputs hardwired to that channel. Each PPS channel independently converts the analog inputs to engineering units and compares the engineering units to the setpoint values for trip or actuations, implementing the required bi-stable function with preset hysteresis. Each PPS channel has no communication or knowledge of the actions or votes from the other three independent channels. Each PPS channel will independently provide votes to scram or not scram or to actuate or not actuate for each input. If multiple copies of the PPS platform are necessary to implement one channel's functions, these separate PPS platform instantiations within one independent PPS channel can communicate only within that channel.

If multiple copies of the PPS platform are necessary to implement one division's functions, these separate instantiations within that division can communicate only within the same division.

The existing RPS, N4S, and ECCS had many sets of four-way redundant transmitters on the same instrument taps, calibrated with the same range, feeding identical trip units. To simplify the system and to ensure that the PPS is working with a consistent set of process parameters, duplicate copies of multiple sets of four-way redundant transmitters are eliminated, leaving one set of four-way redundant transmitters, which will be used by all PPS functions. The complete LAR does not include transmitter removal. Rather, the functional requirements baselines and LAR Framework Document merely document which transmitters will be retained. A separate Design Change is anticipated to remove the surplus transmitters and instrument tubing.

Figure 5 below shows a divisional view of the PPS, including the DAS function in the plantwide DCS and signal interfaces from the SR field sensing elements to the NSR DAS function inputs. A bidirectional arrow is shown between the two DAS segments to indicate that each samples two channels of information, performs engineering unit conversions, performs bi-stable evaluations, and then shares the channel's votes to scram, not scram, actuate, not actuate, isolate, and not isolate through the communication links between the two segments. This conceptual architecture mimics the design of the PPS and RRCS functions being replaced. This architecture ensures that the DAS function in the DCS is independent of the PPS, and thus PPS SCCF cannot adversely affect the operation of the DAS function in the DCS. Similarly, SCCF in the DAS function in the NSR DCS cannot adversely affect operation of the SR PPS.

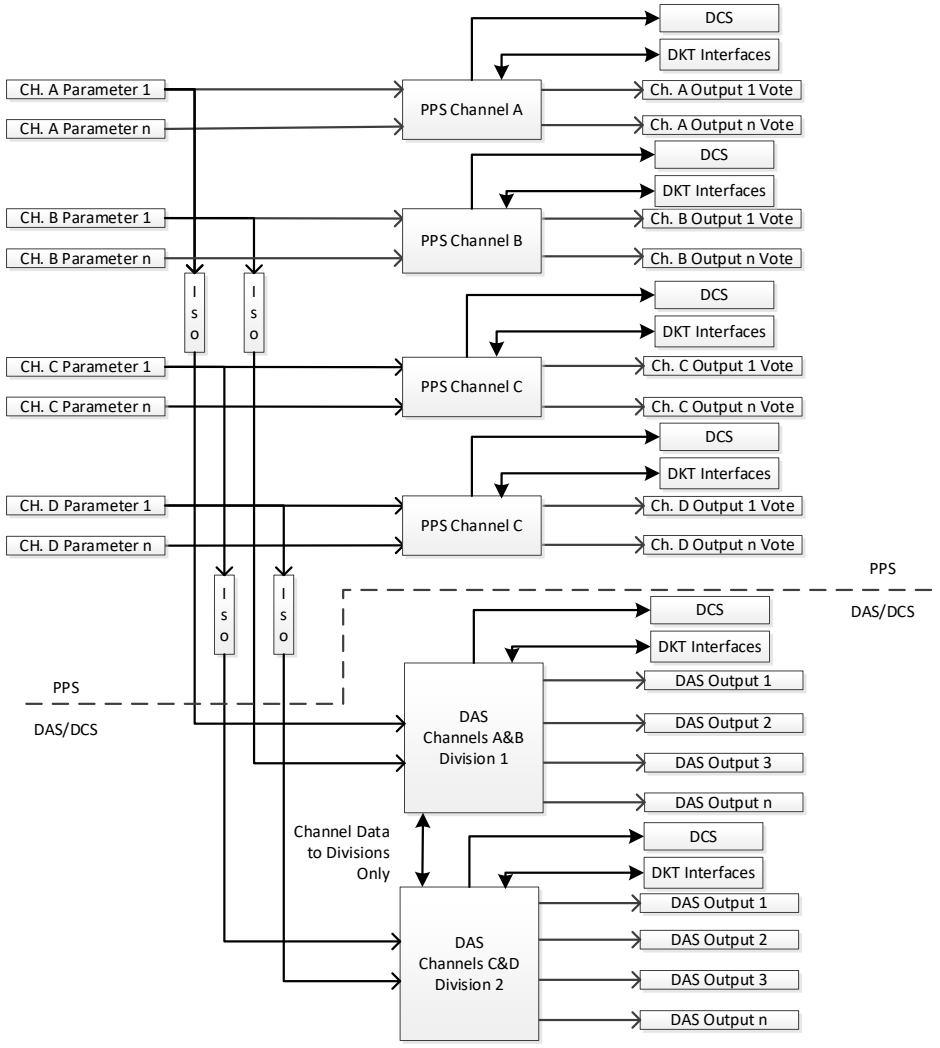

Figure 5. PPS and DAS/DCS Architecture.

3.6.1.1 Research Decisions and Platform Attributes that Support Licensing

The following key platform attributes were adopted by this research to achieve maximum PPS technical capabilities, while at the same time minimizing costs and regulatory risk. Some of these were driven by the general nuclear industry regulatory environment, such as the advantage in leveraging a platform that the NRC has already evaluated and accepted. Others are based on the existing LGS license, where Exelon and LWRS researchers deliberately decided to minimize change to the design functions.

1. To support use of the AR process in DI&C-ISG-06 Revision 2, the implementing utility is required to select one of the NRC prequalified SR platforms with a current NRC SE Report. The PPS design concept makes use of prequalified platform abilities, including field sensor inputs, discrete outputs, communication, and propagation. The design concept intends to remain within the borders established by the latest revision of the selected vendor's Licensing Topical Report and the NRC's SE Report, although the LAR Framework Document does have the potential to expand the boundaries. It is expected that expanding these boundaries may require enabling additional features that are supported by the vendor platforms but not necessarily covered by the associated NRC SE Report.
2. All communications are based on the precepts in DI&C-ISG-04 section on interdivisional communication.
3. The overall PPS design concept retains the ability to perform all of the RPS, N4S, and ECCS safety functions required by the existing license. The number of changes to functionality is small, as summarized below:
    a. The modernized PPS moved from the existing voting scheme to a voting scheme where all available data is made available to all divisions. This new voting scheme is consistent with first-echelon safety systems designs that have more recently been approved by the NRC. This new voting scheme enhances plant operational performance while providing same or better plant safety.
    b. For the Residual Heat Removal function, the modernized system adds the ability for the operator to request various NSR modes of RHR operations. By automating the functions and interlocks under manual operator control, the research team concluded that the automation eliminates various human performance errors, which had the potential to have large safety consequences.
    c. The addition of a manual SLCS inhibit capability in the CR reduces the potential for human performance error during ATWS maintenance, causing an unintended injection of SLCS. This capability is added based on several Operational Events where partial SLCS injections were caused by human error.
4. One important licensing research decision was to reduce the number of identical sets of redundant field sensors. In the existing design, a separate set of four sensors may be provided for the RPS, another set for N4S, and multiple sets for ECCS. In the modernized design concept, one set of the four channelized sensors is retained and used for all PPS functions, improving consistent PPS operational performance ensuring that the PPS operates from consistent data, rather than from multiple sets of what should have been the same data as provided by separate sensors measuring the same physical process value. Surveillance testing is simplified and reduced by eliminating all but one of the identical sets of four redundant transmitters and providing the data as PPS data. Eliminating the unnecessary identical sets greatly reduces the surveillance test and calibration costs for the field instrumentation.
5. Since all RPS, N4S, and ECCS field data are now PPS data, some of the common application logic is combined, such that there is now only one set of logic determining if, for example, reactor water level is beneath Level 2, instead of multiple copies, which allows for the concentration of design and verification and validation (V&V) effort on a single set of bi-stables with hysteresis, rather than

diluting design and V&V attention by implementing a large number of identical sets of logic, differing only in the output point names assigned within the logic.

6. Most surveillance test requirements on the current RPS, N4S, and ECCS are expected to be eliminated. This is based on a comparison of coverage of what would have been the surveillance test requirements against the fault and failure diagnosis capabilities of the envisioned platform and application software. Some platforms prequalified by the NRC have eliminated many surveillance tests such as logic system functional tests and propagation time tests. The only remaining tests are those that require field equipment to respond and thus cannot be demonstrated solely through the logic solver. Elimination of surveillance tests will require additional licensing activity to potentially include a Failure Modes, Effects, and Diagnostics Analysis (FMEDA) of the platform and analysis of the coverage of the existing self-tests and self-diagnostics in the platform and any required supporting platform applications against the faults and failures that would have been uncovered by traditional surveillance tests.
7. While not uniquely a licensing requirement, the intent is to select a PPS platform and an HSI switching solution with long-term support by the platform vendor and HSI switching solution vendor. This avoids having to repeat this licensing process as necessary digital equipment obsolescence management activities occur for the remaining life of the plant. A strong obsolescence program that produces form, fit, and function replacement parts will provide a long-term solution for the PPS and HSI switching solution that will avoid the need to repeatedly relicense the PPS or the HSI switching solution, as long as the vendors' solutions remain viable.
8. A modernization goal is to ultimately achieve a state where most plant I&C functions are migrated to either one SR platform or one NSR platform. The implementing utility will choose one of the prequalified SR platforms for the PPS. While additional SR equipment will exist (e.g., the safety related GEH NUMAC LPRM/APRM/OPRM, radiation monitors, HVAC, embedded digital in the electrical power systems), this selected platform is intended to be the host for the safety systems, including SR displays for Post Accident Monitoring data. The same considerations exist for the NSR platform. This promotes the standardization and reduction in lifecycle support costs over time, while reducing licensing risk by reducing the number of SR I&C systems.
9. The research team identified a NSR plantwide DCS as the platform on which to implement the DAS function. This supports items #7 and #8 directly above while at the same time providing for a solution, which can be shown to be licensable by the NRC. A DAS function is likely required, since most prequalified platforms do not provide sufficient diversity to resolve SCCF regulatory concerns. A D3 Analysis is to be performed in accordance with NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," [Reference 7] and Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," [Reference 8] to determine which (if any) functions from the N4S and ECCS must be duplicated in the DAS function running in the NSR DCS. It is expected that the existing ATWS function provided in the SR RRCS will be migrated to the DCS as part of the DAS function.
10. All SR to NSR isolators required for the DAS to function (including when RRCS ATWS functions are migrated to the NSR DAS function) and for Sequence of Events (SOE) functionality are part of the scope for the PPS and validated as part of PPS testing. This ensures the end-state PPS configuration is fully defined as part of the PPS LAR.
11. The design concept provides all PPS and DAS data to the NSR DCS for display and archiving in a data historian. This, along with the SR DKT architecture presented in Section 3.6.3, provides for a flexible HSI solution for the CR that supports both interim states and the envisioned hybrid end-state for the CR.

12. Cross-comparison of data from all channels is useful to detect field sensors that are not operating correctly, which has been done through manual channel checks performed by an operator periodically (e.g., every shift). This function is useful to detect issues with field sensing or analog to digital conversion in the logic solvers. The modernized system compares all data from all channels and divisions, including data from the DAS function in the NSR DCS, and alarms on persistent disagreements outside some individually selectable band, which is likely to be based on the accepted calibration band for each sensed parameter. This further reduces surveillance requirements.

3.6.1.2 Challenges

It is recognized that some of the items listed in Section 3.6.1.1 challenge established regulatory precepts. These were chosen tactically by the research team to provide the necessary lifecycle cost reductions to support long-term nuclear plant economic viability, while not overly challenging the DI&C-ISG-06, Revision 2, AR process. Some areas of potential licensing challenges, and how they were addressed, are outlined below.

1. Prequalified platforms comply with modern regulatory guidance and IEEE standards. As an example, LGS NPP is licensed to much older standards, which predate digital applications in NPP. Demonstrating PPS compliance with both old and new standards would not be efficient. To address this, changing the licensing basis for just the logic solver replacement (limited to the connections to the existing field sensor, field actuator, and the logic solvers as described in the LAR Framework Document) to new standards appears to be an appropriate path forward, as identified in this research.
2. Reducing the number of sets of redundant plant transmitters, licensed and installed as separate sensing devices, may present challenges in the licensing domain. To address this, only identical transmitters, calibrated to the same ranges and using the same calibration procedures, were targeted for reduction by this research.
3. The basic design concept of the SR DKT architecture to support HSI in the CR and Auxiliary Equipment Room as proposed may present challenges to the NRC I&C reviewers, in that there are no defined channel or division specific displays. Rather, the design concept allows for the sharing of all displays among all video capable systems, whether SR, NSR, or business computing networks. To preclude the NRC issues with non-safety related displays controlling SR equipment, all DKT architecture to equipment displays are qualified SR as identified by this research. DKT architecture communications are based on the precepts in DI&C-ISG-04. Location and information display will be controlled administratively. The DKT Switch will be configured so that only DKTs located at the Reactor Operator Workstation(s) can operate SR plant equipment.
4. Reduction in surveillance testing was a primary driver to reducing lifecycle costs. At the same time, this reduction precludes many operator and maintenance errors which can negatively impact plant performance. The PPS design concept will make use of the same design precepts as are being evaluated by the NRC for Pressurized Water Reactors. Researchers concluded that the same precepts are applicable to a BWR, with appropriate changes for the reactor technology and measured parameters.

3.6.2 Non-Safety Related Diverse Actuation System Architecture

This research presupposes a scenario where a D3 analysis of the implementation of the NRC prequalified platform shows that DAS functionality is required to address the potential for a CCF of the SR platform. This research proposes that DAS functionality be implemented using a NSR DCS. A D3 Analysis is to be performed to determine which (if any) functions from the N4S and ECCS must be duplicated in the DAS function implemented in the NSR DCS. This research targets the existing ATWS function provided in the SR RRCS for migration to the DCS as part of the DAS function.

The complete DCS architecture is not described in Appendix C. Only those aspects of the DCS architecture that directly affect the currently defined DAS function are provided, to provide only those features that the authors view as key and essential for the DAS function.

All of the major industrial DCS vendors have similar features and capabilities, which are incorporated in the DAS function in the DCS, shown in Figure 5 above. Multiple utilities have determined that several DCS platforms provide an acceptable basis for implementing augmented quality NSR control functions, including the provision of acceptable software tools and capabilities. The DCS platform will thus provide an acceptable basis for building a DAS function requiring augmented quality.

For the DAS, two segmented controllers are provided. If the amount of application logic results in insufficient spare capacity, additional pairs of segmented controllers are added. Each of the segmented controllers supports two independent software functions (i.e., channel functions) that read the isolated analog and discrete inputs, convert the analog inputs to engineering unit values, and perform independent bi-stable functions against setpoint constants. The channel functions then provide their votes to not scram, scram, actuate, or not actuate for each parameter to two separate controllers, each of which is the logical equivalent of a PPS division. Each channel function provides data directly to both controllers through normal DCS processes (i.e., named variables in memory). The divisions then implement algorithms that provide the same function as in the PPS and output equivalent discrete signals to the EIMs or directly to the field for the ATWS functions. If the HPCI and RCIC functions are provided in the DAS, methods are provided to implement algorithms that provide the same function in the DAS as in the PPS to support existing flow, new reactor water level, and new reactor pressure control. Methods will be provided for the operator to control these DAS algorithms and control setpoint values.

3.6.2.1 Research Decisions and Platform Attributes that Support Licensing

The platform chosen for the plantwide NSR control and monitoring system is considered proven in-use and selected for high reliability and availability. The following considerations provide a basis for the use of the platform for control, monitoring, and DAS functions.

1. The DCS platform is accepted as a sufficient base on which to build augmented quality applications, including the N4S and ECCS DAS functions and the ATWS function as part of the DAS.
2. The DCS provides a high integrity basis on which to build a complete, appropriately segregated digital control system.
3. The DCS has a sufficiently broad set of analog and discrete inputs and outputs to support the control, monitoring, and DAS functions.
4. The SR to NSR isolators provided by the PPS are of sufficient quality and accuracy to support the DAS functions provided in the DCS.
5. The DCS provides DCS DKT Interfaces (video generators that are interfaced to the video, keyboard, and trackball data streams) in a similar manner as the PPS DKT Interfaces. The DKT Switches and DKTs are thus able to provide switched data access to the DCS as required by the CR operators.
6. The DCS electromagnetic compatibility (EMC) evaluation establishes that the DCS has sufficient immunity and limited emissions for EMC concerns, sufficient to support an augmented quality function.
7. The control and monitoring applications running on the DCS platform are segmented appropriately to resolve regulatory concerns with SCCF.
8. The DCS platform supports the data historian, data display, trending, and similar functions required to eliminate NSR strip chart recorders. This also allows for the elimination of strip chart recorders where the instantaneous indication function is SR but the display and retention of trending data is not SR. Limited trending is provided in the SR DKTs.

9. The DCS platform supports the acquisition of SOE and first-out data with millisecond accuracy, allowing for the elimination of separate SOE recorder functions and the future elimination of CR annunciator systems.
10. For the early detection of data collection issues in the PPS or DAS, the DCS collects data from the PPS and DAS function and cross-compares what should be redundant sensors across PPS channels and across the functions in the DAS. Any persistent errors that are greater than a configurable error band, which could be based on the calibration limits of the individual sensors, generates an alarm or notification (as appropriate) for resolution. This provides for the continuous detection of errors in transmitters or analog to digital conversion.

3.6.2.2 Challenges

It is recognized that some of the items listed in Section 3.6.2.1 challenge established regulatory precepts. These were chosen tactically by the research team to provide the necessary lifecycle cost reductions to support long-term nuclear plant economic viability. Some areas of potential regulatory and technical challenges and how they were addressed are outlined below.

1. Researchers selected a NSR plantwide DCS as the platform on which to implement the DAS function. This is a novel approach for providing the DAS function. This supports the modernization goal to ultimately achieve a state where most plant I&C functions are migrated to either one SR platform or one non-safety related platform. This goal supports reducing the number of independent I&C platforms while meeting regulatory requirements. This reduces acquisition and lifecycle costs associated with maintaining a larger number of disparate I&C platforms. The research decisions and platform attributes to support licensing identified in Section 3.6.2.1 above are intended to provide a solution that can be shown to be licensable by the NRC.
2. In order to validate that the PPS and DAS functions operate correctly together, the PPS and DCS should be tested as an integrated whole before being installed in the plant. If integrated testing of the PPS and DAS functions are not implemented as factory acceptance testing, overlap testing should be performed to sufficiently demonstrate that the PPS, EIM, and DAS function in the DCS provide the prioritized output functions. This testing is in addition to the independent testing for each system. It is highly recommended that the utility hold one vendor responsible for implementing both the PPS and the DAS function, since having two separate vendors has been demonstrated to result in “finger pointing” when integration testing challenges arise rather than resolution.
3. The issues associated with installing the PPS in phases in different refueling outages are not considered in this report. These are left to be addressed by the implementing utility.

3.6.3 Shared, Safety-Related Human-System Interface Architecture

The SR DKT architecture identified by this research provides for a flexible HSI solution for the CR that supports both the interim states and the envisioned hybrid end-state for the CR. A minimal number of manual switches for the PPS remain in the CR. The remaining manual hardwired PPS switches are retained as diverse backups for the PPS itself and act directly on such functions as reactor scram, disconnecting the power from the scram and backup scram valves. All other operator interactions use soft controls on the video displays, using the DKT architecture shown in Figure 6.

The DKT HSIs provide the operator with a display of all field parameters monitored by the PPS as well as DCS screens, to include DAS function screens. The DKTs also provide selected status data for the watchstanding operator, allowing the operator a more complete view of plant parameters than are provided by the existing systems. The existing RPS only informs the operators that a scram or half scram is in progress and provides field parameter data only if the operators dispatch personnel to go up to the Auxiliary Equipment Room and verbally provide data from the analog trip units. The existing N4S and ECCS supply more data to the CR but still require manual data actions to provide data from the analog trip units in the Auxiliary Equipment Room.

Using the switched DKT approach for the primary CR HSI enables an incremental approach to a modern CR. This approach supports the movement of functions within the CR by switching the DKT to a different DKT Interface, repurposing individual DKTs as needed, rather than cutting and patching steel CR cabinets to physically remove and reinstall HSIs in other locations. Other approaches are equally acceptable, as long as the incremental capabilities of the switched DKT approach are incorporated.

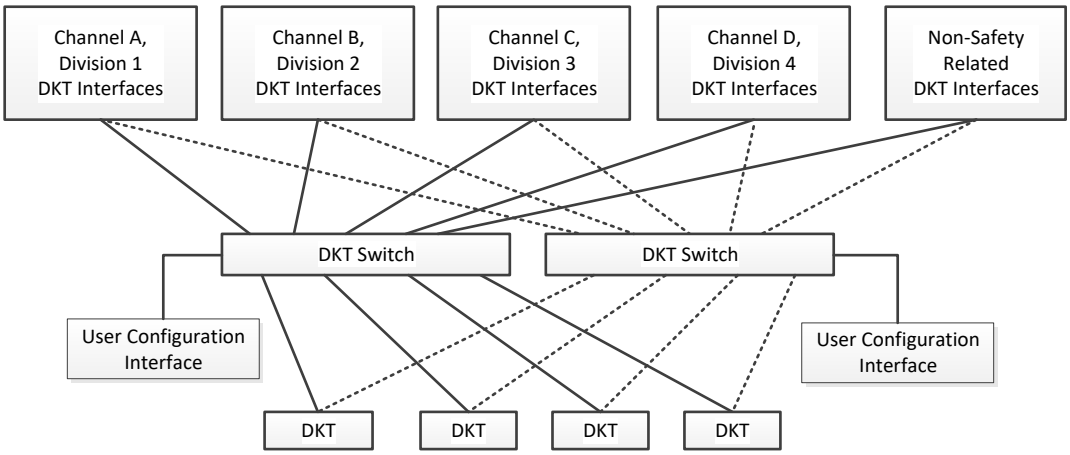

Figure 6. Proposed Display, Keyboard, and Trackball (DKT) Switch Architecture.

3.6.3.1 DKT Switched Architecture

As shown in Figure 6, the selected DKT architecture replaces most indicators and meters as well as most manual operator switches with video displays and soft controls on those video displays. By eliminating indicators and meters and reducing manual controls, the working portion of the CR is made more compact and watchstanding operators can devote more attention to managing plant state and less to accessing and mentally integrating data from disparate sources. When proper HFE techniques are applied, this reduces operator workload and operator errors.

The DKT architecture provides flexibility by not tying a SR function to one location in the CR. Any SR or NSR function can be accessed from any DKT in the CR, with the only restriction being that only DKTs at the watchstanding Reactor Operator's locations have the ability to issue commands to the application logic in the PPS or DCS. This flexibility allows the operators to assign the BISI or Safety Parameter Display System (SPDS) or any other function to any display in the CR, providing data where the data is needed, which is not possible with the existing CR HSI. In the existing CR, during accidents or transients, operators are stationed at various locations in the CR to verbally relay plant status data to the Operations staff manning the CR. In some currently licensed modern nuclear plant CRs, fixed location SR displays provide data from one channel and division, requiring four side-by-side fixed location displays to display all data, along with additional redundant displays to meet the single failure criterion. In those CRs, failure of any one of the fixed location SR displays requires the Operations staff to use a display in another, often inconvenient location until the primary display can be replaced. In this CR, the operator can move to any available DKT and continue with no significant impact on the operator's work processes.

DKT Interfaces are redundant, such that the failure of any element of any one DKT Interface does not deprive the CR of data or control capabilities associated with the device that suffered a single DKT Interface failure. Each DKT Interface provides dual fiber optic connections to redundant DKT Switches. The redundant DKT Switches support the hot-swapping of internal components should a module fail. To maximize reliability and availability, power supplies and controllers within the DKT Switches are redundant. Failure of either DKT Switch Power Supply is alarmed, but the DKT Switch continues to operate. Failure of a DKT only requires the operator to select and use a different DKT. Failure of one of the DKT fiber optic links to a DKT Switch only requires the operator to select the desired DKT Interface again and the DKT communication routed to the other DKT Switch.

The DKT system configuration is maintained in a separate module associated with each DKT Switch. This module interfaces with its respective DKT Switch. The separate module provides the configuration interface to the DKT Switch, separating the configuration management functions from the switching software and thus simplifying the software in the DKT Switch. One function accomplished by the DKT configuration module is to configure the DKTs so that only the Reactor Operator Workstation DKTs can perform soft control functions.

3.6.3.2 Research Decisions and DKT Architecture Attributes that Support Licensing

The following research decisions and DKT architecture attributes were adopted to achieve a standard, universal, and flexible HSI solution while minimizing costs and regulatory risk. This solution also provides maximum flexibility to support multiple transition states driven by SR and NSR I&C upgrades, which will by necessity occur over an extended period of time.

Some of the items listed in Section 3.6.3.1 challenge established regulatory precepts. These were chosen tactically by the research team to provide the solution described above while at the same time providing necessary lifecycle cost reductions to support long-term nuclear plant economic viability. Some areas of potential regulatory and technical challenges and how they were addressed are outlined below.

This design concept supports the above objectives in the following ways:

1. The DKT architecture is based upon available technology currently certified for use in a cyber-security critical environment. This environment requires the capability to segregate classified data between separate connected systems and to prevent any possibility of cross-talk between these systems. Initial evaluations of one vendor's specific technology indicate that their equipment can be commercially dedicated for SR use.

    a. Commercial Grade Dedication (CGD) will require evaluations of each of the software sets in various separate devices, consisting of interfaces to the connected system (e.g. the PPS, the NSR DCS, business network) switching in the DKT Switch, routing configuration, and interfaces at the DKT. Software in the configuration module is considered a software tool and evaluated as appropriate for use. As software designed to be acceptable to the United States Department of Defense and intended for long-term maintainability by the vendor, the authors do not foresee any more than the normal issues with CGD of non-trivial software-based products.

    b. The DKT architecture equipment must be qualified for the operational environment. Based on a review of the evaluated vendor's product, temperature, humidity, power quality, and atmospheric pressure are not issues, as the product is designed as industrial equipment and will be installed in temperature- and humidity-controlled rooms. The lower frequency seismic waveforms may present challenges, based on the current qualification for military shock and vibration. The EMC environment required by NRC Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Revision 2 [Reference 9] is always a potential issue for commercial equipment, since commercial equipment is designed for a normal industrial environment, which typically has lower EMC stressors than listed in RG 1.180 Revision 2.

2. The proposed use of DKTs installs the devices in the CR and the Auxiliary Equipment Room above the CR. The connections between the DKT Interfaces and the DKT Switch as well as between the DKT Switch and the DKTs are over fiber optic cables that are routed within the confines of the CR and the Auxiliary Equipment Room. The DKTs do not have the ability to reprogram the PPS or DCS. The DKTs do not have the ability to overload the logic solvers with messages, since the DKT Interfaces and the video generators to which the DKT Interfaces are installed provide a second layer of message buffering as required by IEEE Standard 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" [Reference 10]. The PPS provides the initial layer of message buffering in the fiber optic transmit and receive modules.

3. All DKT architecture communications are based on the precepts in the United States Nuclear Regulatory Commission DI&C-ISG-04. There is no potential for the postulated failures that drove DI&C-ISG-04 to place restrictions on NSR multidivisional displays, since this architecture provides SR equipment and each DKT can only interface with one operator-selected channel/division at any time. An evaluation of the specific vendor technology referenced above indicates that that the DKT architecture can be shown to comply with the DI&C-ISG-04 concerns identified for multidivisional displays. The reviewed vendor's product had been tested to demonstrate that the cross-talk between switched connections was sufficiently low to support the use of the equipment for code word segregation of classified data, which exceeds any NRC requirement for cross-talk within equipment.
4. The attributes described in Item #3 directly above also address cyber security for the DKT architecture. While a gap analysis with the cyber-security requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks" [Reference 11] will need to be performed, it is expected that the number of gaps identified will be limited.
5. The DKT Interfaces, DKT Switches, and DKTs provide no data storage or means to issue commands to multiple divisions. The DKTs will provide only keyboard data and trackball data back to the DKT Interfaces. DKTs will not be purchased to support flash or thumb drives. This supports addressing both DI&C-ISG-04 communication concerns and 10 CFR 73.54 cyber-security concerns.
6. All connections are made on dual fiber optic links, with video data sent from DKT Interfaces through the DKT Switches to the DKTs and data from the keyboard, trackball, or touch screen sent back through the DKT Switch to the DKT Interface. All communication links provide electrical isolation.
7. Using a standard, universal, and flexible HSI solution will support a holistic Human Factors Engineering effort for the CR consistent with the implementation of a graded approach as described in NUREG-0711, "Human Factors Engineering Program Review Model" [Reference 12]. Following such an approach, interim CR modifications can be more cumulative in nature, rather than requiring rework when transitioning between interim states.
8. Any display can be set by the operators to show any data from any system.
9. Only Reactor Operators are "at the controls." The LAR Framework Document requires use of an allowable connections table within each DKT Switch. The DKT Switches are configured to only allow connections between the Reactor Operator DKTs and DKT Interfaces that possess a soft control capability. All other DKTs in either the CR or the Auxiliary Equipment Room are not allowed to connect to the DKT Interfaces that support soft controls. Of course, all DKTs support on-screen navigation for indication only.
10. Since any DKT can be set to show data from any system, the Operations staff can select the data needed to perform their intended action where the action is to be performed, rather than needing to verbalize data during normal and accident conditions with the existing system data displays widely dispersed and mostly not within the Senior Reactor Operator's vision. With data provided on both SR and NSR graphics, all users can see the data and status of the PPS functions, including the SRO, RO, Emergency Preparedness staff, and the Shift Technical Advisor
11. The SR DKTs implement the SR Post Accident Monitoring System (PAMS) display function, as the SR DKTs provide those parameters from the PPS. This eliminates the need for standalone PAMS devices in a way that is licensable while supporting lifecycle cost reductions. To ensure a diverse PAMS backup exists in case of a PPS SCCF, all DAS function data on the NSR DCS is separately available for display on the DKTs.
12. The BISI for SR systems can be displayed on any DKT and will be continuously visible based on an administrative requirement for the operators to ensure that one or more displays is set to the BISI graphic.

4. Requirements Baseline and License Amendment Framework Document Use

Utilities intending to perform BWR SR I&C upgrades and associated Diverse Actuation System (DAS) installations should tailor the vendor-independent functional requirements baselines and LAR Framework Document produced by this research for use on their particular BWR units. The utilities could then provide these documents to their selected vendor(s) as a starting point for the collaborative development of SR digital I&C requirements, leveraging a design based upon a SR platform prequalified by the NRC and a NSR DAS. A utility and their selected vendor should refine the requirements baselines and LAR Framework Document provided herein collaboratively, to conform them to a utility's specific needs for a particular unit and the capabilities of the selected vendor's product lines. Use of a NRC prequalified platform for the SR digital I&C design enables the use of the DI&C-ISG-06, Revision 2 AR process.

There are two pathways that are expected to be followed when doing this. Each is outlined below.

4.1 First Utility Use

Exelon Generation is pursuing first-echelon SR upgrades at LGS as a first adopter of the revised DI&C-ISG-06, Revision 2 AR process. Because of this and their participation in this research to date, the vendor-independent requirements baselines (Appendices A and B), LAR Framework Document (Appendix C), and the associated Research Decision Matrix (Appendix D) are already tailored to the LGS.

The LAR Framework Document presupposes the need to provide a NSR DAS function on a DCS to address the potential for a CCF of the PPS platform. Whether a DAS is needed at LGS will be independently determined by Exelon through the completion of a D3 analysis of the new LGS PPS platform design. If it is determined separately by Exelon that a DAS is necessary, DAS functionality would likely need to address the concurrent loss of RPS, N4S, and ECCS functions on the PPS platform. To address this potential need, the LAR Framework Document discusses an eventual transition of ATWS functionality to the DAS (resolving RRCS obsolescence), along with addressing the potential need for N4S and ECCS related DAS functionality. Since the current RRCS at LGS provides ATWS functionality to protect against RPS CCF, Exelon may choose to only implement N4S and ECCS related DAS functionality (if needed) in their PPS until such time as they replace the RRCS at LGS. If it is determined that a DAS is not necessary as part of the envisioned SR I&C upgrade at LGS, the portions of Appendices A –C that discuss it will not be applicable.

An objective of this research is to enable Exelon to leverage a subset of the functional requirements baseline document information in Appendix A that envelopes the PPS scope, along with LAR baseline document and Research Decision Matrix information in Appendices C and D, respectively, to engage potential vendors to supply their replacement PPS and associated DAS (if needed). As these documents are vendor-independent by nature, Exelon will need to consider the capabilities of the vendor's prequalified platform to provide the functionality Exelon desires in their selection process.

After the PPS vendor selection, Exelon and their vendor can continue to leverage the research products as described above in a collaborative engineering effort to adapt and conform those products with the capabilities of the selected vendor platform(s) and LGS needs. This will result in unit- and vendor-specific PPS and DAS functional requirements documents. It will also support generation of a unit- and vendor-specific LAR for submittal to the NRC for approval under the DI&C-ISG-06, Revision 2 AR process.

4.2 Subsequent Utility Implementers

It is envisioned that subsequent utility implementers interested in performing first-echelon SR upgrades on their BWR's will follow a process similar to that followed by Exelon LGS. Appendices A through D are intended to provide a starting point for their efforts. In their case, a unit-specific evaluation and revision will need to be performed on the data provided in Appendices A through D to address unit-specific differences and utility-specific goals and objectives. Subsequent utility implementers may

determine, for example, that research decisions as captured in Appendix D are not supportive of their particular situation. Results of this evaluation will need to be reflected in changes to Appendices A through D, as appropriate. Once this is completed, the vendor and regulatory engagement process would be similar.

Additionally, subsequent utility implementers could, with Exelon's cooperation, benchmark the Exelon effort and leverage the results of that effort, along with the research products contained herein, to best tailor them to achieve their objectives.

5. References

1. Code of Federal Regulations, Section 10, Part 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants."
2. Digital Instrumentation and Controls Interim Staff Guidance #06, Revision 2, "Licensing Process."
3. Electric Power Research Institute Report 3002011816, "Digital Engineering Guide: Decision Making Using Systems Engineering."
4. Code of Federal Regulations, Section 10, Part 50, Appendix A "General Design Criteria."
5. Nuclear Energy Institute 06-02, Revision 6, "License Amendment Request Guidelines
6. Digital Instrumentation and Controls Interim Staff Guidance #04, Revision 1, "Highly Integrated Control Rooms & Digital Communication Systems."
7. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems."
8. "Branch Technical Position Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," BTP-7-19. Revision 7.
9. Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Revision 2.
10. Institute of Electrical and Electronics (IEEE) Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
11. Code of Federal Regulations, Section 10, Part 73.54, "Protection of digital computer and communication systems and networks."
12. NUREG-0711, Rev. 3, "Human Factors Engineering Program Review Model," Nuclear Regulatory Commission (2012).

Appendix A

Vendor-Independent Boiling Water Reactor Plant Protection System Functional Requirements Baseline

MPR

1129-0172-SPEC-001
Revision 2

Vendor-Independent Boiling Water Reactor Plant Protection System Functional Requirements Baseline

Prepared for: Battelle Energy Alliance, LLC

Preparer:	Paul Heaney	E-signed by: Paul Heaney on 2020-05-18 13:18:09
Reviewer: (RPS rqmnts Rev 0A)	Timothy Walsh	E-signed by: Timothy Walsh on 2020-05-18 13:39:06
Reviewer: (RCIC rqmnts Rev 0A)	Erik Wiker	E-signed by: Erik Wiker on 2020-05-18 13:34:43
Reviewer: (HPCI/ADS rqmnts Rev 0)	Greg Hadley	E-signed by: Greg Hadley on 2020-05-18 13:22:32
Reviewer:	Matthew Minkoff	E-signed by: Matthew Minkoff on 2020-05-18 14:07:15
Reviewer:	David Herrell	E-signed by: David Herrell on 2020-05-18 13:49:55
Reviewer:	John DiBartolomeo	E-signed by: John DiBartolomeo on 2020-05-18 13:36:30
Approver:	R. Jason Gwaltney	E-signed by: R. Jason Gwaltney on 2020-05-18 14:13:44

QA Statement of Compliance

This document has been prepared, reviewed, and approved in accordance with the Quality Assurance requirements of the MPR Standard Quality Program.

Created: 2020-05-18 13:18:09
Project-Task No. 1129G046-0172

MPR Associates, Inc.
320 King St. • Alexandria, VA 22314
(703) 519-0200 • www.mpr.com

Vendor-Independent Boiling Water Reactor Plant Protection System Functional Requirements Baseline

RECORD OF REVISIONS		
Revision Number	**Pages /Sections Revised**	**Revision Description**
0	All	Original Issue
1	Cover Page Section 1.5.3 Appedices A.1, C.1, D.1, E.1, F.1 and G.1 Appendix H.1	Revised title Added “SR” to describe PPS Added GDC 1 Revised PPS85, PPS87, PPS88, PPS105 and PPS156
2	Appendices B.2, C.2, D.2, E.2, F.2, G.2	Revised system division designations Added CS-FR-294 and CS-FR-295 to Appendix E.2

Table of Contents

Figures

1.0 Introduction

1.1. Purpose

This document identifies vendor-independent Plant Protection System (PPS) safety related (SR) digital platform functional requirements and associated functional requirements for applications that are to be hosted on the PPS. These baseline Boiling Water Reactor (BWR) instrumentation and control (I&C) functional requirements have been developed as a tool for the nuclear industry to engage vendors in a collaborative effort to conform them with the needs of a particular unit and with the capabilities of the selected vendor's product line.

To provide a firm foundation for this requirements baseline, a particular nuclear plant was selected as a reference for this effort. With the cooperation and support of Exelon Generation, the Limerick Generating Station Units 1 and 2 (LGS) was chosen as the reference plant for this effort. Because of this, the information in this document is tailored to the LGS plant design and reflects design decisions made by the Exelon design team to achieve objectives associated with their digital transformation plans. Exelon is using these baseline requirements as part of a pilot effort to perform first echelon SR I&C upgrades at LGS.

When used by other utilities, the baseline requirements provided herein need to be adapted to conform to that utility's particular unit design, the equipment capabilities of that utility's selected vendor's equipment, and to that utility's particular I&C digitalization strategy.

1.2. Background

The designs of the existing BWR SR systems are based on analog and relay component technology that are obsolete and becoming difficult to maintain. In order to address this concern, a solution that supports an overall digital transformation strategy is being pursued. The objective within this document is to provide the framework for an initial migration of select SR systems to a common digital platform, which establishes a prescriptive and cost-effective approach that can support similar future endeavors.

1.3. Description of Scope

1.3.1. The scope of this specification encompasses the following SR systems at each of the LGS units, Unit 1 and Unit 2:

- Reactor Protection System (RPS)
- Nuclear Steam Supply Shutoff System (N4S)
- Emergency Core Cooling Systems (ECCS)
  - Core Spray (CS)
  - High Pressure Coolant Injection (HPCI)
  - Reactor Core Isolation Cooling (RCIC)
  - Low Pressure Coolant Injection System (LPCI) mode of Residual Heat Removal (RHR)
  - Automatic Depressurization System (ADS)

ECCS represents the "family" of systems that provide core cooling. ECCS is not an individual system

1.3.2. This document provides the design, functional and performance requirements for the instrumentation and control (I&C) functionality that represents, to the extent practical, the licensing and design basis of the original systems.

1.3.3. Existing field sensors (that provide inputs to the SR system) and actuated devices (that receive outputs from the SR system) will remain unchanged for purposes of this document. Therefore, the requirements identified are focused on that portion of the original SR systems that support the protection and control logic functionality. Elimination of any Single Component Vulnerability (SCV) is dependent on the specific cost benefit analysis for eliminating such a SCV. While the elimination of SCVs is always desirable, eliminating SCVs in field sensors and actuated devices is beyond the scope of these functional requirements. Accordingly, SCVs in field sensors and actuated devices would be uniquely addressed as part of the design change process associated with each system migration to the common platform.

1.3.4. This document also identifies requirements that define the unique features and capabilities for the digital architecture that is to be employed as the common platform. The common platform supporsts further expansion to support future safety related applications.

1.3.5. The control logic and functionality associated with each of the individual systems listed in Section 1.3.1 shall reside as applications on a single common digital platform defined as the PPS. To that end, the original "systems" shall be termed SR functions within this PPS.

1.3.6. The functionality of the existing SR functions migrated to the PPS will replicate to the extent possible the original systems at LGS, but with additional enhancements that can be leveraged using the capabilities and features of the digital architecture.

1.3.7. The requirements for the PPS have been developed with a goal of reducing instrumentation, eliminating physical switches, indicators, and recorders (to the extent possible), and reducing/eliminating tech spec surveillances, calibration checks, loop calibrations, etc.

1.4. Approach / Concept

1.4.1. By using a single digital platform to support all SR functions, the design can significantly reduce the number of duplicate transmitters for monitored plant variables that are currently provided for the existing SR systems. The objective is to establish a minimum population of monitored parameters that can be shared by each of the SR functions on the PPS. The PPS concept leverages a two division / four channel arrangement that utilizes a 2 out of 4 (2oo4) voting scheme for each of the SR functions, to the extent practical.

Figure 1-1 provides a representation of this logic arrangement.

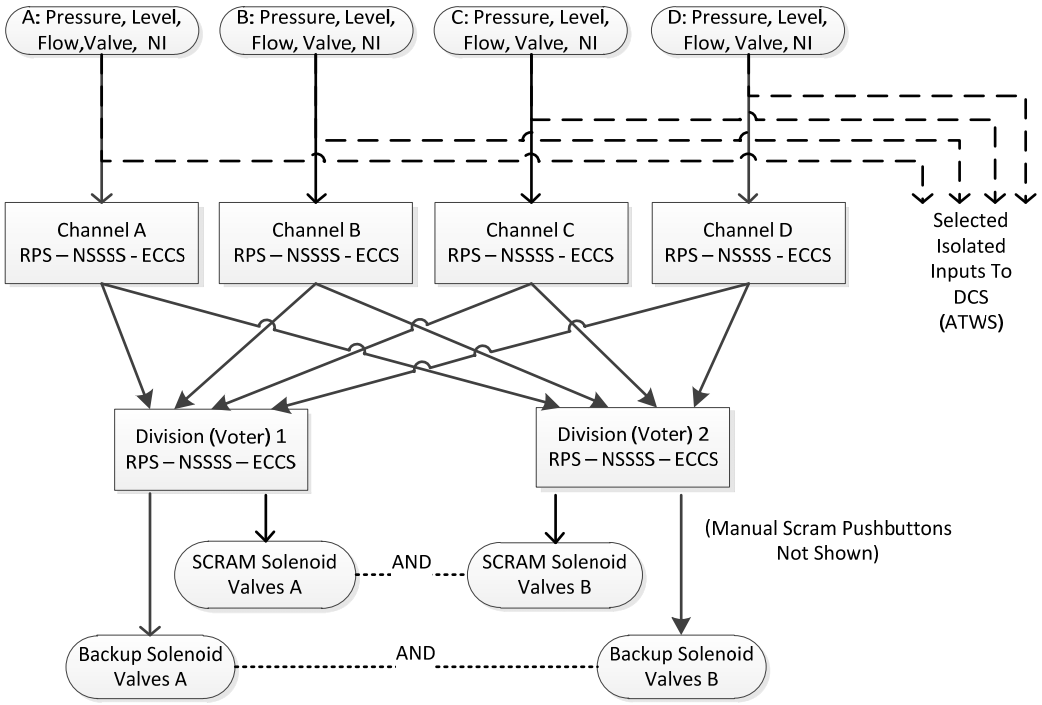

Figure 1-1. Logic Arrangement

1.5. Definitions

1.5.1. ECCS Response Time: The time interval for the instrumentation & control (I&C) portion of the system to fulfill its protective function. This begins with the receipt of an input signal at the input to the ECCS and ends with the ECCS generation of an output signal to an end device to perform its function.

1.5.2. N4S Response Time: The time interval for the instrumentation & control (I&C) portion of the system to fulfill its protective function. This begins with the receipt of an input signal at the input to the N4S and ends with the N4S generation of an output signal to an end device to perform its function.

1.5.3. Plant Protection System: The single common SR digital platform on which the SR protection functions and subfunctions shall exist as applications.

1.5.4. Reactor Protection System Response Time: The time interval for the I&C portion of the system to fulfill its protective function. This begins when the RPS input exceeds its trip setpoint at the channel sensor and ends with the RPS de-energization of the scram pilot valve solenoids.

1.5.5. SR protection subfunctions: Functions which replicate those provided by the LGS original SR systems (CS, HPCI, RCIC, RHR, ADS)

1.5.6. SR protection functions: Functions which replicate those provided by the LGS original SR systems (RPS, ECCS and N4S)

1.5.7. SR Systems: Systems that provide actions necessary to ensure safe shutdown, protect the integrity of radioactive material barriers, or prevent the release of radioactive material in excess of allowable limits. These safety-related systems may consist of components, groups of components, systems, or groups of systems.

1.6. Acronyms and Abbreviations

Term	Definition for this document
1oo1	One-out-of-one (voting)
1oo2	One-out-of-two (voting)
2oo2	Two-out-of-two (voting)
2oo3	Two-out-of-three (voting)
2oo4	Two-out-of-four (voting)
ADS	Automatic Depressurization System
AER	Auxiliary Equipment Room
APRM	Average Power Range Monitor
CFR	Code of Federal Regulations
CS	Core Spray
CSC	Containment Spray Cooling
ECCS	Emergency Core Cooling System
D3	Defense-in-Depth and Diversity
DAS	Diverse Actuation System (function in the DCS)
DCS	Distributed Control System
DST	Daylight Savings Time
ECCS	Emergency Core Cooling System
EIM	Equipment Interface Modules
EWS	Engineering Work Station
FR	Functional Requirements
FRU	Field Replaceable Units

Term	Definition for this document
FTP	File Transfer Protocol
GDC	General Design Criteria
HMI	Human-Machine Interface
HPCI	High Pressure Coolant Injection
HVAC	Heating, Ventilating, and Air Conditioning
I&C	Instrumentation & Controls
I/O	Inputs and Outputs
IT	Information Technology
KVM	Keyboard-Video-Mouse
LGS	Limerick Generating Station
LOCA	Loss of Coolant Accident
MCR	Main Control Room
MSIV	Main Steam Isolation Valve
N4S	Nuclear Steam Supply Shutoff System
NRC	Nuclear Regulatory Commission
NSR	Non-Safety Related
OPRM	Oscillation Power Range Monitor
PPS	Plant Protection System
RCIC	Reactor Core Isolation Cooling
RCPB	Reactor Coolant Pressure Boundary
RHR	Residual Heat Removal
RPS	Reactor Protection System
SCV	Single Component Vulnerability
SDC	Shutdown Cooling
SDOE	Secure Development and Operational Environment
SOE	Sequence of Events
SPC	Suppression Pool Cooling
SR	Safety Related
SRM	Source Range Monitor

Term	Definition for this document
SRO	Senior Reactor Operator
SSC	Systems, Structures and Components
T/C	Thermocouple
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UFSAR	Updated Final Safety Analysis Report
V&V	Verification and Validation
VDU	Visual Display Unit

2.0 System Description and Criteria

2.1. General Description

2.1.1. LGS is located on the east bank of the Schuylkill River in Limerick Township of Montgomery County, Pennsylvania, approximately 4 river miles downriver from Pottstown, 35 river miles upriver from Philadelphia, and 49 river miles above the confluence of the Schuylkill with the Delaware River. Each of the LGS units employs a GE BWR originally designed and licensed to operate at a rated core thermal power of 3293 MWt (100% steam flow) with a corresponding gross electrical output of 1092 MWe. The Units were rerated to a power output of 3458 MWt and a subsequent power uprate through measurement uncertainty recapture (MUR) to 3515 MWt.

2.2. General Design Criteria

2.2.1. The LGS design conforms to the requirements given in 10 CFR 50, Appendix A, "General Design Criteria for Nuclear Power Plants."

2.2.2. The plant is designed to limit the release of radioactive materials to the environment within the limits and guideline values of applicable government regulations pertaining to the release of radioactive materials for normal operations, and for abnormal transients and accidents. Safety-related systems are designed to permit safe plant operation and to accommodate postulated accidents without endangering the health and safety of the public.

2.3. Safety Related Systems Description

2.3.1. General

Safety related systems provide actions necessary to assure safe shutdown, to protect the integrity of radioactive material barriers, and/or to prevent the release of radioactive

material in excess of allowable dose limits. These systems can be components, groups of components, systems, or groups of systems.

2.3.2. Plant Protection System

The PPS is a safety related digital platform that will execute the protective and control functions for the SR systems identified in Sections 2.3.3 through 2.3.5.5. The control and logic functionality of these SR systems exists on the PPS as individual applications.

2.3.3. Reactor Protection System

The RPS initiates an automatic reactor shutdown by insertion of all control rods (scram) if monitored system variables exceed pre-established limits. This action is taken in time to prevent fuel damage and limits system pressure, thus restricting the release of radioactive material. The RPS overrides all operator actions and process controls.

2.3.4. Nuclear Steam Supply Shutoff System

The N4S initiates closure of various automatic isolation valves if monitored system variables exceed pre-established limits. This action limits the loss of coolant from the Reactor Coolant Pressure Boundary (RCPB) and the release of radioactive materials from the RCPB, the primary containment, and the reactor enclosure.

2.3.5. Emergency Core Cooling Systems

The ECCS is comprised of independent core standby cooling systems that maintain fuel clad temperatures below the limits of 10 CFR 50.46 in the event of a breach in the RCPB that results in a loss of reactor coolant.

2.3.5.1 High Pressure Coolant Injection System

The HPCI system provides and maintains an adequate coolant inventory inside the reactor vessel to limit fuel clad temperatures as a result of postulated small breaks in the RCPB.

2.3.5.2 Automatic Depressurization System

The ADS acts to rapidly reduce reactor vessel pressure in a LOCA situation in which the HPCI system fails to maintain reactor vessel water level.

2.3.5.3 Core Spray System

The CS system provides the capability to cool the fuel by spraying water on the core.

2.3.5.4 Residual Heat Removal System (LPCI Mode)

The RHR System is designed to provide heat removal functions for cooling the reactor core and containment during normal plant conditions and postulated accident conditions and to assist cooling the spent fuel pool during refueling. It is designed to permit the low pressure injection of RHR Service Water to the reactor and/or

Containment. The RHR System is able to permit the transfer of suppression pool water to the Radwaste System and the sampling of pumped water.

2.3.5.5 Reactor Core Isolation Cooling System

The RCIC system provides makeup water to the reactor vessel whenever the vessel is isolated from the main condenser and feedwater system.

2.4. Safety Related Systems Criteria

2.4.1. General

2.4.1.1 Safety systems act in response to abnormal operational transients so that fuel cladding retains its integrity as a radioactive material barrier to keep any failures within acceptable limits. Safety systems in one unit are totally separate and independent from, and in no way depend on, the safety systems in the other unit.

2.4.1.2 Safety systems and Engineered Safety Features (ESF) act to ensure that no damage to the nuclear system process barrier results from internal pressures caused by abnormal operational transients or accidents. The ECCS and N4S are the LGS ESF systems.

2.4.1.3 Safety systems and ESF act to prevent radioactive material released from the containment volumes from exceeding the guideline values of applicable regulations.

2.4.1.4 Where specific, precise actions are immediately required in response to accidents, these actions are automatic and require no decision or manipulation of controls by operations personnel.

2.4.1.5 Essential safety actions are carried out by equipment of sufficient redundancy and independence so that no single failure of active components, together with any undetectable failures that might exist in the system's design, prevents the required actions.

3.0 Safety Related System Requirements

The identification of the applicable design and functional requirements for the SR systems to be migrated to the digital platforms begins with a review of relevant documents. The types of documents reviewed included, but were not limited to, the Updated Final Safety Analysis Report (UFSAR), plant drawings, plant procedures, Design Basis Documents (DBDs), specifications, calculations, and system descriptions. Section 5 identifies the list of LGS documentation used in the development of the respective design and functional requirements for the systems. The documents are separately identified throughout the requirements listed in the accompanying appendices.

The requirements for the I&C portions of the system that describe the system functionality are listed as functional requirements in the appendices. The functional requirements incorporate elements that reflect design constraints, physical constraints,

licensing commitments, system interfaces, system boundaries, control philosophy, controlling parameters, etc.

Each of the systems is separately discussed in a section that follows. Each section includes a high level description of the primary function(s) for the respective system. Each system includes additional subsections that are explained as follows:

3.X.1 Interface Requirements: Presents the logical and physical interfaces between the particular system presented in the subsection with other systems, platforms, etc. The developed functional requirements in the appendices account for these interfaces.

3.X.2 Design Requirements: Presents the requirements that establish the licensing and design basis for the existing system that have been incorporated into various codes, criteria and regulatory requirements. For the instrumentation and control portions of the systems, the regulatory guides, 10 CFR 50 Appendix A "General Design Criteria" (GDC), and industry codes and standards that are applicable are listed in the respective design requirements section of the appendices. These design requirements will be required to be addressed when the particular application is migrated to the PPS.

3.X.3 Performance Requirements: Presents the performance requirements associated with the I&C portion of the system that are required to be fulfilled when the particular application is migrated to the PPS. These are listed in the respective design requirements section of the appendices.

3.X.4 Functional Requirements: The requirements for the I&C portions of the system that demonstrate how the system functionality meets the design requirements are listed as functional requirements in the appendices. The functional requirements incorporate elements that reflect design constraints, physical constraints, licensing commitments, system interfaces, system boundaries, control philosophy, and controlling parameters.

3.1. Reactor Protection System

The primary function of the RPS is to initiate rapid insertion of the control rods (scram) in order to:

- Prevent or limit fuel damage following abnormal operational transients;
- Prevent damage to the Reactor Coolant Pressure Boundary (RCPB) as a result of excessive internal pressure; and
- Limit the uncontrolled release of radioactive materials from the fuel assembly or RCPB.

The RPS provides this function by monitoring certain plant parameters and, if one or more parameters exceeds a specified limit, power is removed from the scram pilot valve solenoids in the Control Rod Drive (CRD) System which, when de-energized, exhaust air from the scram valves causing the control rods to scram. As the scram pilot valves are being de-energized, power is applied to the back-up scram valves which also provide an exhaust path for the air

operated scram valves and to the Shutdown Volume Isolation valves, which ensures that reactor coolant exhausted from the control rod scram is captured in the Shutdown Volume.

The functionality of the RPS resides on the PPS as an application.

3.1.1. Interface Requirements

The RPS function will have protection and control logic interfaces with the following PPS functions or external systems:

PPS Functions

N4S

External Systems

120VAC System

Class 1E 125VDC System

Neutron Monitoring System

Reactor Recirculation System

Control Rod Drive System

Reactor Instrumentation System

Main Steam, Turbine, and Extraction Steam Systems

Radiation Monitoring System

Nuclear Boiler System

Feedwater System

DCS Platform

3.1.2. Design Requirements

Design requirements for the RPS include regulatory, industry, and project defined requirements. These are identified in Appendix A.1. The design requirements are identified by a RPS-DR-XX designation.

3.1.3. Performance Requirements

3.1.3.1 RPS Response Time

The response time from the change of state of a sensor input contact or an analog signal for a monitored parameter exceeding a setpoint at the input to the RPS, to and including RPS opening of the contacts on the main trip actuators (scram contactors) is less than 50 milliseconds.

Basis: LGS Design Input (Reference 5.5.13)

3.1.4. Functional Requirements

The functional requirements define the protection and control philosophy required to fulfill the RPS function. These are identified in Appendix A.2. The functional requirements are identified by a RPS-FR-XX designation.

3.2. Nuclear Steam Supply Shutoff System

The primary function of the N4S is to:

- Isolate the Reactor Pressure Vessel (RPV);
- Isolate the Primary Containment; and
- Leak Detection.

The N4S provides this function by monitoring certain plant parameters that indicate a fluid loss or high leakage from the Reactor Coolant Pressure Boundary and initiating automatic closure of redundant isolation valves in piping that penetrates the Primary Containment or Balance of Plant (BOP) systems that provide potential paths for the release of radioactive materials as well as initiating system operational interlocks.

The functionality of the N4S resides on the PPS as an application.

3.2.1. Interface Requirements

The N4S function will have protection and control logic interfaces with the following PPS functions or external systems:

PPS Functions

RPS

RHR

RCIC

HPCI

External Systems

120VAC System

Class 1E 125VDC System

Neutron Monitoring System

Reactor Recirculation System

Reactor Water Cleanup System

Radwaste System

Instrument Air and Nitrogen Systems

Primary Containment Auxiliary Systems

Hydrogen Recombiner System

Suppression Pool Cleanup System

Standby Gas Treatment System

Reactor Enclosure Recirculation System

Reactor Enclosure Cooling Water System

Chilled Water System

OffGas System

Standby Liquid Control System

Radiation Monitoring System

Nuclear Boiler System

DCS Platform

3.2.2. Design Requirements

Design requirements for the N4S include regulatory, industry, and project defined requirements. These are identified in Appendix B.1. The design requirements are identified by a N4S-DR-XX designation.

3.2.3. Performance Requirements

3.2.3.1 N4S Response Time

The N4S signal input to actuation output propagation time is less than 50 milliseconds.

Basis: LGS Design Input (Reference 5.5.13)

3.2.4. Functional Requirements

The functional requirements define the protection and control philosophy required to fulfill the primary function of the N4S. These are identified in Appendix B.2. The functional requirements are identified by a N4S-FR-XX designation.

3.3. High Pressure Coolant Injection System

The primary function of HPCI is to:

- Provide coolant to the reactor vessel following a Small Break LOCA to meet 10 CFR 50.46 requirements until reactor vessel pressure is below the pressure at which CS operation or LPCI mode of the RHR system operation maintains core cooling.
- Provide sufficient coolant to the reactor vessel to prevent the actuation of the Automatic Depressurization System (ADS) and maintain the reactor water level above the top of the reactor core in the event of a small pipe break with a break size of one-inch diameter or less.

The HPCI provides this function by monitoring certain plant parameters that indicate a small break LOCA, and initiating the startup of a steam driven turbine pump and alignment of valves to support a water flow injection pathway to the reactor vessel.

The functionality of the HPCI resides on the PPS as an application.

3.3.1. Interface Requirements

The HPCI function will have protection and control logic interfaces with the following PPS functions or external systems:

PPS Functions

CS

N4S

RCIC

External Systems

120VAC System

Class 1E 125VDC System

Reactor Enclosure Heating, Ventilating, and Air Conditioning (HVAC) System

DCS Platform

3.3.2. Design Requirements

Design requirements for the HPCI include regulatory, industry and project defined requirements. These are identified in Appendix C.1. The design requirements are identified by a HPCI-DR-XX designation.

3.3.3. Performance Requirements

3.3.3.1 HPCI Response Time

The HPCI signal input to actuation output propagation time is less than 100 milliseconds.

Basis: LGS Design Input (Reference 5.5.13)

3.3.4. Functional Requirements

The functional requirements define the protection and control philosophy required to fulfill the primary function of the HPCI. These are identified in Appendix C.2. The functional requirements are identified by a HPCI-FR-XX designation.

3.4. Automatic Depressurization System

The primary function of ADS is to:

- Automatically actuate five ADS SRVs to depressurize the reactor vessel, which allows the RHR System LPCI mode of operation and/or CS System to provide low pressure reactor coolant makeup in the event the HPCI System and/or RCIC System fail to perform their safety functions.

The ADS provides this function by monitoring certain plant parameters and actuating the SRVs.

The functionality of the ADS shall reside on the PPS as an application.

3.4.1. Interface Requirements

The ADS function will have protection and control logic interfaces with the following PPS functions or external systems:

PPS Functions

CS

RHR

External Systems

120VAC System

Class 1E 125VDC System

Nuclear Boiler System

DCS Platform

3.4.2. Design Requirements

Design requirements for the ADS include regulatory, industry and project defined requirements. These are identified in Appendix D.1. The design requirements are identified by an ADS-DR-XX designation.

3.4.3. Performance Requirements

3.4.3.1 ADS Response Time

The ADS signal input to actuation output propagation time is less than 100 milliseconds.

Basis: LGS Design Input (Reference 5.5.13)

3.4.3.2 ADS Actuation Time Delay

A maximum allowable ADS time delay of 117 seconds is established for actuation of ADS upon receipt of all required system initiation signals at the input to the PPS. The time delay is long enough to allow the HPCI system to operate yet not so long that the RHR System LPCI mode and CS System are unable to adequately cool the core if the HPCI System fails to start.

Basis: Technical Specification Table 3.3.3-2

3.4.3.3 High Drywell Pressure Bypass Timer

The maximum allowable time before bypass of the High Drywell Pressure input occurs is 450 seconds. This time delay provides sufficient time for the operator to inhibit the automatic depressurization if Control Room information indicates that the signal is false or ADS is not needed.

Basis: Technical Specification Table 3.3.3-2

3.4.4. Functional Requirements

The functional requirements define the protection and control philosophy required to fulfill the primary function of the ADS. These are identified in Appendix D.2. The functional requirements are identified by an ADS-FR-XX designation.

3.5. Core Spray System

The primary function of CS is to:

- Provide a redundant means for removal of decay heat from the core following a postulated LOCA to meet the requirements of 10CFR50.46
- Provides a means for flooding the Reactor Vessel to remove decay heat from the core to support alternate shutdown cooling

The CS provides this function by monitoring certain plant parameters and initiating the start of pumps and aligning valves for water injection pathways. The CS also sends initiation signals to other ECCS subfunctions.

The functionality of the CS shall reside on the PPS as an application.

3.5.1. Interface Requirements

The CS function will have protection and control logic interfaces with the following PPS functions or external systems:

PPS Functions

ADS

RHR

External Systems

120VAC System

Class 1E 125VDC System

4kV System

Diesel Generator and Auxiliary Systems

DCS Platform

3.5.2. Design Requirements

Design requirements for the CS include regulatory, industry and project defined requirements. These are identified in Appendix E.1. The design requirements are identified by a CS-DR-XX designation.

3.5.3. Performance Requirements

3.5.3.1 CS Response Time

The CS signal input to actuation output propagation time is less than 100 milliseconds.

Basis: LGS Design Input (Reference 5.5.13)

3.5.4. Functional Requirements

The functional requirements define the protection and control philosophy required to fulfill the primary function of the CS. These are identified in Appendix E.2. The functional requirements are identified by a CS-FR-XX designation.

3.6. Residual Heat Removal System

The primary function of RHR is to:

- Restore and maintain the reactor vessel water level by the use of the Low Pressure Coolant Injection (LPCI) mode after a Loss-of-Coolant Accident (LOCA)

Alternate functions of the RHR are to:

- Limit the Suppression Pool water temperature by the use of the Suppression Pool Cooling (SPC) mode during normal plant operation

- Provide Drywell and Wetwell spray by the use of the Containment Spray Cooling (CSC) mode after a LOCA

- Remove reactor core decay heat and sensible heat from the primary reactor system by the use of the Shutdown Cooling (SDC) mode

The RHR/LPCI mode provides this function by monitoring certain plant parameters and automatically initiating the start of pumps and aligning valves for water injection pathways. The other modes are started and aligned manually.

The functionality of the RHR resides on the PPS as an application.

3.6.1. Interface Requirements

The RHR function will have protection and control logic interfaces with the following PPS functions or external systems:

PPS Functions

CS

ADS

RCIC

N4S

HPCI

External Systems

120VAC System

Class 1E 125VDC System

4kV System

Standby Liquid Control System

DCS Platform

3.6.2. Design Requirements

Design requirements for the RHR include regulatory, industry, and project defined requirements. These are identified in Appendix F.1. The design requirements are identified by a RHR-DR-XX designation.

3.6.3. Performance Requirements

3.6.3.1 RHR LPCI Mode Response Time

The RHR signal input to actuation output propagation time is less than 100 milliseconds.

Basis: LGS Design Input (Reference 5.5.13)

3.6.4. Functional Requirements

The functional requirements define the protection and control philosophy required to fulfill the primary function of the RHR. These are identified in Appendix F.2. The functional requirements are identified by a RHR-FR-XX designation.

3.7. Reactor Core Isolation Cooling System

The primary function of RCIC is to:

- Provide sufficient coolant to the reactor vessel during a reactor isolation event accompanied by the loss-of-coolant flow from the Feedwater System.
- Provide sufficient coolant inventory in the reactor vessel to allow for a complete plant shutdown in the event of a loss of normal feedwater until the reactor is depressurized to a level where the Shutdown Cooling Mode of the Residual Heat Removal (RHR) System can be placed into operation.
- Provide coolant inventory and temperature control when the reactor vessel is isolated and maintained in the hot standby condition.

The RCIC provides this function by monitoring certain plant parameters and initiating the startup of a steam driven turbine pump and alignment of valves to support a flow injection pathway.

The functionality of the RCIC resides on the PPS as an application.

3.7.1. Interface Requirements

The RCIC function will have protection and control logic interfaces with the following PPS functions or external systems:

PPS Functions

CS

RHR

N4S

HPCI

External Systems

120VAC System

Class 1E 125VDC System

Reactor Enclosure HVAC System

DCS Platform

3.7.2. Design Requirements

Design requirements for the RCIC include regulatory, industry, and project defined requirements. These are identified in Appendix G.1. The design requirements are identified by a RCIC-DR-XX designation.

3.7.3. Performance Requirements

3.7.3.1 RCIC Response Time

The RCIC signal input to actuation output propagation time is less than 100 milliseconds.

Basis: LGS Design Input (Reference 5.5.13)

3.7.4. Functional Requirements

The functional requirements define the protection and control philosophy required to fulfill the primary function of the RCIC. These are identified in Appendix G.2. The functional requirements are identified by a RCIC-FR-XX designation.

4.0 SR Platform Requirements

In order to support the digital transformation strategy, a common digital platform is to be leveraged. The identification of the applicable functional requirements for the SR platform was based on the familiarity with features and capabilities that are available with and unique to digital platform designs. Many of these functional requirements reflect typical architecture, HMI, communication and other related requirements prevalent in the industry.

Requirements for the PPS are identified in Appendix H.1 and are identified by a PPS-XX designation.

4.1. Functional Requirements

There are a number of functional requirements identified that that are unique to the needs of the LGS project. Platform requirements have been identified and categorized into several categories as identified below.

Safety Classification

Platform Architecture

System Inputs and Outputs (I/O)

Independence, Separation, and Segmentation

Health Monitoring

Surveillance Testing

Communication

Human-Machine Interface (HMI)

Visual Display Unit (VDU) Displays

Data Historian, Sequence of Events, Data Transmission

Cyber Security

Simulator

4.2. Environmental Characteristics

Electromagnetic Compatibility

Cabinet Requirements

Environmental Parameters

5.0 References

5.1. Code of Federal Regulations (CFR)

Appendix A to 10 CFR Part 50, General Design Criteria (GDC) for Nuclear Power Plants

5.1.1. GDC 1 - Quality Standards and Records

5.1.2. GDC 2 - Design Bases for Protection Against Natural Phenomena

5.1.3. GDC 3 - Fire Protection

5.1.4. GDC 4 - Environmental and Dynamic Effects Design Bases

5.1.5. GDC 10 - Reactor Design

5.1.6. GDC 12 - Suppression of Reactor Power Oscillations

5.1.7. GDC 13 - Instrumentation and Control

5.1.8. GDC 15 - Reactor Coolant System Design

5.1.9. GDC 19 - Control Room

5.1.10. GDC 20 - Protection System Functions

5.1.11. GDC 21 - Protection System Reliability and Testability

5.1.12. GDC 22 - Protection System Independence

5.1.13. GDC 23 - Protection System Failure Modes

5.1.14. GDC 24 - Separation of Protection and Control Systems

5.1.15. GDC 25 - Protection System Requirements for Reactivity Control Malfunctions

5.1.16. GDC 29 - Protection Against Anticipated Operational Occurrences

5.1.17. GDC 33 - Reactor Coolant Makeup

5.1.18. GDC 35 – Emergency Core Cooling

5.1.19. GDC 37 - Testing of Emergency Core Cooling System

5.2. Nuclear Regulatory Commission (NRC)

5.2.1. Regulatory Guide 1.6 (March 1971) - Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems (Safety Guide 6)

5.2.2. Regulatory Guide 1.22 (February 1972) - Periodic Testing of Protection System Actuation Functions (Safety Guide 22)

5.2.3. Regulatory Guide 1.29 (September 1978) - Seismic Design Classification

5.2.4. Regulatory Guide 1.30 (August 1972) - Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment (Safety Guide 30)

5.2.5. Regulatory Guide 1.32 (February 1977) - Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants

5.2.6. Regulatory Guide 1.47 (May 1973) - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

5.2.7. Regulatory Guide 1.53 (June 1973) - Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems

5.2.8. Regulatory Guide 1.62 (October 1973) - Manual Initiation of Protective Actions

5.2.9. Regulatory Guide 1.75 (September 1978) - Physical Independence of Electric Systems

5.2.10. Regulatory Guide 1.89 (November 1974) - Qualification of Class 1E Equipment for Nuclear Power Plants

5.2.11. Regulatory Guide 1.97 (December 1980) - Instrumentation for Light-Water- Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following and Accident

5.2.12. Regulatory Guide 1.100 (August 1977) - Seismic Qualification of Electric Equipment for Nuclear Power Plants

5.2.13. Regulatory Guide 1.105 (November 1976) - Instrument Setpoints

5.2.14. Regulatory Guide 1.118 (June 1978) - Periodic Testing of Electric Power and Protection Systems

5.2.15. Regulatory Guide 1.152 (July 2011) - Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

5.2.16. Regulatory Guide 1.153 (June 1996) - Criteria for Safety Systems

5.2.17. Regulatory Guide 1.168 (July 2013) - Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

5.2.18. Regulatory Guide 1.169 (July 2013) - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

5.2.19. Regulatory Guide 1.170 (July 2013) - Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

5.2.20. Regulatory Guide 1.171 (July 2013) - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

5.2.21. Regulatory Guide 1.172 (July 2013) - Software Requirement Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants

5.2.22. Regulatory Guide 1.173 (July 2013) - Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

5.2.23. Regulatory Guide 1.180 (December 2019) - Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems

5.2.24. Regulatory Guide 1.209 (March 2007) - Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants

5.2.25. DI&C-ISG-04, Interim Staff Guidance, Revision 1, Highly-Integrated Control Rooms – Communications Issues (HICRc)

5.2.26. NUREG/CR-6303, 1994, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems

5.2.27. NUREG/CR-6463, 1996, Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems

5.2.28. NUREG-0700, Rev 2, Human-System Interface Design Review Guidelines

5.2.29. NUREG-0711, Rev 3, Human Factors Engineering Program Review Model

5.3. Industry Standards

5.3.1. IEEE Std. 279-1971 - IEEE Standard Criteria for Protection Systems for Nuclear Power Generating Stations

5.3.2. IEEE Std. 308 (1971 and 1974) - Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations

5.3.3. IEEEStd. 323 (1971 and 2003) - General Guide for Qualifying Class 1 Electric Equipment for Nuclear Power Generating Stations

5.3.4. International Electrotechnical Commission (IEC)/IEEE 60780/323 2016, Nuclear facilities – Electrical equipment important to safety – Qualification

5.3.5. IEEE Std. 336 (1971 and 2010) - IEEE Standard Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment during the Construction of Nuclear Power Generating Stations

5.3.6. IEEE Std. 338 (1971, 1975, 1977, 1987, and 2012) - Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems

5.3.7. IEEE Std. 344 (1971 or 1975) - Guide for Seismic Qualification of Class 1 Electric Equipment for Nuclear Power Generating Stations

5.3.8. IEEE Std. 379 (1972 or 1977, 2003, and 2014) - Guide for the Application of the Single Failure Criterion to Nuclear Power Generating Station Protection Systems

5.3.9. IEEE Std. 384 (1977 and 2018) - Criteria for Independence of Class 1E Equipment and Circuits

5.3.10. IEEE Std. 603 (1991 and 2018) - Standard Criteria for Safety Systems for Nuclear Power Generating Stations

5.3.11. IEEE Std. 7-4.3.2 (2003 and 2016) - Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

5.3.12. ANS 3.5-2009, Nuclear Power Plant Simulators for Use in Operator Training and Examination

5.4. Limerick Drawings

5.4.1. M-1-C71-1020-E-020 Sheets 1 through 14, “Elementary Diagram Reactor Protection System”

5.4.2. M-1-B21-1090-E-027 Sheets 1 through 15, “Elementary Diagram Nuclear Steam Supply Shutoff System”

5.4.3. B21-1090-E-034, “Elementary Diagram HV-051-2F008”

5.4.4. B21-1090-E-035, “Elementary Diagram HV-051-2F009”

5.4.5. B21-1090-E-036, “Elementary Diagram HV-051-2F015A”

5.4.6. B21-1090-E-037, “Elementary Diagram HV-051-2F015B”

5.4.7. B21-1090-E-038, “Elementary Diagram HV-041-2F016”

5.4.8. M-1-E41-1040-E-001 Sheets 1 and 2, “Elementary Diagram HPCI System”

5.4.9. M-1-E41-1040-E-002, “Elementary Diagram HPCI System”

5.4.10. M-1-E41-1040-E-003, “Elementary Diagram HPCI System”

5.4.11. M-1-E41-1040-E-004, “Elementary Diagram HPCI System”

5.4.12. M-1-E41-1040-E-005, “Elementary Diagram HPCI System”

5.4.13. M-1-E41-1040-E-006, “Elementary Diagram HPCI System”

5.4.14. M-1-E41-1040-E-007, “Elementary Diagram HPCI System”

5.4.15. M-1-E41-1040-E-008, “Elementary Diagram HPCI System”

5.4.16. M-1-E41-1040-E-009, “Elementary Diagram HPCI System”

5.4.17. M-1-E41-1040-E-012 Sheets 1 and 2, “Elementary Diagram HPCI System”

5.4.18. M-1-E41-1040-E-013 Sheets 1 through 6, “Elementary Diagram HPCI System”

5.4.19. M-1-E41-1040-E-014 Sheets 1 and 2, “Elementary Diagram HPCI System”

5.4.20. M-1-E41-1040-E-015, “Elementary Diagram HPCI System”

5.4.21. M-1-E41-1040-E-016, “Elementary Diagram HPCI System”

5.4.22. E41-1040-E-031, “Schematic HV-055-1F011 HPCI, RCIC PP. Test Return to CST Condensate”

5.4.23. E41-1040-E-033, “Schematic HV-055-1F072 HPCI Turbine Exhaust PCIV Exhaust”

5.4.24. M-1- B21-1060-E-001, “Elementary Diagram Auto Depressurization System”

5.4.25. M-1- B21-1060-E-002, “Elementary Diagram Auto Depressurization System”

5.4.26. M-1- B21-1060-E-003, “Elementary Diagram Auto Depressurization System”

5.4.27. M-1- B21-1060-E-004, “Elementary Diagram Auto Depressurization System”

5.4.28. M-1- B21-1060-E-005, “Elementary Diagram Auto Depressurization System”

5.4.29. M-1- B21-1060-E-006, “Elementary Diagram Auto Depressurization System”

5.4.30. M-1- B21-1060-E-007, “Elementary Diagram Auto Depressurization System”

5.4.31. M-1- B21-1060-E-008, “Elementary Diagram Auto Depressurization System”

5.4.32. M-1- B21-1060-E-009, “Elementary Diagram Auto Depressurization System”

5.4.33. M-1- B21-1060-E-010, “Elementary Diagram Auto Depressurization System”

5.4.34. M-1- B21-1060-E-011, “Elementary Diagram Auto Depressurization System”

5.4.35. M-1- E21-1040-E-001, “Elementary Diagram Core Spray System”

5.4.36. M-1- E21-1040-E-002, “Elementary Diagram Core Spray System”

5.4.37. M-1- E21-1040-E-003, “Elementary Diagram Core Spray System”

5.4.38. M-1- E21-1040-E-004 Sheets 1 and 2, “Elementary Diagram Core Spray System”

5.4.39. M-1- E21-1040-E-005, “Elementary Diagram Core Spray System”

5.4.40. M-1- E21-1040-E-006, “Elementary Diagram Core Spray System”

5.4.41. M-1- E21-1040-E-007, “Elementary Diagram Core Spray System”

5.4.42. M-1- E21-1040-E-008, “Elementary Diagram Core Spray System”

5.4.43. M-1- E21-1040-E-009, “Elementary Diagram Core Spray System”

5.4.44. M-1- E21-1040-E-010, “Elementary Diagram Core Spray System”

5.4.45. M-1- E21-1040-E-011, “Elementary Diagram Core Spray System”

5.4.46. M-1- E21-1040-E-012, “Elementary Diagram Core Spray System”

5.4.47. M-1- E21-1040-E-013, “Elementary Diagram Core Spray System”

5.4.48. M-1- E21-1040-E-014, “Elementary Diagram Core Spray System”

5.4.49. M-1- E21-1040-E-015, “Elementary Diagram Core Spray System”

5.4.50. M-1- E21-1040-E-016, “Elementary Diagram Core Spray System”

5.4.51. M-1- E21-1040-E-017, “Elementary Diagram Core Spray System”

5.4.52. M-1- E11-1040-E-001, “Elementary Diagram Residual Heat Removal System”

5.4.53. M-1- E11-1040-E-002, “Elementary Diagram Residual Heat Removal System”

5.4.54. M-1- E11-1040-E-003, “Elementary Diagram Residual Heat Removal System”

5.4.55. M-1- E11-1040-E-004, “Elementary Diagram Residual Heat Removal System”

5.4.56. M-1- E11-1040-E-005, “Elementary Diagram Residual Heat Removal System”

5.4.57. M-1- E11-1040-E-006, “Elementary Diagram Residual Heat Removal System”

5.4.58. M-1- E11-1040-E-007, “Elementary Diagram Residual Heat Removal System”

5.4.59. M-1- E11-1040-E-008, “Elementary Diagram Residual Heat Removal System”

5.4.60. M-1- E11-1040-E-009, “Elementary Diagram Residual Heat Removal System”

5.4.61. M-1- E11-1040-E-010, “Elementary Diagram Residual Heat Removal System”

5.4.62. M-1- E11-1040-E-011, “Elementary Diagram Residual Heat Removal System”

5.4.63. M-1- E11-1040-E-012, “Elementary Diagram Residual Heat Removal System”

5.4.64. M-1- E11-1040-E-013, “Elementary Diagram Residual Heat Removal System”

5.4.65. M-1- E11-1040-E-014, “Elementary Diagram Residual Heat Removal System”

5.4.66. M-1- E11-1040-E-015 Sheets 1 and 2, “Elementary Diagram Residual Heat Removal System”

5.4.67. M-1- E11-1040-E-016, “Elementary Diagram Residual Heat Removal System”

5.4.68. M-1- E11-1040-E-017, “Elementary Diagram Residual Heat Removal System”

5.4.69. M-1- E11-1040-E-018 Sheets 1 and 2, “Elementary Diagram Residual Heat Removal System”

5.4.70. M-1- E11-1040-E-019, “Elementary Diagram Residual Heat Removal System”

5.4.71. M-1- E11-1040-E-020, “Elementary Diagram Residual Heat Removal System”

5.4.72. M-1- E11-1040-E-021, “Elementary Diagram Residual Heat Removal System”

5.4.73. M-1- E11-1040-E-022, “Elementary Diagram Residual Heat Removal System”

5.4.74. M-1- E11-1040-E-023, “Elementary Diagram Residual Heat Removal System”

5.4.75. M-1- E11-1040-E-024, “Elementary Diagram Residual Heat Removal System”

5.4.76. M-1- E11-1040-E-025, “Elementary Diagram Residual Heat Removal System”

5.4.77. M-1- E11-1040-E-026, “Elementary Diagram Residual Heat Removal System”

5.4.78. M-1- E11-1040-E-027, “Elementary Diagram Residual Heat Removal System”

5.4.79. M-1- E11-1040-E-028, “Elementary Diagram Residual Heat Removal System”

5.4.80. M-1- E11-1040-E-029, “Elementary Diagram Residual Heat Removal System”

5.4.81. E11-1040-E-059, “Schematic – HV-051-1F003A, 1A RHR RTX Shell Side Outlet Vlv Outlet”

5.4.82. E11-1040-E-060, “Schematic – HV-051-1F003B, 1B RHR RTX Shell Side Outlet Vlv Outlet”

5.4.83. E11-1040-E-061, “Schematic – HV-051-1F007A, 1A RHR PP Min Flow Vlv Min Flow A”

5.4.84. E11-1040-E-062, “Schematic – HV-051-1F010A, 1C RHR PP Full Flow Test Return Vlv”

5.4.85. E11-1040-E-063, “Schematic – HV-051-1F004A, 1A RHR PP Suction PCIV Suction A”

5.4.86. E11-1040-E-064, “Schematic – HV-051-1F004B, 1B RHR PP Suction PCIV Suction B”

5.4.87. E11-1040-E-065, “Schematic – HV-051-1F006A, 1A RHR Shutdown Cooling Suction MOV”

5.4.88. E11-1040-E-066, “Schematic – HV-051-1F006B, 1B RHR PP CLG Suct Vlv Suction B”

5.4.89. E11-1040-E-067, “Schematic – HV-051-1F017A, 1A RHR LPCI INJ PCIV Outboard A”

5.4.90. E11-1040-E-068, “HV-051-1F017B, 1B RHR LPCI INJ PCIV Outboard B”

5.4.91. E11-1040-E-069, “Schematic – HV-051-1F024A, 1A RHR PP Full Flow Test Return Vlv”

5.4.92. E11-1040-E-070, “Schematic – HV-051-1F024B, 1B RHR PP Full Flow Test Return Vlv”

5.4.93. E11-1040-E-071, “Schematic – HV-051-1F027A, 1A RHR Supp Pool Spray Line PCIV”

5.4.94. E11-1040-E-072, “Schematic – HV-051-1F027B, 1B RHR Supp Pool Spray Line PCIV”

5.4.95. E11-1040-E-073, “Schematic – HV-051-1F047A, 1A RHR HTX Shell Side Inlet Vlv Inlet”

5.4.96. E11-1040-E-074, “Schematic – HV-051-1F048A, 1A RHR HTX Shell Side Bypass Vlv Heat Exch Bypass”

5.4.97. E11-1040-E-093, “Schematic – HV-051-1F047B, 1B RHR HTX Shell Side Inlet Vlv Inlet”

5.4.98. E11-1040-E-094, “Schematic – HV-051-1F073, RHR Service Water Crosstie Cross Tie”

5.4.99. E11-1040-E-095, “Schematic – HV-C-051-1F048B, 1B RHR HTX, Shell Side Bypass Vlv Heat Exch”

5.4.100. M-1-E51-1040-E-001, “Elementary Diagram – Reactor Core Isolation”

5.4.101. M-1-E51-1040-E-002, “Elementary Diagram – Reactor Core Isolation”

5.4.102. M-1-E51-1040-E-003, “Elementary Diagram – Reactor Core Isolation”

5.4.103. M-1-E51-1040-E-004, “Elementary Diagram – Reactor Core Isolation”

5.4.104. M-1-E51-1040-E-005, “Elementary Diagram – Reactor Core Isolation”

5.4.105. M-1-E51-1040-E-006, “Elementary Diagram – Reactor Core Isolation”

5.4.106. M-1-E51-1040-E-007 Sheets 1 and 2, “Elementary Diagram – Reactor Core Isolation”

5.4.107. M-1-E51-1040-E-008, “Elementary Diagram – Reactor Core Isolation”

5.4.108. M-1-E51-1040-E-009, “Elementary Diagram – Reactor Core Isolation”

5.4.109. M-1-E51-1040-E-010, “Elementary Diagram – Reactor Core Isolation”

5.4.110. M-1-E51-1040-E-011, “Elementary Diagram – Reactor Core Isolation”

5.4.111. M-1-E51-1040-E-012, “Elementary Diagram – Reactor Core Isolation”

5.4.112. M-1-E51-1040-E-013, “Elementary Diagram – Reactor Core Isolation”

5.4.113. M-1-E51-1040-E-014, “Elementary Diagram – Reactor Core Isolation”

5.4.114. M-1-E51-1040-E-015, “Elementary Diagram – Reactor Core Isolation”

5.4.115. M-1-E51-1040-E-016, “Elementary Diagram – Reactor Core Isolation”

5.4.116. M-1-E51-1040-E-017, “Elementary Diagram – Reactor Core Isolation”

5.4.117. M-1-E51-1040-E-040, “Schematic HV-049-1F002 RCIC Bar Cond Vac Pump Disch PCIV (Disch)”

5.4.118. M-1-E51-1040-E-041, “Schematic HV-049-1F010 RCIC PP Suction From CST Vlv (Cond Tk Suction)”

5.4.119. M-1-E51-1040-E-042, “Schematic HV-049-1F012 RCIC PP Disch Outbd Isol Vlv (Discharge)”

5.4.120. M-1-E51-1040-E-043, “Schematic HV-049-1F013 RCIC PP Disch Inbrd PCIV (Feed)”

5.4.121. M-1-E51-1040-E-044, “Schematic HV-049-1F019 RCIC Pump Min Flow PCIV (Min Flow)”

5.4.122. M-1-E51-1040-E-045, “Schematic HV-049-1F022 RCIC Full Flow Test Vlv (Test Isol)”

5.4.123. M-1-E51-1040-E-046, “Schematic HV-049-1F029 RCIC PP Suction From Suppression Pool (Supp Pool Suction)”

5.4.124. M-1-E51-1040-E-047, “Schematic HV-049-1F031 RCIC Pump Suction From Supp Pool PCIV (Supp Pool)”

5.4.125. M-1-E51-1040-E-048, “Schematic HV-049-1F060 RCIC Turbine Exh PCIV (Exhaust)”

5.4.126. M-1-E51-1040-E-049, “Schematic HV-050-1F045 RCIC Stm Supply Vlv (Inlet)”

5.4.127. M-1-E51-1040-E-050, “Schematic HV-050-1F046 RCIC Lube Oillg Wtr Supply Vlv (Cooling Water)

5.4.128. M-1-E51-1040-E-051, “Schematic HV-050-112 Reactor Core Isolation Cooling Turbine Trip Throttle Valve”

5.4.129. M-1-E51-1040-E-052, “Schematic HV-049-1F007 Main Steam Supply Inbrd PCIV Inboard”

5.4.130. M-1-E51-1040-E-053, “Schematic HV-049-1F008 RCIC Steam Line Outboard PCIV Outboard”

5.4.131. M-1-E51-1040-E-054, “Schematic HV-049-1F080 RCIC Turb Exhaust Line Vac Bkr PCIV Outboard”

5.4.132. M-1-E51-1040-E-055, “Schematic HV-049-1F084 RCIC Turb Exhaust Vacuum Bkr PCIV Inboard”

5.4.133. M-1-B21-1050-E-001, “Elementary Diagram Steam Leak Detection Schematic”

5.4.134. M-1-B21-1050-E-002, “Elementary Diagram Steam Leak Detection Schematic”

5.4.135. M-1-B21-1050-E-003, “Elementary Diagram Steam Leak Detection Schematic”

5.4.136. M-1-B21-1050-E-004, “Elementary Diagram Steam Leak Detection Schematic”

5.4.137. M-1-B21-1050-E-005, “Elementary Diagram Steam Leak Detection Schematic”

5.4.138. M-1-B21-1050-E-006, “Elementary Diagram Steam Leak Detection Schematic”

5.4.139. M-1-B21-1050-E-007, “Elementary Diagram Steam Leak Detection Schematic”

5.4.140. M-1-B21-1050-E-008, “Elementary Diagram Steam Leak Detection Schematic”

5.4.141. M-1-B21-1050-E-009, “Elementary Diagram Steam Leak Detection Schematic”

5.5. Limerick Specific Documents

5.5.1. LGS Unit 1 Technical Specification (Thru Amendment 235)

5.5.2. LGS Updated Final Safety Analysis Report (UFSAR), Rev 16

5.5.3. M-171, Rev 17, Specification for Environmental Service Conditions Limerick Generating Stations Units 1&2

5.5.4. Procedure GP-8, Rev 20, “Primary and Secondary Containment Isolation Reset / Bypass and Restoration”

5.5.5. Procedure GP-8.1, Rev 16, “Auomatic Actuations by Isolation Signals”

5.5.6. Design Basis Document L-S-06, Rev 10, “Reactor Protection System”

5.5.7. Design Basis Document L-S-26, Rev 4. “Primary Containment Isolation System”

5.5.8. Design Basis Document L-S-03, Rev 20, “High Pressue Coolant Injection System”

5.5.9. Design Basis Document L-S-31, Rev 4, “Automatic Depressurixation System”

5.5.10. Design Basis Document L-S-44, Rev 11, “Core Spray System”

5.5.11. Design Basis Document L-S-09, Rev 21, “Residual Heat Removal System”

5.5.12. Design Basis Document L-S-39, Rev 13, “Reactor Core isolation Cooling System”

5.5.13. LGS E-mail from George Bonanni dated 3/26/20

A

A.1 RPS Design Requirements

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-1	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. 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. 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.	GDC 1 - Quality standards and records.
RPS-DR-2	Structures, systems, and components important to safety shall be designed to withstand the effect of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions.	GDC 2 - Design Bases for Protection Against Natural Phenomena
RPS-DR-3	Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions.	GDC 3 - Fire protection
RPS-DR-4	Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents (LOCAs).	GDC 4 - Environmental and dynamic effects design bases
RPS-DR-5	The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.	GDC 10 - Reactor design

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-6	The reactor core and associated coolant, control, and protection systems shall be designed to assure that power oscillations which can result in conditions exceeding specified acceptable fuel design limits are not possible or can be reliably and readily detected and suppressed.	GDC 12 - Suppression of reactor power oscillations
RPS-DR-7	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.	GDC 13 - Instrumentation and control
RPS-DR-8	The reactor coolant system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences.	GDC 15 - Reactor coolant system design
RPS-DR-9	A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. 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 I&C 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.	GDC 19 - Control Room

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-10	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.	GDC 20 - Protection system functions
RPS-DR-11	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.	GDC 21 - Protection system reliability and testability
RPS-DR-12	The protection system shall be designed to ensure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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.	GDC 22- Protection system independence
RPS-DR-13	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.	GDC 23 - Protection system failure modes

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-14	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.	GDC 24 - Separation of protection and control systems
RPS-DR-15	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.	GDC 25 - Protection system requirements for reactivity control malfunctions
RPS-DR-16	The protection and reactivity control systems shall be designed to ensure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.	GDC 29 - Protection against anticipated operational occurrences
RPS-DR-17	The protection system shall be designed to permit periodic testing of its initiation functions inclusive of the actuation devices and actuated equipment when the reactor is in operation.	Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions (Safety Guide 22)
RPS-DR-18	Those structures, systems, and components (SSC) that should be designed to remain functional if the Safe Shutdown Earthquake (SSE) occurs shall be designated as Seismic Category I. (This includes Systems or portions of systems that are required for reactor shutdown; all electric and mechanical devices and circuitry between the process and the input terminals of the actuator systems involved in generating signals that initiate protective action; systems or portions of systems that are required for (1) monitoring of systems important to safety and (2) actuation of systems important to safety.)	Regulatory Guide 1.29 - Seismic Design Classification

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-19	The RPS shall comply with the requirements of Appendix B to 10 CFR Part 50 for the installation, inspection, and testing of nuclear power plant instrumentation and electric equipment.	Regulatory Guide 1.30 - Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment (Safety Guide 30)
RPS-DR-20	The RPS shall meet the requirements for design, operation, and testing of safety-related power systems within nuclear power plants as defined within IEEE Std. 308.	Regulatory Guide 1.32 - Criteria for Power Systems for Nuclear Power Plants
RPS-DR-21	The RPS shall meet the requirements for indicating the bypass or inoperable status of portions of the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the system it actuates to perform their safety-related functions:	Regulatory Guide 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
RPS-DR-22	The RPS shall comply with the IEEE Std. 279 requirement that any single failure within the protection system shall not prevent proper protective action at the system level when required, by utilizing the guidance in IEEE Std. 379-1972 for applying the single-failure criterion to the design and analysis of nuclear power plant protection systems.	Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Safety Systems
RPS-DR-23	The RPS shall provide a means for manual initiation of protective actions.	Regulatory Guide 1.62 - Manual Initiation of Protective Actions
RPS-DR-24	The RPS shall meet the requirements for physical independence of the circuits and electric equipment comprising or associated with the Class 1E power system, the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety related functions.	Regulatory Guide 1.75 - Physical Independence of Electric Systems
RPS-DR-25	The RPS shall comply with design verification requirements to verify adequacy of design under the most adverse design conditions.	Regulatory Guide 1.89 - Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-26	The RPS shall comply with the requirement to: (1) provide information required to permit the operator to take preplanned manual actions to accomplish safe plant shutdown; (2) determine whether the reactor trip, engineered safety feature systems, and manually initiated safety systems and other systems important to safety are performing their intended functions (i.e., reactivity control, core cooling, maintaining reactor coolant system integrity, and maintaining containment integrity); (3) provide information to the operators that will enable them to determine the potential for causing a gross breach of the" barriers to radioactivity release (i.e., fuel cladding, reactor coolant pressure boundary, and containment) and to determine if a gross breach of a barrier has occurred.	Regulatory Guide 1.97 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants
RPS-DR-27	The RPS shall comply with design verification requirements to verify the seismic adequacy of electric equipment.	Regulatory Guide 1.100 - Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants
RPS-DR-28	The RPS design shall implement setpoints that ensure sufficient margin between Technical Specification limits and the trip setpoint to account for instrument inaccuracy, calibration uncertainties, and instrument drift. Consideration of instrument span and range as well as environmental influences must be included.	Regulatory Guide 1.105 - Instrument Setpoint
RPS-DR-29	The RPS shall comply with the requirements for periodic testing of electric power and protection systems.	Regulatory Guide 1.118 - Periodic Testing of Electric Power and Protection Systems
RPS-DR-30	The RPS shall, with precision and reliability, initiate a reactor scram to prevent or limit fuel damage following abnormal operational transients; prevent damage to the RCPB as a result of excessive internal pressure; and limit the uncontrolled release of radioactive materials from the fuel assembly or RCPB.	IEEE Std. 603, Section 5.0 Safety System Criteria and 6.1 Automatic Control

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-31	The RPS shall initiate a trip when the monitored plant parameter exceeds the following trip setpoint: Scram Discharge Volume (SDV) water level > 260' 9-5/8" elevation (Unit 1: 25.45 gal, Unit 2: 25.58 gal) Reactor Vessel Water Level < 12.5 inches above instrument zero Drywell Pressure > 1.68 psig Reactor Vessel Pressure > 1096 psig	IEEE Std. 603, Section 6.1 Automatic Control
RPS-DR-32	The RPS time response from the change of state of a sensor input contact or an analog signal for exceeding a setpoint, to and including opening of the contacts on the main trip actuators (scram contactors) shall be less than 50 milliseconds: Neutron Flux (APRM) Reactor Vessel Pressure Reactor Vessel Water Level Main Steam Line Isolation Valve Position Turbine Stop Valve Position Main Turbine Control Valve Fast Closure	IEEE Std. 603, Section 4.10
RPS-DR-33	The RPS shall be capable of initiating a reactor scram under all modes of reactor operation.	IEEE Std. 603, Section 4.1
RPS-DR-34	The RPS shall be capable of initiating a reactor scram via discrete signals (contact input) from a manually initiated switch.	IEEE Std. 603, Section 6.2 Manual Control
RPS-DR-35	The RPS shall ensure that the protective action, once started, continues to completion.	IEEE Std. 603, Section 5.2 Completion of Protective Action
RPS-DR-36	Any single failure within the RPS shall not prevent proper protective action at the system level when required.	IEEE Std. 603, Section 5.1 Single Failure Criterion and IEEE Std. 7-4.3.2 Section 5.1 Single Failure Criterion

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-37	Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.	IEEE Std. 603 section 5.3 Quality and IEEE Std. 7-4.3.2 section 5.3 Quality
RPS-DR-38	Type test data or reasonable engineering extrapolation based on test data shall be available to verify that protection system equipment shall meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements.	IEEE Std. 603 section 5.4 Equipment Qualification and IEEE Std. 7-4.3.2 section 5.4 Equipment Qualification
RPS-DR-39	All protection system channels shall be designed to maintain necessary functional capability under extremes of conditions (as applicable) relating to environment, energy supply, malfunctions, and accidents.	IEEE Std. 603 section 5.5 System Integrity and IEEE Std. 7-4.3.2 and section 5.5 Independence
RPS-DR-40	Channels that provide signals for the same protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 System Integrity
RPS-DR-41	Any equipment that is used for both protective and control functions shall be classified as part of the protection system and shall meet all the applicable requirements.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence
RPS-DR-42	The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system and shall meet all the applicable requirements. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-43	Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
RPS-DR-44	Provisions shall be included so that the protective action can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
RPS-DR-45	Where a credible single event can cause a control system action that results in a condition requiring protective action and can concurrently prevent the protective action from those protection system channels designated to provide principal protection against the condition, then alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design bases.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
RPS-DR-46	To the extent feasible and practical, protection system inputs shall be derived from signals that are direct measures of the desired variables.	IEEE Std. 603 section 6.4 Derivation of System Inputs
RPS-DR-47	Means shall be provided for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
RPS-DR-48	Capability shall be provided for testing and calibrating channels and the devices used to derive the final system output signal from the various channel signals.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
RPS-DR-49	For those parts of the system where the required interval between testing will be less than the normal time interval between generating station shutdowns, there shall be capability for testing during power operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-50	The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective action at the systems level.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
RPS-DR-51	During such operation, the active parts of the system shall of themselves continue to meet the single failure criterion.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
RPS-DR-52	Where operating requirements necessitate automatic or manual bypass of a protective function, the design shall be such that the bypass will be removed automatically whenever permissive conditions are not met.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
RPS-DR-53	Devices used to achieve automatic removal of the bypass of a protective function are part of the protection system and shall be designed in accordance with these criteria.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
RPS-DR-54	If the protective action of some part of the system has been bypassed or deliberately rendered inoperative for any purpose, this fact shall be continuously indicated in the control room.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RPS-DR-55	The design shall permit the administrative control of the means for manually bypassing channels or protective functions.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
RPS-DR-56	Where it is necessary to change to a more restrictive set point to provide adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of assuring that the more restrictive set point is used.	IEEE Std. 603 section 6.8 Setpoints
RPS-DR-57	The devices used to prevent improper use of less restrictive set points shall be considered a part of the protection system and shall be designed in accordance with the other provisions of these criteria regarding performance and reliability.	IEEE Std. 603 section 6.8 Setpoints
RPS-DR-58	The protection system shall be so designed that, once initiated, a protective action at the system level shall go to completion.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-59	Return to operation shall require subsequent deliberate operator action.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action
RPS-DR-60	The protection system shall include means for manual initiation of each protective action at the system level (for example, reactor trip, containment isolation, safety injection, core spray, etc).	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
RPS-DR-61	No single failure within the manual, automatic, or common portions of the protection system shall prevent initiation of protective action by manual or automatic means.	IEEE Std. 603 section 7.2 Manual Control
RPS-DR-62	Manual initiation should depend upon the operation of a minimum of equipment.	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
RPS-DR-63	The design shall permit the administrative control of access to all set point adjustments, module calibration adjustments, and test points.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
RPS-DR-64	Protective actions shall be indicated and identified down to the channel level.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RPS-DR-65	The protection system shall be designed to provide the operator with accurate, complete, and timely information pertinent to its own status and to generating station safety.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RPS-DR-66	The design shall minimize the development of conditions which would cause meters, annunciators, recorders, alarms, etc, to give anomalous indications confusing to the operator.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RPS-DR-67	The system shall be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.	IEEE Std. 603 section 5.10 Repair

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-68	In order to provide assurance that the requirements given in this document can be applied during the design, construction, maintenance, and operation of the plant, the protection system equipment (for example, interconnecting wiring, components, modules, etc), shall be identified distinctively as being in the protection system.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
RPS-DR-69	This identification shall distinguish between redundant portions of the protection system. (In the installed equipment, components, or modules mounted in assemblies that are clearly identified as being in the protection system do not themselves require identification.) All software, firmware, and programmable logic shall be identified in accordance with IEEE Std. 7-4.3.2 Clause 5.11.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
RPS-DR-70	RPS shall conform to the design criteria and features for Class 1E electric systems to ensure that functional requirements under the conditions produced by design basis events are met.	IEEE Std. 308 - Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations
RPS-DR-71	RPS shall conform to the methods for demonstrating the qualification of Class 1E equipment including components or equipment of any interface whose failure could adversely affect the performance of Class 1E systems and electronic equipment.	IEEE Std. 323 - Qualifying Class 1E Equipment for Nuclear Power Generating Stations
RPS-DR-72	RPS shall conform to the design and operational criteria for the performance of periodic testing of nuclear power generating station safety systems.	IEEE Std. 338 - Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems
RPS-DR-73	RPS shall meet its Class 1E performance requirements during and following one SSE (safe shutdown earthquake) preceeded by a number of OBEs (operating basis earthquakes).	IEEE Std. 344 - Guide for Seismic Qualification of Class 1 Electric Equipment for Nuclear Power Generating Stations
RPS-DR-74	RPS shall meet the single failure criterion as described and classified in IEEE Std. 379.	IEEE Std. 379 - Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

RPS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RPS-DR-75	RPS shall meet the criteria and requirements for establishing and maintaining the independence of Class 1E equipment and circuits and auxiliary supporting features by physical separation and electrical isolation.	IEEE Std. 384 - Criteria for Independence of Class 1E Equipment and Circuits

A.2 RPS Functional Requirements

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-1	The PPS/RPS shall be capable of initiating a scram signal either automatically when any of the monitored parameters exceeds a pre-established value, or by manual initiation.	GDC 10, GDC 12, GDC 20, GDC 25, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-2	PPS/RPS shall be comprised of two (2) independent and separate divisions (Division 1 and Division 2)	GDC 21, Reg Guide 1.22, Reg Guide 1.53, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379	
RPS-FR-3	The PPS/RPS shall have four (4) independent channels (Channel A, Channel B, Channel C and Channel D) that each provide votes / signals to 2oo4 voters in each of the divisions.	GDC 21, Reg Guide 1.22, Reg Guide 1.53, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379	The four channels are common to both divisions.
RPS-FR-4	Each channel shall receive an input from each of the following monitored parameters that are provided as common inputs to the PPS platform and are shared by each of the PPS functions: • Reactor Vessel Pressure (RVP) • Reactor Vessel Water Level 3 (RWL3) • Drywell High Pressure (DHP)	GDC 10, GDC 12, GDC 20, GDC 25, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-5	Each channel shall receive contact input from each of the following monitored parameters: • Scram Discharge Volume Level HI (CI6) • Main Steam Line Isolation Valve (MSIV) Position (CI7) • Main Steam Line Isolation Valve (MSIV) Position (CI8) • Turbine Stop Valve (TSV) Position (CI9) • Turbine Stop Valve (TSV) Position (CI10)	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	For CI7, the contact input is "seen" by the channel as a single input but is comprised of two MSIV inboard (IB) and outboard (OB) position contacts connected in series and assigned to each channel as follows: Channel A: MSIV A (IB), MSIV A (OB) Channel B: MSIV C (IB), MSIV C (OB) Channel B: MSIV A (IB), MSIV A (OB) Channel D: MSIV B (IB), MSIV B (OB) For CI8, the contact input is "seen" by the channel as a single input but is comprised of two MSIV inboard (IB) and outboard (OB) position contacts connected in series and assigned to each channel as follows: Channel A: MSIV B (IB), MSIV B (OB) Channel B: MSIV D (IB), MSIV D (OB) Channel C: MSIV C (IB), MSIV C (OB) Channel D: MSIV D (IB), MSIV D (OB) For CI9, each channel shall receive a contact input from the assigned TSV as follows: Channel A: TSV 3 Channel B: TSV 1 Channel C: TSV 1 Channel D: TSV 2 For CI10, each channel shall receive a contact input from the assigned TSV as follows: Channel A: TSV 4 Channel B: TSV 2 Channel C: TSV 3 Channel D: TSV 4

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-6	Each channel shall receive contact input from each of the following monitored parameters (cont'd): • Turbine Control Valve Fast Closure (CI11) • Source Range Neutron Flux (CI12) • IRM/OPRM/APRM Neutron Flux (CI13) • IRM/OPRM/APRM Neutron Flux (CI14)	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	For CI11, The TCV contacts area assigned to each channel as follows: Channel A: TCV 1 Channel B: TCV 3 Channel C: TCV 2 Channel D: TCV 4 For CI13, the contact input is "seen" by the channel as a single input but is comprised of several field contacts connected together for the following parameters and assigned to each channel as follows: Channel A: IRM A / APRM 1 / RMS Channel B: IRM C / APRM 3 / RMS Channel C: IRM B / APRM 2 / RMS Channel D: IRM D / APRM 4 / RMS For CI14, the contact input is "seen" by the channel as a single input but is comprised of several field contacts connected together for the following parameters and assigned to each channel as follows: Channel A: IRM E / APRM 1 / RMS Channel B: IRM G / APRM 3 / RMS Channel C: IRM F / APRM 2 / RMS Channel D: IRM H / APRM 4 / RMS
RPS-FR-7	Each channel shall also receive the following 4-20 mA inputs: • Scram Discharge Volume Level (SDVL) • Turbine 1st Stage Pressure (TSP)	Original Design	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-8	Each channel shall receive the following contact inputs: • Reactor Mode Switch SCRAM (S/D mode (contact closed)) (CI1) • Reactor Mode Switch SCRAM Reset Interlock (S/D mode (contact closed)) (CI2) • Reactor Mode Switch MSIV Bypass (CI3) • Reactor Mode Switch SDV HI Water Level Bypass (CI4) • Reactor Mode Switch SCRAM (S/D mode (contact open)) (CI5)	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-9	Each input to a channel (mA or contact input) shall be voted on by the channel based on the condition (condition met or not met).	Project design approach	The term "shall be voted on" indicates that the channel performs a bi-stable comparison against a pre-determined configurable setpoint to determine whether the input is at or above/below the setpont value.
RPS-FR-10	Each channel shall provide the status of the vote (e.g. vote to scram or not scram; vote to annunciate, etc.) to each of the divisions.	Project design approach	The terms “scram”, “not scram”, “annunciate” describe different types of votes that may be provided by a channel. A particular vendor solution may combine one or more of the vote types into a single channel vote based on the capabilities of the platform.
RPS-FR-11	Each division shall determine whether the votes for each type of input satisfy the voting criteria (e.g. 2oo4).	Project design approach	
RPS-FR-12	Each division shall generate an output for a scram when the required voting has been satisfied.	Project design approach	As an example, the RWL3 input to Channels A, B, C and D shall be sent to a 2oo4 voter in each of the divisions (Division 1 and Division 2). When at least two of the four RWL3 inputs to the 2oo4 voter satisfy the vote to SCRAM, the associated division generates an output.

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-13	Each input to a channel shall have an associated 2oo4 voter within each division to ensure that trip inputs are voted separately.	GDC 21, Reg Guide 1.22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379	
RPS-FR-14	A scram output signal from both divisions, at the same time, shall be necessary to cause the PPS/RPS to initiate a reactor scram (shutdown).	GDC 21, Reg Guide 1.22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379	Each division shall de-energize its associated SCRAM pilot solenoid valves. A single division shall not be capable of de-energizing both sets of SCRAM pilot solenoid valves.
RPS-FR-15	The PPS/RPS shall be a normally energized system (fail-safe type design). (i.e. initiate a scram on loss of electrical power)	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-16	The PPS/RPS shall be powered by 120VAC +/- 10% (108 to 132 VAC) power.	Design driven	
RPS-FR-17	The two divisions shall be isolated from each other.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-18	Each division shall be clearly identified to reduce the possibility of personnel causing inadvertent trips or undesired operating conditions.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-19	All physical switches (as needed) and soft controls shall provide both electrical and physical separation between the logic trip channels and the divisions.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-20	Failure of a single system component shall not prevent normal protective action of the safety system.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-21	Redundant sensor circuits in each channel (e.g. sensors, wiring, transmitter, amplifier) shall be electrically, mechanically and physically independent so that they are unlikely to be disabled by a common cause.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-22	Each division shall provide annunciation for AUTO SCRAM DIVISION and indicating light capability via the HMI and transmit computer data to the non-safety related (SR) DCS platform when a scram output signal is initiated either manually or automatically.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-23	Each division shall include a manual scram feature located in the control room that requires two distinct actions (e.g. arming prior to functioning) to be completed.	GDC 21, Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-24	Each division manual scram feature shall provide annunciation for MANUAL SCRAM SWITCH ARMED via the HMI upon completing the first distinct action.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-25	Each division manual scram shall generate a scram output signal on the second distinct action.	Project design approach	
RPS-FR-26	Each division manual scram shall execute independent of the division voting	Project design approach	It is intended that the manual scram will not be subject to software common cause failure of the PPS logic.
RPS-FR-27	A manually generated scram output signal from both divisions, at the same time, shall be necessary to cause the PPS/RPS to initiate a reactor scram (shutdown).	GDC 21, Reg Guide 1.22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379	
RPS-FR-28	Each channel shall provide a vote to scram to each division when the CI5 input condition is met. (contact closure when Reactor Mode Switch placed in Shutdown position)	GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-29	Division 1 shall initiate a scram output signal when 2oo4 scram votes for CI5 input are received.	Project design approach	
RPS-FR-30	Division 2 shall initiate a scram output signal when 2oo4 scram votes for CI5 input are received.	Project design approach	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-31	Each channel shall provide a vote to not scram to each division 10 seconds after the CI5 input condition is met (contact closure when Reactor Mode Switch placed in Shutdown position).	GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	This provides a bypass that allows each of the divisions to be reset after 10 second in the presence of a closed contact for CI5.
RPS-FR-32	Each division shall provide annunciation for MANUAL SCRAM and indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when a CI5 scram output signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-33	Each division shall provide annunciation for SHUTDOWN MODE SCRAM BYPASSED via the HMI when 2oo4 not scram votes for CI5 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-34	Each channel shall provide a vote to scram to each division when the CI12 input condition is satisfied (contact open).	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-35	Division 1 shall initiate a scram output signal when 2oo4 scram votes for CI12 input are received.	Project design approach	
RPS-FR-36	Division 2 shall initiate a scram output signal when 2oo4 scram votes for CI12 input are received.	Project design approach	
RPS-FR-37	Each channel shall provide a vote to scram to each division when the CI13 input is satisfied (contact open).	GDC 10, GDC 12, GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-38	Division 1 shall initiate a scram output signal when 2oo4 scram votes for CI13 input are received.	Project design approach	
RPS-FR-39	Division 2 shall initiate a scram output signal when 2oo4 scram votes for CI13 input are received.	Project design approach	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-40	Each division shall provide annunciation for NEUTRON MONITORING SYSTEM TRIP via the HMI and transmit computer data to the non-SR DCS platform when a CI13 scram output signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-41	Each channel shall provide a vote to scram to each division when the CI14 input is satisfied (contact open).	GDC 10, GDC 12, GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-42	Division 1 shall initiate a scram output signal when 2oo4 scram votes for CI14 input are received.	Project design approach	
RPS-FR-43	Division 2 shall initiate a scram output signal when 2oo4 scram votes for CI14 input are received.	Project design approach	
RPS-FR-44	Each division shall provide annunciation for NEUTRON MONITORING SYSTEM TRIP via the HMI and transmit computer data to the non-SR DCS platform when a CI14 scram output signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-45	Each channel shall provide a vote to scram to each division when DHP exceeds setpoint high.	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-46	Division 1 shall initiate a scram output signal when 2oo4 scram votes for DHP input are received.	Project design approach	
RPS-FR-47	Division 2 shall initiate a scram output signal when 2oo4 scram votes for DHP input are received.	Project design approach	
RPS-FR-48	Each division shall provide annunciation for DRYWELL HI PRESS TRIP via the HMI and transmit computer data to the non-SR DCS platform when a DHP scram output signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-49	Each channel shall provide a vote to annunciate to each division when DHP exceeds setpoint high.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-50	Division 1 shall provide annunciation for DRYWELL HI/LO PRESS via the HMI when 2oo4 annunciate votes for DHP high input are received.	Project design approach	
RPS-FR-51	Division 2 shall provide provide annunciation for DRYWELL HI/LO PRESS via the HMI when 2oo4 annunciate votes for DHP high input are received.	Project design approach	
RPS-FR-52	Each channel shall provide a vote to annunciate to each division when DHP exceeds setpoint low.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-53	Division 1 shall provide provide annunciation for DRYWELL HI/LO PRESS via the HMI when 2oo4 annunciate votes for DHP low input are received.	Project design approach	
RPS-FR-54	Division 2 shall provide provide annunciation for DRYWELL HI/LO PRESS via the HMI when 2oo4 annunciate votes for DHP low input are received.	Project design approach	
RPS-FR-55	Each channel shall provide a vote to scram to each division when RVP exceeds setpoint high.	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-56	Division 1 shall initiate a scram output signal when 2oo4 scram votes for RVP input are received.	Project design approach	
RPS-FR-57	Division 2 shall initiate a scram output signal when 2oo4 scram votes for RVP input are received.	Project design approach	
RPS-FR-58	Each division shall provide annunciation for REACTOR HI PRESS TRIP via the HMI and transmit computer data to the non-SR DCS platform when a RVP scram output signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-59	Each channel shall provide a vote to scram to each division when RWL3 exceeds setpoint low.	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-60	Division 1 shall initiate a scram output signal when 2oo4 scram votes for RWL3 input are received.	Project design approach	
RPS-FR-61	Division 2 shall initiate a scram output signal when 2oo4 scram votes for RWL3 input are received.	Project design approach	
RPS-FR-62	Each division shall provide annunciation for REACTOR WATER BELOW LEVEL 3 TRIP via the HMI and transmit computer data to the non-SR DCS platform when a RWL3 scram output signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-63	Each channel shall provide a vote to scram to each division when SDVL exceeds setpoint high.	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-64	Division 1 shall initiate a scram output signal when 2oo4 scram votes for SDVL input are received.	Project design approach	
RPS-FR-65	Division 2 shall initiate a scram output signal when 2oo4 scram votes for SDVL input are received.	Project design approach	
RPS-FR-66	Each division shall provide annunciation for SCRAM DISCHARGE VOLUME HI LEVEL TRIP via the HMI and transmit computer data to the non-SR DCS platform when a SDVL scram output signal is initiated	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-67	Each channel shall provide a vote to scram to each division when CI6 is satisfied (contact open).	Project design approach	
RPS-FR-68	Division 1 shall initiate a scram output signal when 2oo4 scram votes for CI6 input are received.	Project design approach	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-69	Division 2 shall initiate a scram output signal when 2oo4 scram votes for CI6 input are received.	Project design approach	
RPS-FR-70	Each division shall provide annunciation for SCRAM DISCHARGE VOLUME HI LEVEL TRIP via the HMI and transmit computer data to the non-SR DCS platform when a CI6 scram output signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-71	Each channel shall provide a vote to bypass to each division if CI4 is satisfied (contact closed).	Project design approach	
RPS-FR-72	Each division shall provide a means, under administrative control, to manually bypass each channel's SDVL vote to scram when 2oo4 bypass votes for CI4 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-73	Each division shall provide a means, under administrative control, to manually bypass each channel's CI6 vote to scram when 2oo4 bypass votes for CI4 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-74	Each division shall provide annunciation for SCRAM DISCHARGE VOLUME HI LEVEL SCRAM BYPASSED via the HMI when SDVL is bypassed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-75	Each division shall provide annunciation for SCRAM DISCHARGE VOLUME HI LEVEL SCRAM BYPASSED via the HMI when CI6 is bypassed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-76	Each division shall generate an output to RMCS for Rod Withdrawal Block interlock when SDVL **and** CI6 are bypassed.	System Interface	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-77	Division 1 shall provide a means to manually test the closure function of the SDV Vent and Drain Isolation Valves by de-energizing 120VAC solenoid A of valves C11-F009 and C11-F182.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-78	Division 2 shall provide a means to manually test the closure function of the SDV Vent and Drain Isolation Valves by de-energizing 120VAC solenoid B of valves C11-F009 and C11-F182.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-79	Each channel shall provide a vote to scram to each division when MSIV inputs CI7 **and** CI8 are satisfied (contact open).	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-80	Division 1 shall initiate a scram output signal when 2oo4 scram votes for MSIV CI7/CI8 are received.	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-81	Division 2 shall initiate a scram output signal when 2oo4 scram votes for MSIV CI7/CI8 are received.	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-82	Each division shall provide annunciation for MSIV NOT FULLY OPEN TRIP via the HMI and transmit computer data to the non-SR DCS platform when a MSIV CI7/CI8 scram output signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-83	Each channel shall provide a vote to not scram to each division to provide a bypass of the MSIV CI7 input when CI3 is satisfied (contact closed)	GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-84	Each channel shall provide a vote to not scram to each division to provide a bypass of the MSIV CI8 input when CI3 is satisfied (contact closed)	GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-85	Each division shall provide annunciation for MSIV CLOSURE SCRAM BYPASSED via the HMI when 2oo4 not scram votes for MSIV CI7 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-86	Each division shall provide annunciation for MSIV CLOSURE SCRAM BYPASSED via the HMI when 2oo4 not scram votes for MSIV CI8 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-87	Each channel shall provide the means to manually test the MSIV inputs for the MSIVs associated with the channel, one steam line at a time.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-88	Each channel shall provide a vote to scram to each division when TSV inputs CI9 **and** CI10 are satisfied (contact open).	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-89	Division 1 shall initiate a scram output signal when 2oo4 scram votes for TSV CI9/CI10 are received.	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-90	Division 2 shall initiate a scram output signal when 2oo4 scram votes for TSV CI9/CI10 are received.	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-91	Each division shall provide annunciation for TURBINE STOP VALVE CLOSURE TRIP via the HMI and transmit computer data to the non-SR DCS platform when a TSV CI9/CI10 scram output signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-92	Division 1 shall provide one output to Recirc Pump trip logic "A" when the TSV CI9/CI10 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-93	Division 1 shall provide indicating light capability via the HMI when the TSV CI9/CI10 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-94	Division 1 shall provide one output to Recirc Pump trip logic "B" when the TSV CI9/CI10 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-95	Division 1 shall provide indicating light capability via the HMI when the TSV CI9/CI10 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-96	Division 2 shall provide one output to Recirc Pump trip logic "A" when the TSV CI9/CI10 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-97	Division 2 shall provide indicating light capability via the HMI when the TSV CI9/CI10 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-98	Division 2 shall provide one output to Recirc Pump trip logic "B" when the TSV CI9/CI10 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-99	Division 2 shall provide indicating light capability via the HMI when the TSV CI9/CI10 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-100	Each channel shall provide a vote to inhibit to each division when TSP is below setpoint.	Project design approach	
RPS-FR-101	Division 1 shall inhibit the TSV related outputs to Recirc Pump trip logic "A" when 2oo4 inhibit votes for TSP are received.	System Interface	
RPS-FR-102	Division 1 shall inhibit the TSV related outputs to Recirc Pump trip logic "B" when 2oo4 inhibit votes for TSP are received.	Project design approach	
RPS-FR-103	Division 2 shall inhibit the TSV related outputs to Recirc Pump trip logic "A" when 2oo4 inhibit votes for TSP are received.	Project design approach	
RPS-FR-104	Division 2 shall inhibit the TSV related outputs to Recirc Pump trip logic "B" when 2oo4 inhibit votes for TSP are received.	Project design approach	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-105	Each channel shall provide a vote to not scram to each division to provide a bypass of the TSV CI9 input when TSP is below setpoint.	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-106	Each channel shall provide a vote to not scram to each division to provide a bypass of the TSV CI10 input when TSP is below setpoint.	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-107	Each division shall provide annunciation for TURBINE CONTROL VALVE / STOP VALVE BYPASSED via the HMI when 2oo4 not scram votes for TSV CI9 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-108	Each division shall provide annunciation for TURBINE CONTROL VALVE / STOP VALVE BYPASSED via the HMI when 2oo4 not scram votes for TSV CI10 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-109	Each channel shall provide the means to manually test the TSV inputs for the TSVs associated with the channel, one steam line at a time.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-110	Each channel shall provide a vote to scram to each division when TCV input CI11 is satisfied (contact open).	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-111	Division 1 shall initiate a scram output signal when 2oo4 scram votes for TCV CI11 are received.	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-112	Division 2 shall initiate a scram output signal when 2oo4 scram votes for TCV CI11 are received.	GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-113	Each division shall provide annunciation for TURBINE CONTROL VALVE FAST CLOSURE TRIP via the HMI and transmit computer data to the non-SR DCS platform when a TCV CI11 scram output signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-114	Division 1 shall provide one output to Recirc Pump trip logic "A" when the TCV CI11 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-115	Division 1 shall provide indicating light capability via the HMI when the TCV CI11 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-116	Division 1 shall provide one output to Recirc Pump trip logic "B" when the TCV CI11 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-117	Division 1 shall provide indicating light capability via the HMI when the TCV CI11 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-118	Division 2 shall provide one output to Recirc Pump trip logic "A" when the TCV CI11 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-119	Division 2 shall provide indicating light capability via the HMI when the TCV CI11 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-120	Division 2 shall provide one output to Recirc Pump trip logic "B" when the TCV CI11 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-121	Division 2 shall provide indicating light capability via the HMI when the TCV CI11 scram output signal is initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-122	Each channel shall provide a vote to not scram to each division to provide a bypass of the TCV input (CI11) when TSP is below setpoint.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-123	Each division shall provide annunciation for TURBINE CONTROL VALVE / STOP VALVE BYPASSED via the HMI when 2oo4 not scram votes for TCV CI11 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-124	Each channel shall provide a vote to inhibit to each division when TSP is below setpoint.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-125	Division 1 shall inhibit the TCV related outputs to Recirc Pump trip logic "A" when 2oo4 inhibit votes for TSP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-126	Division 1 shall inhibit the TCV related outputs to Recirc Pump trip logic "B" when 2oo4 inhibit votes for TSP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-127	Division 2 shall inhibit the TCV related outputs to Recirc Pump trip logic "A" when 2oo4 inhibit votes for TSP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-128	Division 2 shall inhibit the TCV related outputs to Recirc Pump trip logic "B" when 2oo4 inhibit votes for TSP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-129	Each division shall inhibit the reset of the scram output signal and logic for 10 seconds following a full scram condition.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-130	Each division shall provide a means for manually resetting a SCRAM as follows: • Provide an output that restores 120VAC power to both the "A" and "B" solenoids of scram pilot valves for rod groups 1 through 4 • Provide an output that restores 120VAC power to the both the "A" and "B" solenoids for the SDV Vent and Drain Pilot valves • Provide an output that removes 125VDC power from the "A" and "B" backup scram valve solenoids	IEEE Std. 603/IEEE Std. 7-4.3.2	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-131	Each division shall provide a means, under administrative control, to disable the TSV and TCV related outputs to Recirc Pump trip logic "A" and Recirc Pump trip logic "B" and provide annunciation via the HMI.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-132	Division 1 scram output signals shall function to de-energize the 120 VAC "A" solenoids for the Scram Pilot valves (Groups 1 through 4).	GDC 21, Reg Guide 1.22, Reg Guided 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379	Each scram pilot valve has two solenoids: one that receives a signal from Division 1 and the other from Division 2. There are 185 scram pilot valves arranged in four groups: Group 1: 45 scram pilot valves; Group 2: 45 scram pilot valves; Group 3: 47 scram pilot valves; Group 4: 48 scram pilot valves
RPS-FR-133	On a scram output, Division 1 shall provide annunciation for AUTO SCRAM and indicating light capability via the HMI and transmit computer data to the non-SR DCS platform.	GDC 21, Reg Guide 1.22, Reg Guided 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379	
RPS-FR-134	Division 2 scram output signals shall function to de-energize the 120 VAC "B" solenoids for the Scram Pilot valves (Groups 1 through 4).	GDC 21, Reg Guide 1.22, Reg Guided 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379	
RPS-FR-135	On a scram output, Division 2 shall provide annunciation for AUTO SCRAM and indicating light capability via the HMI and transmit computer data to the non-SR DCS platform.	GDC 21, Reg Guide 1.22, Reg Guided 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379	
RPS-FR-136	Division 1 scram output signals shall function to de-energize the 120 VAC "A" and "B" solenoids for the SDV Vent and Drain Pilot valves.	GDC 21, Reg Guide 1.22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379	There are two SDV Vent and Drain Pilot valves each with two solenoids (Train A solenoid and Train B solenoid). Each requires a signal from both Trip Systems to function.

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-137	Division 2 scram output signals shall function to de-energize the 120 VAC "A" and "B" solenoids for the SDV Vent and Drain Pilot valves.	GDC 21, Reg Guide 1.22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379	
RPS-FR-138	Each division shall provide a scram output signal to the Feedwater System.	System Interface	
RPS-FR-139	Each division shall provide SR to NSR isolation for the output signal to the NSR Feedwater System.	Project design approach	
RPS-FR-140	Each division scram output signal shall function to energize the 125 VDC solenoids for the "A" and "B" Back-up Scram valves. (Note that scram signals from both Division 1 and Division 2 are required to energize the 125 VDC solenoids for the Back-up Scram valves.)	IEEE Std. 603/IEEE Std. 7-4.3.2	There are two Back-up Scram solenoid valves (one associated with Trip System A, and one associated with Trip System B).
RPS-FR-141	Upon energization of the 125 VDC solenoids for the Back-up Scram valves, each division shall provide data for display via the HMI and to the non-SR DCS platform.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-142	In response to valve position sensor contact inputs from each of two SDV vent valves, each division shall provide indicating lights via the HMI and transmit computer data to the non-SR DCS platform to indicate open position.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-143	In response to valve position sensor contact inputs from each of two SDV vent valves, each division shall provide indicating lights via the HMI to indicate close position.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-144	In response to valve position sensor contact inputs from each of two SDV drain valves, each division shall provide indicating lights via the HMI and transmit computer data to the non-SR DCS platform to indicate open position.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-145	In response to valve position sensor contact inputs from each of two SDV drain valves, each division shall provide indicating lights via the HMI to indicate close position.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-146	Each division shall provide a means to manually provide annunciation and an alarm light via the HMI.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-147	The maximum operating time from receipt of a condition met signal (contact state change or analog signal exceeding setpoint), to and including opening of the contacts on the main trip actuators (scram contactors), shall be less than 50 milliseconds.	IEEE Std. 603/IEEE Std. 7-4.3.2	Ensures that the RPS logic responds sufficiently fast so as to be effective in limiting the various transients. The 50 milliseconds is an analytical limit used in transient analyses that involve the scram function.
RPS-FR-148	Each division shall provide annunciation via the HMI in response to an unacceptable operating status condition.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RPS-FR-149	Each channel shall provide the means to perform functional tests during normal plant operation.	GDC 21, Reg Guide 1.22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
RPS-FR-150	Each channel and each division shall provide sufficient features and documented evaluations to support elimination of most Technical Specification Surveillance Tests, and minimize the requirements for manual calibration checks.	Project design approach	
RPS-FR-151	For all PPS inputs that have the potential to require manual test insertion or external measurement of input or output values (i.e., use of an external digital multi meter by a technician), test jacks are provided in the cabinets.	Project design approach	

RPS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RPS Requirement**	**PPS/RPS Source / Basis**	**Notes / Clarification**
RPS-FR-152	For all inputs that have the potential to require manual multi-point calibration checks with external calibration equipment, knife edge disconnects along with test jacks are incorporated in the field termination panels.	Project design approach	

B

B.1 N4S Design Requirements

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-1	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. 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. 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.	GDC 1 - Quality standards and records.
N4S-DR-2	Structures, systems, and components important to safety shall be designed to withstand the effect of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions.	GDC 2 - Design Bases for Protection Against Natural Phenomena
N4S-DR-3	Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions.	GDC 3 - Fire protection
N4S-DR-4	Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents (LOCAs).	GDC 4 - Environmental and dynamic effects design bases
N4S-DR-5	The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.	GDC 10 - Reactor design

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-6	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.	GDC 13 - Instrumentation and control
N4S-DR-7	A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. 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 I&C 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.	GDC 19 - Control Room
N4S-DR-8	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.	GDC 20 - Protection system functions

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-9	The protection system shall be designed for high functional reliability and in-service 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.	GDC 21 - Protection system reliability and testability
N4S-DR-10	The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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.	GDC 22- Protection system independence
N4S-DR-11	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.	GDC 23 - Protection system failure modes
N4S-DR-12	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.	GDC 24 - Separation of protection and control systems

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-13	The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.	GDC 29 - Protection against anticipated operational occurrences
N4S-DR-14	A system to remove residual heat shall be provided. The system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified acceptable fuel design limits and the design conditions of the reactor coolant pressure boundary are not exceeded.	GDC 34 - Residual heat removal.
N4S-DR-15	The protection system shall be designed to permit periodic testing of its initiation functions inclusive of the actuation devices and actuated equipment when the reactor is in operation.	Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions (Safety Guide 22)
N4S-DR-16	Those structures, systems, and components (SSC) that should be designed to remain functional if the Safe Shutdown Earthquake (SSE) occurs shall be designated as Seismic Category I. (This includes Systems or portions of systems that are required for reactor shutdown; all electric and mechanical devices and circuitry between the process and the input terminals of the actuator systems involved in generating signals that initiate protective action; systems or portions of systems that are required for (1) monitoring of systems important to safety and (2) actuation of systems important to safety.)	Regulatory Guide 1.29 - Seismic Design Classification
N4S-DR-17	The N4S shall comply with the requirements of Appendix B to 10 CFR Part 50 for the installation, inspection, and testing of nuclear power plant instrumentation and electric equipment.	Regulatory Guide 1.30 - Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment (Safety Guide 30)
N4S-DR-18	The N4S shall meet the requirements for indicating the bypass or inoperable status of portions of the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the system it actuates to perform their safety-related functions:	Regulatory Guide 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-19	The N4S shall comply with the IEEE Std. 279 requirement that any single failure within the protection system shall not prevent proper protective action at the system level when required, by utilizing the guidance in IEEE Std. 379-1972 for applying the single-failure criterion to the design and analysis of nuclear power plant protection systems.	Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Safety Systems
N4S-DR-20	The N4S shall provide a means for manual initiation of protective actions.	Regulatory Guide 1.62 - Manual Initiation of Protective Actions
N4S-DR-21	The N4S shall meet the requirements for physical independence of the circuits and electric equipment comprising or associated with the Class 1E power system, the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety related functions.	Regulatory Guide 1.75 - Physical Independence of Electric Systems
N4S-DR-22	The N4S shall comply with design verification requirements to verify adequacy of design under the most adverse design conditions.	Regulatory Guide 1.89 - Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants
N4S-DR-23	The N4S shall comply with the requirement to: (1) provide information required to permit the operator to take preplanned manual actions to accomplish safe plant shutdown; (2) determine whether the reactor trip, engineered safety feature systems, and manually initiated safety systems and other systems important to safety are performing their intended functions (i.e., reactivity control, core cooling, maintaining reactor coolant system integrity, and maintaining containment integrity); (3) provide information to the operators that will enable them to determine the potential for causing a gross breach of the barriers to radioactivity release (i.e., fuel cladding, reactor coolant pressure boundary, and containment) and to determine if a gross breach of a barrier has occurred.	Regulatory Guide 1.97 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-24	The N4S shall comply with design verification requirements to verify the seismic adequacy of electric equipment.	Regulatory Guide 1.100 - Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants
N4S-DR-25	The N4S design shall implement setpoints that assure sufficient margin between Technical Specification limits and the trip setpoint to account for instrument inaccuracy, calibration uncertainties and instrument drift. Consideration of instrument span and range as well as environmental influences must be included.	Regulatory Guide 1.105 - Instrument Setpoint
N4S-DR-26	The N4S shall comply with the requirements for periodic testing of electric power and protection systems.	Regulatory Guide 1.118 - Periodic Testing of Electric Power and Protection Systems
N4S-DR-27	N4S shall, with precision and reliability, initiate the closure of specific isolation valves based on the sensing of specified process variables.	IEEE Std. 603, Section 5.0 Safety System Criteria and 6.1 Automatic Control

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-28	The listed N4S isolation shall initiate when the monitored plant parameter exceeds the following trip setpoint: Reactor Vessel Water Level 1 < -129 inches Reactor Vessel Water Level 2 < -38 inches Reactor Vessel Water Level 3 < 12.5 inches Drywell High Pressure > 1.68 psig Reactor Pressure < 455 psig Main Steam Line Pressure < 840 psig Main Steam Line Flow > 122.1 psid Condenser Vacuum 10.5 psia Outboard MSIV Room Temp > 192^{o}F Turbine Encl - Main Steam Line Tunnel Temp > 192^{o}F Reactor Vessel Pressure > 75 psig RWCS Δ flow > 54.9 gpm RWCS HX Room Area Temp > 120^{o}F RWCS Pump Room Area Temp > 155^{o}F RWCS HX Room Area Ventilation Δ Temp > 32^{o}F RWCS Pump Room Area Ventilation Δ Temp > 52^{o}F HPCI Steam Line Δ Pressure > 974" H2O HPCI Steam Supply Pressure < 100 psig HPCI Turbine Exhaust Diaphragm Pressure > 10 psig HPCI Equipment Room Temp 180^{o}F HPCI Equipment Room Δ Temp > 104^{o}F HPCI Pipe Routing Area Temp 180^{o}F HPCI Steam Line Δ Pressure Timer > 3 sec, <12.5 seconds	IEEE Std. 603, Section 6.1 Automatic Control

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-29	The listed N4S isolation shall initiate when the monitored plant parameter exceeds the following trip setpoint: RCIC Steam Line Δ Pressure > 373" H2O RCIC Steam Supply Pressure < 64.5 psig RCIC Turbine Exhaust Diaphragm Pressure > 10 psig RCIC Equipment Room Temp 180°F RCIC Equipment Room Δ Temp > 109°F RCIC Pipe Routing Area Temp 180°F RCIC Steam Line Δ Pressure Timer > 3 sec, <12.5 seconds North Stack Effluent Radiation > 2.1 µCi/cc Reactor Encl Ventilation Exhaust Duct Radiation > 1.35 mR/h Primary Containment Instrument Gas to Drywell Δ Pressure < 2.0 psi Refueling Area Unit 1 Ventilation Exhaust Duct Radiation > 2.0 mR/h Refueling Area Unit 2 Ventilation Exhaust Duct Radiation > 2.0 mR/h	IEEE Std. 603, Section 6.1 Automatic Control
N4S-DR-30	The signal input to actuation output propagation time of the N4S logic shall be less than 50 milliseconds.	IEEE Std. 603, Section 4.10
N4S-DR-31	The N4S shall be capable of initiating under all required modes of reactor operation.	IEEE Std. 603, Section 4.1
N4S-DR-32	The N4S shall ensure that the protective action, once started, continues to completion.	IEEE Std. 603, Section 5.2 Completion of Protective Action
N4S-DR-33	Any single failure within the N4S shall not prevent proper protective action at the system level when required.	IEEE Std. 603, Section 5.1 Single Failure Criterion and IEEE Std. 7-4.3.2 Section 5.1 Single Failure Criterion

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-34	Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.	IEEE Std. 603 section 5.3 Quality and IEEE Std. 7-4.3.2 section 5.3 Quality
N4S-DR-35	Type test data or reasonable engineering extrapolation based on test data shall be available to verify that protection system equipment shall meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements.	IEEE Std. 603 section 5.4 Equipment Qualification and IEEE Std. 7-4.3.2 section 5.4 Equipment Qualification
N4S-DR-36	All protection system channels shall be designed to maintain necessary functional capability under extremes of conditions (as applicable) relating to environment, energy supply, malfunctions. and accidents.	IEEE Std. 603 section 5.5 System Integrity and IEEE Std. 7-4.3.2 and section 5.5 Independence
N4S-DR-37	Channels that provide signals for the same protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 System Integrity
N4S-DR-38	Any equipment that is used for both protective and control functions shall be classified as part of the protection system and shall meet all the applicable requirements.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence
N4S-DR-39	The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system and shall meet all the applicable requirements. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-40	Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
N4S-DR-41	Provisions shall be included so that the protective action can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
N4S-DR-42	Where a credible single event can cause a control system action that results in a condition requiring protective action and can concurrently prevent the protective action from those protection system channels designated to provide principal protection against the condition, then alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design bases.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
N4S-DR-43	To the extent feasible and practical, protection system inputs shall be derived from signals that are direct measures of the desired variables.	IEEE Std. 603 section 6.4 Derivation of System Inputs
N4S-DR-44	Means shall be provided for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
N4S-DR-45	Capability shall be provided for testing and calibrating channels and the devices used to derive the final system output signal from the various channel signals.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
N4S-DR-46	For those parts of the system where the required interval between testing will be less than the normal time interval between generating station shutdowns, there shall be capability for testing during power operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-47	The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective action at the systems level.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
N4S-DR-48	During such operation, the active parts of the system shall of themselves continue to meet the single failure criterion.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
N4S-DR-49	Where operating requirements necessitate automatic or manual bypass of a protective function, the design shall be such that the bypass will be removed automatically whenever permissive conditions are not met.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
N4S-DR-50	Devices used to achieve automatic removal of the bypass of a protective function are part of the protection system and shall be designed in accordance with these criteria.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
N4S-DR-51	If the protective action of some part of the system has been bypassed or deliberately rendered inoperative for any purpose, this fact shall be continuously indicated in the control room.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
N4S-DR-52	The design shall permit the administrative control of the means for manually bypassing channels or protective functions.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
N4S-DR-53	Where it is necessary to change to a more restrictive set point to provide adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of assuring that the more restrictive set point is used.	IEEE Std. 603 section 6.8 Setpoints
N4S-DR-54	The devices used to prevent improper use of less restrictive set points shall be considered a part of the protection system and shall be designed in accordance with the other provisions of these criteria regarding performance and reliability.	IEEE Std. 603 section 6.8 Setpoints
N4S-DR-55	The protection system shall be so designed that, once initiated, a protective action at the system level shall go to completion.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-56	Return to operation shall require subsequent deliberate operator action.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action
N4S-DR-57	The protection system shall include means for manual initiation of each protective action at the system level (for example, reactor trip, containment isolation, safety injection, core spray, etc).	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
N4S-DR-58	No single failure within the manual, automatic, or common portions of the protection system shall prevent initiation of protective action by manual or automatic means.	IEEE Std. 603 section 7.2 Manual Control
N4S-DR-59	Manual initiation should depend upon the operation of a minimum of equipment.	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
N4S-DR-60	The design shall permit the administrative control of access to all set point adjustments, module calibration adjustments, and test points.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
N4S-DR-61	Protective actions shall be indicated and identified down to the channel level.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
N4S-DR-62	The protection system shall be designed to provide the operator with accurate, complete, and timely information pertinent to its own status and to generating station safety.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
N4S-DR-63	The design shall minimize the development of conditions which would cause meters, annunciators, recorders, alarms, etc, to give anomalous indications confusing to the operator.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
N4S-DR-64	The system shall be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.	IEEE Std. 603 section 5.10 Repair

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-65	In order to provide assurance that the requirements given in this document can be applied during the design, construction, maintenance, and operation of the plant, the protection system equipment (for example, interconnecting wiring, components, modules, etc), shall be identified distinctively as being in the protection system.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
N4S-DR-66	This identification shall distinguish between redundant portions of the protection system. (In the installed equipment, components, or modules mounted in assemblies that are clearly identified as being in the protection system do not themselves require identification.) All software, firmware, and programmable logic shall be identified in accordance with IEEE Std. 7-4.3.2 Clause 5.11.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
N4S-DR-67	N4S shall conform to the design criteria and features for Class 1E electric systems to ensure that functional requirements under the conditions produced by design basis events are met.	IEEE Std. 308 - Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations
N4S-DR-68	N4S shall conform to the methods for demonstrating the qualification of Class 1E equipment including components or equipment of any interface whose failure could adversely affect the performance of Class 1E systems and electronic equipment.	IEEE Std. 323 - Qualifying Class 1E Equipment for Nuclear Power Generating Stations
N4S-DR-69	N4S shall conform to the design and operational criteria for the performance of periodic testing of nuclear power generating station safety systems.	IEEE Std. 338 - Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems
N4S-DR-70	N4S shall meet its Class 1E performance requirements during and following one SSE (safe shutdown earthquake) preceeded by a number of OBEs (operating basis earthquakes).	IEEE Std. 344 - Guide for Seismic Qualification of Class 1 Electric Equipment for Nuclear Power Generating Stations
N4S-DR-71	N4S shall meet the single failure criterion as described and classified in IEEE Std. 379.	IEEE Std. 379 - Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

N4S DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
N4S-DR-72	N4S shall meet the criteria and requirements for establishing and maintaining the independence of Class 1E equipment and circuits and auxiliary supporting features by physical separation and electrical isolation.	IEEE Std. 384 - Criteria for Independence of Class 1E Equipment and Circuits

B.2 N4S Functional Requirements

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-1	PPS/N4S shall be capable of providing signals to automatically initiate closure of various isolation valves if monitored system variables exceed pre-established limits, or by manual initiation.	GDC 19, GDC 20, GDC 54, GDC 60, 10CFR50.67, 10CFR20, 10CFR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-2	PPS/N4S shall be comprised of four (4) divisions (Division 1, Division 2, Division 3 and Division 4) that are capable of initiating isolations for separate valve groups based on conditions of monitored system variables	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-3	The PPS/NSSS shall have four (4) independent channels (Channel A, Channel B, Channel C and Channel D) that each provide votes/signals to each of the divisions.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	The four channels are common to each of the divisions.
N4S-FR-4	The PPS/N4S shall be capable of being powered by 120VAC +/- 10% (108 to 132 VAC) power.	Original design feature	
N4S-FR-5	Each division shall provide outputs that are capable of interfacing with 120VAC loads.	Original design feature	
N4S-FR-6	Each division shall provide outputs that are capable of interfacing with 125VDC loads (MSIV solenoids).	Original design feature	
N4S-FR-7	The PPS/N4S logic shall be a normally energized system (fail-safe type design). (i.e., initiate isolations on loss of electrical power).	GDC 21, GDC 23, Reg Guide 1.47	
N4S-FR-8	Each input to a channel (ma or contact input) shall be voted on by the channel based on the condition (condition met or not met).	Project design approach	The term "shall be voted on" indicates that the channel performs a bi-stable comparison against a pre-determined configurable setpoint to determine whether the input is at or above/below the setpoint value.

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-9	Each channel shall provide the status of the vote (e.g. vote to not function if condition not met; vote to function if condition met, vote to annunciate) to each of the divisions.	Project design approach	The terms “not function”, “function”, “annunciate” describe different types of votes that may be provided by a channel (Note -others may be specified within the requirements). A particular vendor solution may combine one or more of the vote types into a single channel vote based on the capabilities of the platform.
N4S-FR-10	Each division shall determine whether the votes to function for each type of input satisfy the voting criteria (e.g. 2oo4).	Project design approach	
N4S-FR-11	Each division shall execute a function when the voting criteria are satisfied.	Project design approach	
N4S-FR-12	Each input to a channel shall have an independent voter (e.g. 2oo4) within each division to ensure that trip inputs are voted separately.	Project design approach	
N4S-FR-13	Each division shall generate an output for an isolation trip initiation, when the required voting has been satisfied.	Project design approach	As an example, the RWL1 input to Channels A, B, C, and D shall be sent to a 2oo4 voter in each of the divisions (Division 1, Division 2, Division 3 and Division 4). When at least two of the four RWL1 inputs to the 2oo4 voter achieve a trip state, the associated division generates an output. The generated output may be dependent on additional voting to be satisfied. Some isolation outputs require different voting schemes which are described within the requirement.

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-14	Each channel shall receive an input from each of the following monitored parameters that are provided as common inputs to the PPS platform and are shared by each of the PPS functions: • Reactor Vessel Water Level 1 (RWL1) • Reactor Vessel Water Level 2 (RWL2) • Reactor Vessel Water Level 3 (RWL3) • Reactor Vessel Pressure (RVP) • Drywell Pressure (DP)	GDC 13, GDC 19, GDC 20, GDC 30, GDC 60, 10CFR20, 10CFR50.67, 10CFR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-15	Each channel shall receive analog (4-20 mA) inputs from for each of the following monitored parameters: • Main Steam Line Flow (MSLF) (qty - 4) • Main Steam Line Pressure (MSLP) • Condenser Vacuum (CV)	Original design feature	Each channel receives a Main Steam Line Flow input from Steam Line "A", "B", "C" and "D".

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-16	Channel A shall receive Type T thermocouple (T/C) inputs from the following areas: • RCIC Pipe Area - Ambient Temp (Qty - 5) (RCPAT) • RCIC Equipment Area - Ambient Temp (Qty - 1) (RCEAT1) • RCIC Equipment Area - Ambient Temp (Qty - 1) (RCEAT2) • RCIC Equipment Area - Differential Temp (Qty - 2 pairs) (RCEDT) • Main Steam Line - Ambient Temp (Qty - 4) (MSLAT1) • Main Steam Line - Ambient Temp (Qty - 1) (MSLAT2) • Main Steam Line - Differential Temp (Qty - 1 pair) (MSLDT) • RWCU - Ambient Temp (qty - 6) (RWAT) • RWCU - Differential Temp (qty - 6 pairs) (RWDT)	Project design approach	
N4S-FR-17	Channel A shall provide a vote to isolate to each division when any of the four (4) MSLAT1 temperature inputs exceeds setpoint.	Project design approach	
N4S-FR-18	Channel A shall provide a vote to annunciate to each division when any of the four (4) MSLAT1 temperature inputs exceeds setpoint.	Project design approach	
N4S-FR-19	Channel A shall provide a vote to isolate to each division when any of the six (6) RWAT or six (6) RWDT temperature inputs exceeds setpoint.	Project design approach	
N4S-FR-20	Channel A shall provide a vote to annunciate to each division when any of the six (6) RWAT or six (6) RWDT temperature inputs exceeds setpoint.	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-21	Channel A shall provide a vote to isolate to each division when any of the five (5) RCPAT temperature inputs or one (1) RCEAT1 temperature input or two (2) RCEDT temperature input exceeds setpoint.	Project design approach	
N4S-FR-22	Channel A shall provide a vote to annunciate to each division when any of the five (5) RCPAT temperature inputs or one (1) RCEAT1 temperature input or two (2) RCEDT temperature input exceeds setpoint.	Project design approach	
N4S-FR-23	Channel A shall provide a vote to annunciate to each division when the RCEAT2 temperature input exceeds setpoint.	Project design approach	
N4S-FR-24	Channel A shall provide a vote to annunciate to each division when the MSLAT2 temperature input exceeds setpoint.	Project design approach	
N4S-FR-25	Channel A shall provide a vote to annunciate to each division when the MSLDT temperature input exceeds setpoint.	Project design approach	
N4S-FR-26	Division 1 shall provide a signal to PPS/RCIC when 1oo2 isolate votes for RCPAT / RCEAT1 / RCEDT temperature input are received.	Project design approach	
N4S-FR-27	Division 1 shall provide a signal to PPS/RCIC when 1oo2 annunciate votes for RCPAT / RCEAT1 / RCEDT temperature input are received.	Project design approach	
N4S-FR-28	Division 1 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 2oo4 annunciate votes are received for the MSLAT1 input.	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-29	Division 1 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 1oo2 annunciate votes are received for the RWAT / RWDT input.	Project design approach	
N4S-FR-30	Division 1 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 1oo2 annunciate votes are received for the RCPAT / RCEAT1 / RCEDT input.	Project design approach	
N4S-FR-31	Division 1 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 1oo1 annunciate votes are received for the RCEAT2 input.	Project design approach	
N4S-FR-32	Division 1 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 1oo1 annunciate votes are received for the MSLAT2 input.	Project design approach	
N4S-FR-33	Division 1 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 1oo1 annunciate votes are received for the MSLDT input.	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-34	Channel B shall receive Type T T/C inputs from the following areas: • HPCI Pipe Area - Ambient Temp (Qty - 4) (HPPAT) • HPCI Equipment Area - Ambient Temp (Qty - 1) (HPEAT1) • HPCI Equipment Area - Ambient Temp (Qty - 1) (HPEAT2) • HPCI Equipment Area - Differential Temp (Qty - 1 pair) (HPEDT) • Main Steam Line - Ambient Temp (Qty - 4) (MSLAT1)	Project design approach	
N4S-FR-35	Channel B shall provide a vote to isolate to each division when any of the four (4) MSLAT1 temperature inputs exceeds setpoint.	Project design approach	
N4S-FR-36	Channel B shall provide a vote to annunciate to each division when any of the four (4) MSLAT1 temperature inputs exceeds setpoint.	Project design approach	
N4S-FR-37	Channel B shall provide a vote to isolate to each division when any of the four (4) HPPAT temperature inputs or one (1) HPEAT1 temperature input or one (1) HPEDT temperature input exceeds setpoint.	Project design approach	
N4S-FR-38	Channel B shall provide a vote to annunciate to each division when any of the four (4) HPPAT temperature inputs or one (1) HPEAT1 temperature input or one (1) HPEDT temperature input exceeds setpoint.	Project design approach	
N4S-FR-39	Channel B shall provide a vote to annunciate to each division when the HPEAT2 temperature input exceeds setpoint.	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-40	Division 2 shall provide a signal to PPS/HPCI when 1oo2 isolate votes for HPPAT / HPEAT1 / HPEDT temperature input are received.	Project design approach	
N4S-FR-41	Division 2 shall provide a signal to PPS/HPCI when 1oo2 annunciate votes for HPPAT / HPEAT1 / HPEDT temperature input are received.	Project design approach	
N4S-FR-42	Division 2 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 2oo4 annunciate votes are received for the MSLAT1 input.	Project design approach	
N4S-FR-43	Division 2 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 1oo2 annunciate votes for the HPPAT / HPEAT1 / HPEDT temperature input are received.	Project design approach	
N4S-FR-44	Division 2 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 1oo1 annunciate votes are received for the HPEAT2 input.	Project design approach	
N4S-FR-45	Logic trip channel C shall receive Type T T/C inputs from the following areas: • RCIC Pipe Area - Ambient Temp (Qty - 5) (RCPAT) • RCIC Equipment Area - Ambient Temp (Qty - 1) (RCEAT1) • RCIC Equipment Area - Differential Temp (Qty - 1 pairs) (RCEDT) • Main Steam Line - Ambient Temp (Qty - 4) (MSLAT1) • RHR - Ambient Temp (qty - 1) (RHRATC) • RHR - Differential Temp (qty - 1 pair) (RHRDTC)	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-46	Channel C shall provide a vote to isolate to each division when any of the four (4) MSLAT1 temperature inputs exceeds setpoint.	Project design approach	
N4S-FR-47	Channel C shall provide a vote to annunciate to each division when any of the four (4) MSLAT1 temperature inputs exceeds setpoint.	Project design approach	
N4S-FR-48	Channel C shall provide a vote to isolate to each division when any of the five (5) RCPAT temperature inputs or one (1) RCEAT1 temperature input or one (1) RCEDT temperature input exceeds setpoint.	Project design approach	
N4S-FR-49	Channel C shall provide a vote to annunciate to each division when any of the five (5) RCPAT temperature inputs or one (1) RCEAT1 temperature input or one (1) RCEDT temperature input exceeds setpoint.	Project design approach	
N4S-FR-50	Channel C shall provide a vote to annunciate to each division when either the one (1) RHRAT temperature input or the one (1) RHRDT temperature input exceeds setpoint.	Project design approach	
N4S-FR-51	Division 3 shall provide a signal to PPS/RCIC when 1oo2 isolate votes for RCPAT / RCEAT1 / RCEDT temperature input are received.	Project design approach	
N4S-FR-52	Division 3 shall provide a signal to PPS/RCIC when 1oo2 annunciate votes for RCPAT / RCEAT1 / RCEDT temperature input are received.	Project design approach	
N4S-FR-53	Division 3 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 2oo4 annunciate votes are received for the MSLAT1 input.	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-54	Division 3 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 1oo2 annunciate votes are received for the RCPAT / RCEAT1 / RCEDT temperature input.	Project design approach	
N4S-FR-55	Division 3 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 1oo2 annunciate votes for the RHRAT / RHRDT temperature input are received.	Project design approach	
N4S-FR-56	Channel D shall receive Type T T/C inputs from the following areas: • HPCI Pipe Area - Ambient Temp (Qty - 4) (HPPAT) • HPCI Equipment Area - Ambient Temp (Qty - 1) (HPEAT1) • HPCI Equipment Area - Differential Temp (Qty - 1 pair) (HPEDT) • Main Steam Line - Ambient Temp (Qty - 4) (MSLAT1) • RHR - Ambient Temp (qty - 1) (RHRAT) • RHR - Differential Temp (qty - 1 pair) (RHRDT) • RWCU - Ambient Temp (qty - 6) (RWAT) • RWCU - Differential Temp (qty - 6 pairs) (RWDT)	Project design approach	
N4S-FR-57	Channel D shall provide a vote to isolate to each division when any of the four (4) MSLAT1 temperature inputs exceeds setpoint.	Project design approach	
N4S-FR-58	Channel D shall provide a vote to annunciate to each division when any of the four (4) MSLAT1 temperature inputs exceeds setpoint.	Project design approach	
N4S-FR-59	Channel D shall provide a vote to isolate to each division when any of the six (6) RWAT or six (6) RWDT temperature inputs exceeds setpoint.	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-60	Channel D shall provide a vote to annunciate to each division when any of the six (6) RWAT or six (6) RWDT temperature inputs exceeds setpoint.	Project design approach	
N4S-FR-61	Channel D shall provide a vote to isolate to each division when any of the four (4) HPPAT temperature inputs or one (1) HPEAT1 temperature input or one (1) HPEDT temperature input exceeds setpoint.	Project design approach	
N4S-FR-62	Channel D shall provide a vote to annunciate to each division when any of the four (4) HPPAT temperature inputs or one (1) HPEAT1 temperature input or one (1) HPEDT temperature input exceeds setpoint.	Project design approach	
N4S-FR-63	Channel D shall provide a vote to annunciate to each division when either the one (1) RHRAT temperature input or the one (1) RHRDT temperature input exceeds setpoint.	Project design approach	
N4S-FR-64	Division 4 shall provide a signal to PPS/HPCI when 1oo2 isolate votes for HPPAT / HPEAT1 / HPEDT temperature input are received.	Project design approach	
N4S-FR-65	Division 4 shall provide a signal to PPS/HPCI when 1oo2 annunciate votes for HPPAT / HPEAT1 / HPEDT temperature input are received.	Project design approach	
N4S-FR-66	Division 4 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 2oo4 annunciate votes are received for the MSLAT1 input.	Project design approach	
N4S-FR-67	Division 4 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 1oo2 annunciate votes for the RWAT / RWDT temperature input are received.	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-68	Division 4 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 1oo2 annunciate votes for the HPPAT / HPEAT1 / HPEDT temperature input are received.	Project design approach	
N4S-FR-69	Division 4 shall provide annunciation for STEAM LEAK DETECTION SYSTEM HI TEMP / TROUBLE via the HMI when 1oo2 annunciate votes for the RHRAT / RHRDT temperature input are received.	Project design approach	
N4S-FR-70	Channel A and Channel D shall receive analog (4-20 mA) inputs from for each of the following monitored parameters: • RWCU Flow to Main Condenser (RFMC) • RWCU Flow to Feedwater (RFF) • RWCU Suction from Reactor (RSR)	Project design approach	
N4S-FR-71	Channel A shall condition each of the RFMC, RFF and RSR signals through a square root converter.	Project design approach	
N4S-FR-72	Channel A shall sum the conditioned signals for RFMC, RFF and RSR to obtain a RWCU differential flow signal (DFS).	Project design approach	
N4S-FR-73	Channel A shall provide the DFS signal to Division 1.	Project design approach	
N4S-FR-74	Division 1 shall provide the DFS signal for indicator display via the HMI.	Project design approach	
N4S-FR-75	Channel D shall condition each of the RFMC, RFF and RSR signals through a square root converter.	Project design approach	
N4S-FR-76	Channel D shall sum the conditioned signals for RFMC, RFF and RSR to obtain a RWCU differential flow signal (DFS).	Project design approach	
N4S-FR-77	Channel D shall provide the DFS signal to Division 4.	Project design approach	
N4S-FR-78	Division 4 shall provide the DFS signal for indicator display via the HMI.	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-79	Channel A shall initiate a timer when DFS exceeds setpoint.	Project design approach	
N4S-FR-80	Channel A shall provide a vote to annunciate to Division 1.	Project design approach	
N4S-FR-81	Division 1 shall provide annunciation for RWCU HI DIFF FLOW ISO TIMER INITIATED via the HMI when a 1oo1 annunciate vote for DFS high is received.	Project design approach	
N4S-FR-82	Channel D shall initiate a timer when DFS exceeds setpoint.	Project design approach	
N4S-FR-83	Channel D shall provide a vote to annunciate to Division 4.	Project design approach	
N4S-FR-84	Division 4 shall provide annunciation for RWCU HI DIFF FLOW ISO TIMER INITIATED via the HMI when a 1oo1 annunciate vote for DFS high is received.	Project design approach	
N4S-FR-85	Channel A shall provide a vote to isolate to each division when the DFS timer expires.	Project design approach	
N4S-FR-86	Channel D shall provide a vote to isolate to each division when the DFS timer expires.	Project design approach	
N4S-FR-87	Each channel shall receive the following contact inputs: • Turbine Stop Valve (CI1) • Reactor Building Radiation K91 5-9 (CI7) • Reactor Building Radiation K91 6-10 (CI10) • Refuel Floor Radiation K92 5-9 (CI8) • Refuel Floor Radiation K92 6-10 (CI11) • Reactor Mode Switch MSL Low Pressure Bypass (CI17)	GDC 13, GDC 19, GDC 20, GDC 30, GDC 60, 10CFR20, 10CFR50.67, 10CFR100	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-88	Channel A and Channel B shall receive the following contact inputs: • Main Steam Line Radiation (CI2) • not used (CI9)	GDC 13, GDC 19, GDC 20, GDC 30, GDC 60, 10CFR20, 10CFR50.67, 10CFR100	LGS decision - CI9 input not to be included
N4S-FR-89	Channel A and Channel D shall receive the following contact input: • Standby Liquid Control Pump operating status (CI3) • not used (CI4) • not used (CI5) • Loss of Valve and Logic Power / MOV overcurrent 49X (CI12)	GDC 13, GDC 19, GDC 20, GDC 30, GDC 60, 10CFR20, 10CFR50.67, 10CFR100	
N4S-FR-90	Channel D shall receive the following contact input: • RWCU Non-Regenerative HX temperatures (CI6) • G31-F004 74-21619-10 (CI14) • G31-F004 LS2 (CI16) • 03-2BQ052 Logic Reset (CI18)	GDC 13, GDC 19, GDC 20, GDC 30, GDC 60, 10CFR20, 10CFR50.67, 10CFR100	
N4S-FR-91	Channel A shall receive the following contact input: • G31-F001 74-21150-15 (CI13) • G31-F001 LS2 (CI15) • 03-2AQ076 Logic Reset (CI19)	Original design feature	
N4S-FR-92	Each channel shall include a manual isolation initiation feature located in the control room that requires two distinct actions (e.g. arming prior to functioning) to be completed.	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-93	Channel A shall provide a vote to annunciate to Division 1 upon the first distinct action for the associated manual isolation initiation feature being satisfied.	Project design approach	
N4S-FR-94	Channel B shall provide a vote to annunciate to Division 2 upon the first distinct action for the associated manual isolation initiation feature being satisfied.	Project design approach	
N4S-FR-95	Channel C shall provide a vote to annunciate to Division 3 upon the first distinct action for the associated manual isolation initiation feature being satisfied.	Project design approach	
N4S-FR-96	Channel D shall provide a vote to annunciate to Division 4 upon the first distinct action for the associated manual isolation initiation feature being satisfied.	Project design approach	
N4S-FR-97	Division 1 shall provide annunciation for MANUAL ISOLATION SWITCH ARMED via the HMI when 1oo1 annunciate votes are received for the first distinct action for the manual isolation initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-98	Division 2 shall provide annunciation for MANUAL ISOLATION SWITCH ARMED via the HMI when 1oo1 annunciate votes are received for the first distinct action for the manual isolation initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-99	Division 3 shall provide annunciation for MANUAL ISOLATION SWITCH ARMED via the HMI when 1oo1 annunciate votes are received for the first distinct action for the manual isolation initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-100	Division 4 shall provide annunciation for MANUAL ISOLATION SWITCH ARMED via the HMI when 1oo1 annunciate votes are received for the first distinct action for the manual isolation initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-101	Channel A shall provide a vote for manual initiation to Division 1 on the second distinct action being satisfied.	Project design approach	
N4S-FR-102	Channel A shall provide a vote to annunciate to Division 1 on the second distinct action being satisfied.	Project design approach	
N4S-FR-103	Channel B shall provide a vote for manual initiation to Division 2 on the second distinct action being satisfied.	Project design approach	
N4S-FR-104	Channel B shall provide a vote to annunciate to Division 2 on the second distinct action being satisfied.	Project design approach	
N4S-FR-105	Channel C shall provide a vote for manual initiation to Division 3 on the second distinct action being satisfied.	Project design approach	
N4S-FR-106	Channel C shall provide a vote to annunciate to Division 3 on the second distinct action being satisfied.	Project design approach	
N4S-FR-107	Channel D shall provide a vote for manual initiation to Division 4 on the second distinct action being satisfied.	Project design approach	
N4S-FR-108	Channel D shall provide a vote to annunciate to Division 4 on the second distinct action being satisfied.	Project design approach	
N4S-FR-109	The N4S isolation outputs to close valves shall be designed so that manual resetting of the system logic will not result in the reopening of the valves.	NUREG-0578	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-110	The N4S isolation outputs to close valves shall be designed so that valves will continue to close until full closure has been achieved, once an isolation signal has been initiated, without being able to be stopped or reopened.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-111	The N4S isolation outputs to close valves shall be designed so that after reaching full closure, the valves will not automatically reopen after the closure signal has ceased.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-112	A manual isolation of the MSIVs (in Group 1A) shall require an isolation signal from Division 1 **AND** an isolation signal from Division 4 when 1oo1 trip systems for a manual initiation is received.	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
N4S-FR-113	Division 1 shall provide a manual isolation signal for the MSIVs (in Group 1A) when 1oo1 votes for a manual initiation is received.	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
N4S-FR-114	Division 4 shall provide a manual isolation signal for the MSIVs (in Group 1A) when 1oo1 votes for a manual initiation is received.	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
N4S-FR-115	A manual isolation of the MSIVs (in Group 1) shall require an isolation signal from Division 3 **AND** an isolation signal from Division 2.	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
N4S-FR-116	Division 3 shall provide a manual isolation signal for the MSIVs (in Group 1A) when 1oo1 votes for a manual initiation is received.	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
N4S-FR-117	Division 2 shall provide a manual isolation signal for the MSIVs (in Group 1A) when 1oo1 votes for a manual initiation is received.	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-118	Division 1 shall provide an isolation signal when 1oo1 isolate vote for a manual initiation is received that closes all of the valves ("inboard") in the following groups: • Group IA • Group IB • Group IIA • Group IIB • Group III • Group VIA • Group VIB • Group VIC • Group VIIIA • Group VIIIB	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
N4S-FR-119	Division 1 shall provide annunciation for N4S MANUAL ISOLATION via the HMI when 1oo1 annunciate votes are received for the second distinct action is satisfied.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-120	Division 3 shall provide a isolation signal when 1oo1 isolate vote for a manual initiation is received that closes all of the valves ("inboard") in the following groups: • Group IA • Group VIC • Group VIIA	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
N4S-FR-121	Division 3 shall provide annunciation for N4S MANUAL ISOLATION via the HMI when 1oo1 annunciate votes are received for the second distinct action is satisfied.	IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-122	Division 2 shall provide a isolation signal when 1oo1 isolate vote for a manual initiation is received that closes all of the valves ("outboard") in the following groups: • Group IA • Group VIC	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
N4S-FR-123	Division 2 shall provide annunciation for N4S MANUAL ISOLATION via the HMI when 1oo1 annunciate votes are received for the second distinct action is satisfied.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-124	Division 4 shall provide a isolation signal when 1oo1 isolate vote for a manual initiation is received that closes all of the valves ("outboard") in the following groups: • Group IA • Group IB • Group IIA • Group IIB • Group III • Group VIA • Group VIB • Group VIC • Group VIIA • Group VIIB • Group VIIIA • Group VIIIB	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-125	Division 4 shall provide annunciation for N4S MANUAL ISOLATION via the HMI when 1oo1 annunciate votes are received for the second distinct action is satisfied.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-126	Division 1 shall have the capability via HMI soft controls to initiate a limited manual isolation that provides an output to close all of the valves ("inboard") in the following group: • Group VIA • Group VIB • Group VIIIB	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
N4S-FR-127	Division 4 shall have the capability via HMI soft controls to initiate a limited manual isolation that provides an output to close all of the valves ("outboard") in the following groups: • Group VIA • Group VIB • Group VIIB • Group VIIIB	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
N4S-FR-128	Division 1 shall provide a means to manually reset the logic associated with the limited manual isolation.	Original design feature	
N4S-FR-129	Division 4 shall provide a means to manually reset the logic associated with the limited manual isolation.	Original design feature	
N4S-FR-130	Each channel shall provide a vote to allow bypass to each division when CI1 is satisfied (contact open).	Original design feature	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-131	Each division shall allow manual bypass via the HMI of the channel isolate votes for the CV input when 2oo4 votes for CI1 bypass input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-132	Each division shall provide annunciation for MAIN CONDENSER LO VACUUM BYPASS via the HMI when the manual bypass of CV input is executed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-133	Each channel shall bypass the MSLP input when CI17 is satisfied (contact closed).	Original design feature	
N4S-FR-134	Each channel shall provide a vote to isolate to each division when RWL2 exceeds setpoint low.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-135	Each division shall provide annunciation for REACTOR WATER BELOW LEVEL 2 TRIP via the HMI when 2oo4 isolate votes for RWL2 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-136	Each division shall provide annunciation for STEAM TUNNEL HI TEMP via the HMI and transmit computer data to the non-SR DCS platform when 2oo4 isolate votes for MSLAT1 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-137	Each channel shall provide a vote to isolate to each of the divisions when any of the four (4) MSLF inputs exceeds setpoint high.	Project design approach	
N4S-FR-138	Each division shall provide annunciation for STEAM LINE HI FLOW via the HMI and transmit computer data to the non-SR DCS platform when 2oo4 isolate votes for MSLF input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-139	Each channel shall provide a vote to isolate to each of the divisions when MSLP input exceeds setpoint low.	Project design approach	
N4S-FR-140	Each division shall provide annunciation for MAIN STEAM LINE LO PRESS via the HMI when 2oo4 isolate votes for MSLP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-141	Each channel shall provide a vote to isolate to each of the divisions when CV input exceeds setpoint low.	Project design approach	
N4S-FR-142	Each division shall provide annunciation for MAIN CONDENSER LO VACUUM via the HMI when 2oo4 isolate votes for CV input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-143	Each channel shall provide a vote to isolate to each of the divisions when RVP input exceeds setpoint low.	Project design approach	
	Group IA Isolation		
N4S-FR-144	Each division shall provide a Group IA isolation signal when 2oo4 isolate votes for MSLAT1 input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-145	Each division shall provide a Group IA isolation signal when 2oo4 isolate votes for RWL1 input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-146	Each division shall provide a Group IA isolation signal when 2oo4 isolate votes for MSLF input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-147	Each division shall provide a Group IA isolation signal when 2oo4 isolate votes for MSLP input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-148	Each division shall provide a Group IA isolation signal when 2oo4 isolate votes for CV input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-149	Each division shall provide annunciation for N4S MSIV INITIATED and indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when a Group IA isolation signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-150	Division 1 shall provide a Group IA isolation output that de-energizes the 120 VAC pilot solenoid for the following MSIVs: • B21-F022A • B21-F022B • B21-F022C • B21-F022D	Original design feature	
N4S-FR-151	Division 1 shall provide indicator and indicating light capability via the HMI for monitoring the 120VAC pilot solenoid for the following MSIVs: • B21-F022A • B21-F022B • B21-F022C • B21-F022D	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-152	Division 1 shall provide a Group IA isolation output that de-energizes the 125 VDC pilot solenoid for the following MSIVs: • B21-F028A • B21-F028B • B21-F028C • B21-F028D	IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-153	Division 1 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform based on 125VDC limit switch contact inputs for the following MSIVs: • B21-F028A • B21-F028B • B21-F028C • B21-F028D	Original design feature	
N4S-FR-154	Division 1 shall provide indicating light and indicator capability via the HMI and transmit computer data to the non-SR DCS platform for monitoring the 125VDC pilot solenoid for the following MSIVs: • B21-F028A • B21-F028B • B21-F028C • B21-F028D	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-155	Division 2 shall provide a Group IA isolation output that de-energizes the 125 VDC pilot solenoid for the following MSIVs: • B21-F022A • B21-F022B • B21-F022C • B21-F022D	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-156	Division 2 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform based on 125VDC limit switch contact inputs for the following MSIVs: • B21-F022A • B21-F022B • B21-F022C • B21-F022D	Original design feature	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-157	Division 2 shall provide indicating light and indicator capability via the HMI and transmit computer data to the non-SR DCS platform for monitoring the 125VDC pilot solenoid for the following MSIVs: • B21-F022A • B21-F022B • B21-F022C • B21-F022D	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-158	Division 2 shall provide a Group IA isolation output that de-energizes the 120 VAC pilot solenoid for the following MSIVs: • B21-F028A • B21-F028B • B21-F028C • B21-F028D	Original design feature	
N4S-FR-159	Division 2 shall provide indicating light and indicator capability via the HMI for monitoring the 120VAC pilot solenoid for the following MSIVs: • B21-F028A • B21-F028B • B21-F028C • B21-F028D	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-160	Division 3 shall provide a Group IA isolation output that de-energizes the 120 VAC pilot solenoid for the following MSIVs: • B21-F022A • B21-F022B • B21-F022C • B21-F022D	Original design feature	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-161	Division 3 shall provide indicator and indicating light capability via the HMI for monitoring the 120VAC pilot solenoid for the following MSIVs: • B21-F022A • B21-F022B • B21-F022C • B21-F022D	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-162	Division 3 shall provide a Group IA isolation output that de-energizes the 125 VDC pilot solenoid for the following MSIVs: • B21-F028A • B21-F028B • B21-F028C • B21-F028D	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-163	Division 3 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform based on 125VDC limit switch contact inputs for the following MSIVs: • B21-F028A • B21-F028B • B21-F028C • B21-F028D	Original design feature	
N4S-FR-164	Division 3 shall provide indicating light and indicator capability via the HMI and transmit computer data to the non-SR DCS platform for monitoring the 125VDC pilot solenoid for the following MSIVs: • B21-F028A • B21-F028B • B21-F028C • B21-F028D	IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-165	Division 4 shall provide a Group IA isolation output that de-energizes the 125 VDC pilot solenoid for the following MSIVs: • B21-F022A • B21-F022B • B21-F022C • B21-F022D	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-166	Division 4 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform based on 125VDC limit switch contact inputs for the following MSIVs: • B21-F022A • B21-F022B • B21-F022C • B21-F022D	Original design feature	
N4S-FR-167	Division 4 shall provide indicating light and indicator capability via the HMI and transmit computer data to the non-SR DCS platform for monitoring the 125VDC pilot solenoid for the following MSIVs: • B21-F022A • B21-F022B • B21-F022C • B21-F022D	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-168	Division 4 shall provide a Group IA isolation output that de-energizes the 120 VAC pilot solenoid for the following MSIVs: • B21-F028A • B21-F028B • B21-F028C • B21-F028D	Original design feature	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-169	Division 4 shall provide indicating light and indicator capability via the HMI for monitoring the 120VAC pilot solenoid for the following MSIVs: • B21-F028A • B21-F028B • B21-F028C • B21-F028D	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-170	Each division shall provide a means to manually test the function of each of the following valves and associated valve position indication capability via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches. • B21-F022A • B21-F022B • B21-F022C • B21-F022D • B21-F028A • B21-F028B • B21-F028C • B21-F028D	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-171	A Group 1A isolation output from both Division 1 **AND** Division 2 shall be required to close valve B21-F016.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-172	Division 1 **AND** Division 2 shall provide indicating light capability via the HMI when the isolation output to valve B21-F016 is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-173	Division 1 shall provide a means to manually open or close valve B21-F016 From the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-174	Division 1 shall provide valve B21-F016 position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-175	A Group 1A isolation output from both Division 3 **AND** Division 4 shall be required to close valve B21-F019.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-176	Division 3 **AND** Division 4 shall provide indicating light capability via the HMI when the isolation output to valve B21-F019 is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-177	Division 4 shall provide a means to manually introduce a momentary signal to open or close valve B21-F019 or terminate valve motion midstream from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-178	Division 4 shall provide valve B21-F019 position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
	Group IB Isolation		
N4S-FR-179	Division 1 shall provide a Group IB isolation signal when 2oo4 isolate votes for RWL2 Input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-180	The Division 1 Group IB isolation signal shall de-energize the 120VAC solenoids to close valves B32-F019 and B21-F084.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-181	Division 1 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when a Group IB isolation signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-182	Division 1 shall provide a means to manually open or close valve B32-F019 from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-183	Division 1 shall provide valve B32-F019 position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-184	Division 1 shall provide a means to manually open or close valve B21-F084 from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-185	Division 1 shall provide valve B21-F084 position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-186	Division 4 shall provide a Group IB isolation signal when 2oo4 isolate votes for RWL2 Input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-187	The Division 4 Group IB isolation signal shall de-energize the 120VAC solenoids to close valves B32-F020 and B21-F085.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-188	Division 4 shall provide a means to manually open or close valve B32-F020 from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-189	Division 4 shall provide valve B32-F020 position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-190	Division 4 shall provide a means to manually open or close valve B21-F085 from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-191	Division 4 shall provide valve B21-F085 position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-192	Division 4 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when a Group IB isolation signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-193	Channel A shall provide a vote to trip to each of the divisions when CI2 is satisfied (contact open).	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-194	Channel B shall provide a vote to trip to each of the divisions when CI2 is satisfied (contact open).	Project design approach	
N4S-FR-195	Division 1 shall provide a Group IB isolation signal when 1oo2 trip votes for CI2 input are received to isolate the Condenser Off Gas Mechanical Vacuum Pump Line.	GDC 60	
N4S-FR-196	Division 2 shall provide a Group IB isolation signal when 1oo2 trip votes for CI2 input are received to isolate the Condenser Off Gas Mechanical Vacuum Pump Line.	GDC 60	
	Group IIA Isolation		
N4S-FR-197	Each channel shall provide a vote to isolate to each of the divisions when RWL3 input exceeds setpoint low.	Project design approach	
N4S-FR-198	Division 1 shall provide a Group IIA isolation signal when 2oo4 isolate votes for RWL3 input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-199	Division 1 shall provide a Group IIA isolation signal when 2oo4 isolate votes for RVP input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-200	A Group IIA isolation signal from Division 1 shall be close the following valves: • E11-F009 • E11-F050A • HV51-1(2)51A • E11-F050B • HV51-1(2)151B	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-201	Division 1 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when the Group IIA isolation is provided.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-202	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E11-F009 or terminate valve motion midstream from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-203	Division 1 shall provide interlocks that prohibit valve E11-F009 from being manually opened if a Group IIA isolation signal is present.	Original design feature	
N4S-FR-204	Division 1 shall provide valve E11-F009 position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-205	Division 4 shall provide a Group IIA isolation signal when 2oo4 isolate votes for RWL3 input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-206	Division 4 shall provide a Group IIA isolation signal when 2oo4 isolate votes for RVP input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-207	A Group IIA isolation signal from Division 4 shall close the following valves: • E11-F008 • E11-F015A • E11-F015B	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-208	Division 4 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when the Group IIA isolation is provided.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-209	Division 4 shall provide a means to manually introduce a momentary signal to open or close valve E11-F008 or terminate valve motion midstream from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-210	Division 4 shall provide valve E11-F008 position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-211	Division 4 shall provide a means to manually introduce a momentary signal to open or close valve E11-F015A or terminate valve motion midstream from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-212	Division 4 shall provide valve E11-F015A position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-213	Division 4 shall provide a means to manually introduce a momentary signal to open or close valve E11-F015B or terminate valve motion midstream from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-214	Division 4 shall provide valve E11-F015B position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
	Group IIB Isolation		
N4S-FR-215	Each channel shall provide a vote to isolate to each of the divisions when DP input exceeds setpoint low.	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-216	Division 1 shall provide a Group IIB isolation signal when 2oo4 isolate votes for RWL3 input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 34, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-217	Division 1 shall provide a Group IIB isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 34, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-218	A Group IIB isolation signal from Division 1 shall close the following valves: • E11-F040 • E11-F079A • E11-F079B	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 34, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-219	Division 1 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when the Group IIB isolation is provided.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-220	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E11-F040 or terminate valve motion midstream from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-221	Division 1 shall provide valve E11-F040 position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-222	Division 1 shall provide a means to manually open or close valve E11-F079A from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-223	Division 1 shall provide valve E11-F079A position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-224	Division 1 shall provide a means to manually open or close valve E11-F079B from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-225	Division 1 shall provide valve E11-F079B position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-226	Division 4 shall provide a Group IIB isolation signal when 2oo4 isolate votes for RWL3 input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 34, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-227	Division 4 shall provide a Group IIB isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 34, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-228	A Group IIB isolation signal from Division 4 shall close the following valves: • E11-F049 • E11-F080A • E11-F080B	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 34, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-229	Division 4 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when the Group IIB isolation is provided.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-230	Division 4 shall provide a means to manually introduce a momentary signal to open or close valve E11-F049 or terminate valve motion midstream from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-231	Division 4 shall provide valve E11-F049 position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-232	Division 4 shall provide a means to manually open or close valve E11-F080A from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-233	Division 4 shall provide valve E11-F080A position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-234	Division 4 shall provide a means to manually open or close valve E11-F080B from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-235	Division 4 shall provide valve E11-F080B position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
	Group III Isolation		
N4S-FR-236	Channel A shall provide a vote to isolate to each of the divisions when CI3 is satisfied (contact open).	Project design approach	
N4S-FR-237	Channel D shall provide a vote to isolate to each of the divisions when CI3 is satisfied (contact open).	Project design approach	
N4S-FR-238	Channel D shall provide a vote to isolate to each of the divisions when CI6 is satisfied (contact open).	Project design approach	
N4S-FR-239	Channel A shall provide a vote to annunciate to each of the divisions when CI13 is satisfied (contact closed).	Project design approach	
N4S-FR-240	Channel D shall provide a vote to annunciate to each of the divisions when CI14 is satisfied (contact closed).	Project design approach	
N4S-FR-241	Channel A shall provide a vote to isolate to each of the divisions when CI15 is satisfied (contact closed).	Project design approach	
N4S-FR-242	Channel D shall provide a vote to isolate to each of the divisions when CI16 is satisfied (contact closed).	Project design approach	
N4S-FR-243	Division 1 shall provide a Group III isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-244	Division 1 shall provide a Group III isolation signal when 1oo2 isolate votes for CI3 input are received.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-245	Division 1 shall provide a Group III isolation signal when 1oo2 isolate votes for RWAT/RWDT input are received.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-246	Division 1 shall provide a Group III isolation signal when 1oo2 isolate votes for DFS input are received.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-247	A Group III isolation signal from Division 1 shall close valve G31-F001.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-248	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve G31-F001 or terminate valve motion midstream from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-249	Division 1 shall provide valve G31-F001 position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-250	Division 1 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when the Group III isolation is provided.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-251	Division 1 shall provide annunciation for RWCU SYSTEM ISOLATED via the HMI when 1oo1 annunciate votes CI13 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-252	Division 1 shall provide three (3) outputs to the RWCU system when 1oo1 isolate votes for CI15 input is received.	Original design feature	
N4S-FR-253	Division 4 shall provide a Group III isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-254	Division 4 shall provide a Group III isolation signal when 1oo2 isolate votes for CI3 input are received.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-255	Division 4 shall provide a Group III isolation signal when 1oo2 isolate votes for RWAT/RWDT input are received.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-256	Division 4 shall provide a Group III isolation signal when 1oo2 isolate votes for DFS input are received.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-257	Division 4 shall provide a Group III isolation signal when 1oo1 isolate votes for CI6 input are received.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-258	A Group III isolation signal from Division 4 shall close valve G31-F004.	GDC 21, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-259	Division 4 shall provide annunciation for RWCU FILTER INLET HI TEMP ISOLATION via the HMI when 1oo1 isolate votes for CI6 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-260	Division 4 shall provide a means to manually introduce a momentary signal to open or close valve G31-F004 or terminate valve motion midstream from the control room.	GDC 21, IEEE Std. 338, Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-261	Division 4 shall provide valve G31-F004 position indication capability via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-262	Division 4 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when the Group III isolation is provided.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-263	Division 4 shall provide annunciation for RWCU SYSTEM ISOLATED via the HMI when 1oo1 annunciate votes for CI14 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-264	Division 4 shall provide three (3) outputs to the RWCU system when 1oo1 isolate votes for CI16 input is received.	Original design feature	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
	Group VIA Isolation		
N4S-FR-265	Each channel shall provide a vote to isolate to each of the divisions when CI10 is satisfied (contact open).	Project design approach	
N4S-FR-266	Each channel shall provide a vote to isolate to each of the divisions when CI11 is satisfied (contact open).	Project design approach	
N4S-FR-267	Division 1 shall provide a Group VIA isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-268	Division 1 shall provide a Group VIA isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-269	Division 1 shall provide a Group VIA isolation signal when 2oo4 isolate votes for CI10 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-270	Division 1 shall provide a Group VIA isolation signal when 2oo4 isolate votes for CI11 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-271	A Group VIA isolation signal from Division 1 shall close the following valves: • HV-57-121 / -221 • HV-57-131 / -231 • HV-57-123 / -223 • HV-57-124 / -224 • HV-57-115 / -215 • HV-57-112 / -212	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-272	Division 4 shall provide a Group VIA isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-273	Division 4 shall provide a Group VIA isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-274	Division 4 shall provide a Group VIA isolation signal when 2oo4 isolate votes for CI10 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-275	Division 4 shall provide a Group VIA isolation signal when 2oo4 isolate votes for CI11 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-276	A Group VIA isolation signal from Division 4 shall close the following valves: • HV-57-109 / -209 • HV-57-135 / -235 • HV-57-147 / -247 • HV-57-114 / -214 • HV-57-104 / -204	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
	Group VIB Isolation		
N4S-FR-277	Division 1 shall provide a Group VIB isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-278	Division 1 shall provide a Group VIB isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-279	Division 1 shall provide a Group VIB isolation signal when 2oo4 isolate votes for CI10 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-280	Division 1 shall provide a Group VIB isolation signal when 2oo4 isolate votes for CI11 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-281	A Group VIB isolation signal from Division 1 shall close the following valves: • HV-57-117 / -217 • HV-57-118 / -218 • HV-57-160A / -260A	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-282	Division 4 shall provide a Group VIB isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-283	Division 4 shall provide a Group VIB isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-284	Division 4 shall provide a Group VIB isolation signal when 2oo4 isolate votes for CI10 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-285	Division 4 shall provide a Group VIB isolation signal when 2OO4 isolate votes for CI11 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-286	A Group VIB isolation signal from Division 4 shall close the following valves: • HV-57-111 / -211 • HV-57-105 / -205 • HV-57-160B / -260B	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
	Group VIC Isolation		
N4S-FR-287	Each channel shall provide a vote to isolate to each of the divisions when CI7 is satisfied (contact open).	Project design approach	
N4S-FR-288	Each channel shall provide a vote to isolate to each of the divisions when CI8 is satisfied (contact open).	Project design approach	
N4S-FR-289	Division 1 shall provide a Group VIC isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-290	Division 1 shall provide a Group VIC isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-291	Division 1 shall provide a Group VIC isolation signal when 2oo4 isolate votes for CI7 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-292	Division 1 shall provide a Group VIC isolation signal when 2oo4 isolate votes for CI8 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-293	A Group VIC isolation signal from Division 1 shall close the following valves: • SV-57-133 • SV-57-183 • SV-57-191	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-294	Division 2 shall provide a Group VIC isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-295	Division 2 shall provide a Group VIC isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-296	Division 2 shall provide a Group VIC isolation signal when 2oo4 isolate votes for CI7 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-297	Division 2 shall provide a Group VIC isolation signal when 2oo4 isolate votes for CI8 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-298	A Group VIC isolation signal from Division 2 shall close the following valves: • SV-26-190B • SV-26-190D • SV-57-132 • SV-57-134 • SV-57-150 • SV-57-181	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-299	Division 3 shall provide a Group VIC isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-300	Division 3 shall provide a Group VIC isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-301	Division 3 shall provide a Group VIC isolation signal when 2oo4 isolate votes for CI7 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-302	Division 3 shall provide a Group VIC isolation signal when 2oo4 isolate votes for CI8 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-303	A Group VIC isolation signal from Division 3 shall close the following valves: • HV-57-161 • HV-57-162 • FV-C-DO-101A • HV-57-166 • SV-26-190A • SV-26-190C • SV-57-184 • SV-57-185 • SV-57-186 • SV-57-190 • SV-57-195	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-304	Division 4 shall provide a Group VIC isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-305	Division 4 shall provide a Group VIC isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-306	Division 4 shall provide a Group VIC isolation signal when 2oo4 isolate votes for CI7 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-307	Division 4 shall provide a Group VIC isolation signal when 2oo4 isolate votes for CI8 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-308	A Group VIC isolation signal from Division 4 shall close the following valves: • HV-57-163 • HV-57-164 • FV-C-DO-101B • HV-57-169 • HV-57-116 • SV-57-141 • SV-57-142 • SV-57-143 • SV-57-144 • SV-57-145 • SV-57-159	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
	Group VIIA Isolation		
N4S-FR-309	Division 3 shall provide a Group VIIA isolation signal when 2oo4 isolate votes for RWL1 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-310	Division 3 shall provide a Group VIIA isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-311	Division 3 shall provide a Group VIIA isolation signal when 2oo4 isolate votes for CI7 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-312	A Group VIIA isolation signal from Division 3 shall close the following valves: • HV-59-101 • HV-59-129A	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-313	Division 4 shall provide a Group VIIA isolation signal when 2oo4 isolate votes for RWL1 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-314	Division 4 shall provide a Group VIIA isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-315	Division 4 shall provide a Group VIIA isolation signal when 2oo4 isolate votes for CI7 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-316	A Group VIIA isolation signal from Division 4 shall close the following valves: • HV-59-102 • HV-59-129B • HV-59-135	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
	Group VIIB Isolation		
N4S-FR-317	Division 4 shall provide a Group VIIB isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-318	Division 4 shall provide a Group VIIB isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-319	Division 4 shall provide a Group VIIB isolation signal when 2oo4 isolate votes for CI10 input are received.	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-320	A Group VIIB isolation signal from Division 4 shall close the following valves: • HV-59-131	GDC 13, GDC 19, GDC 20, GDC 21, GDC 22, GDC 29, GDC 54, GDC 55, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
	Group VIIIA Isolation		
N4S-FR-321	Division 1 shall provide a Group VIIIA isolation signal when 2oo4 isolate votes for RWL1 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-322	Division 1 shall provide a Group VIIIA isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-323	A Group VIIIA isolation signal from Division 1 shall close the following valves: • HV-87-120A • HV-87-121A • HV-87-120B • HV-87-121B • HV-13-106 • HV-13-107	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-324	Division 4 shall provide a Group VIIIA isolation signal when 2oo4 isolate votes for RWL1 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-325	Division 4 shall provide a Group VIIIA isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-326	A Group VIIIA isolation signal from Division 4 shall close the following valves: • HV-87-128 • HV-87-129 • HV-87-122 • HV-87-123 • HV-13-108 • HV-13-111	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
	Group VIIIB Isolation (Drywell Sump (DS), Suppression Pool Cleanup (SPC), TIP)		
N4S-FR-327	Division 1 shall provide a Group VIIIB (DS/SPC/TIP) isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-328	Division 1 shall provide a Group VIIIB (DS/SPC/TIP) isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-329	A Group VIIIB (DS/SPC/TIP) isolation signal from Division 1 shall close the following valves: • HV-61-110 • HV-61-130 • HV-52-127	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-330	A Group VIIIB (DS/SPC/TIP) isolation signal from Division 1 shall withdraw the TIP.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-331	Division 1 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when a Group VIIIB (DS/SPC/TIP) isolation signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-332	Division 4 shall provide a Group VIIIB (DS/SPC/TIP) isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-333	Division 4 shall provide a Group VIIIB (DS/SPC/TIP) isolation signal when 2oo4 isolate votes for DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-334	A Group VIIIB (DS/SPC/TIP) isolation signal from Division 4 shall close the following valves: • HV-61-111 • HV-61-131 • HV-52-128	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-335	Division 4 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when a Group VIIIB (DS/SPC/TIP) isolation signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
	Group VIIIB Isolation (Bypass Barrier Block and Vents (BBBV))		
N4S-FR-336	Division 4 shall provide a Group VIIIB (BBBV) isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-337	Division 4 shall provide a Group VIIIB (BBBV) isolation signal when 2oo4 isolate votes for DP input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-338	Division 4 shall provide a Group VIIIB (BBBV) isolation signal when 2oo4 isolate votes for CI10 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-339	Division 4 shall provide a Group VIIIB (BBBV) isolation signal when 2oo4 isolate votes for CI11 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-340	A Group VIIIB (BBBV) isolation signal from Division 4 shall close the following valves: • HV-57-165 • HV-57-167 • HV-41-142 • HV-41-143 • HV-46-127 • HV-46-128	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
	Group VIIIB Isolation (PCIG Block and Vents (PCIG))		
N4S-FR-341	Division 4 shall provide a Group VIIIB (PCIG) isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-342	Division 4 shall provide a Group VIIIB (PCIG) isolation signal when 2oo4 isolate votes for DP input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-343	Division 4 shall provide a Group VIIIB (PCIG) isolation signal when 2oo4 isolate votes for CI10 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-344	A Group VIIIB (PCIG) isolation signal from Division 4 shall close the following valves: • HV-59-140 • HV-59-141 • HV-59-142 • HV-59-143	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
	Group VIIIB Isolation (ECCS Process Lines)		
N4S-FR-345	Each channel shall provide a vote to isolate to each of the divisions when RVP input exceeds setpoint low **AND** DP input exceeds setpoint low	Project design approach	
N4S-FR-346	Division 1 shall provide a Group VIIIB (ECCS) isolation signal when 2oo4 isolate votes for RVP/DP input are received.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-347	A Group VIIIB (ECCS) isolation signal from Division 1 shall close the following valves: • HV-52-1F015A • HV-52-1F015B • HV-51-1F027A • HV-51-1F027B • HV-C-51-1F103A • HV-C-51-1F104A	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-348	A Group VIIIB (ECCS) isolation signal from Division 1 shall withdraw the TIP.	GDC 13, GDC 16, GDC 19, GDC 20, GDC 21, GDC 22, GDC 54, GDC 56, GDC 60, 10CFR20, 10CFR50.67, 10CR100, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-349	Division 1 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform when a Group VIIIB (ECCS) isolation signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-350	Division 1 shall provide a Group VIIIB isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	This group of valves is listed in L-S-26 but not specifically in GP-8.1. Need to confirm channels and whether valves are isolated.
N4S-FR-351	Division 1 shall provide a Group VIIIB isolation signal when 2oo4 isolate votes for DP input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-352	Division 1 shall provide a Group VIIIB isolation signal when 2oo4 isolate votes for CI10 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-353	Division 1 shall provide a Group VIIIB isolation signal when 2oo4 isolate votes for CI11 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-354	A Group VIIIB isolation signal from Division 1 shall close the following valves: • HV-76-141 • HV-76-142 • HV-76-157 • HV-76-158 • HV-76-107 • HV-76-108 • HV-76-109 • HV-76-030-1 • HV-76-030-2	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-355	Division 4 shall provide a Group VIIIB isolation signal when 2oo4 isolate votes for RWL2 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	This group of valves is listed in L-S-26 but not specifically in GP-8.1. Need to confirm channels and whether valves are isolated.
N4S-FR-356	Division 4 shall provide a Group VIIIB isolation signal when 2oo4 isolate votes for DP input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-357	Division 4 shall provide a Group VIIIB isolation signal when 2oo4 isolate votes for CI10 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-358	Division 4 shall provide a Group VIIIB isolation signal when 2oo4 isolate votes for CI11 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-359	A Group VIIIB isolation signal from Division 4 shall close the following valves: • HV-76-141 • HV-76-142 • HV-76-157 • HV-76-158 • HV-76-107 • HV-76-108 • HV-76-109 • HV-76-030-1 • HV-76-030-2	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-360	Division 1 shall provide a Group VIIIB isolation signal when 2oo4 isolate votes for CI11 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	This group of valves is listed in L-S-26 but not specifically in GP-8.1. Need to confirm channels and whether valves are isolated.
N4S-FR-361	A Group VIIIB isolation signal from Division 1 shall close the following valves: • HV-76-117 • HV-76-118 • HV-76-167 • HV-76-168	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-362	Division 4 shall provide a Group VIIIB isolation signal when 2oo4 isolate votes for CI11 input are received.	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	This group of valves is listed in L-S-26 but not specifically in GP-8.1. Need to confirm channels and whether valves are isolated.

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-363	A Group VIIIB isolation signal from Division 4 shall close the following valves: • HV-76-117 • HV-76-118 • HV-76-167 • HV-76-168	GDC 21, IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-364	Channel A shall provide a vote to reset to Division 1 when CI19 input is satisfied (contact closed).	Project design approach	
N4S-FR-365	Channel D shall provide a vote to reset to Division 4 when CI18 input is satisfied (contact closed).	Project design approach	
N4S-FR-366	Division 1 shall be capable of being manually reset as long as the trip condition(s) that initiated the trip has cleared **AND** the respective MSIV 120VAC pilot solenoid energized permissive **AND** the respective MSIV 125VDC pilot solenoid energized permissive are satisfied **AND** 1oo1 reset votes from CI19 input are received.	Original design feature	
N4S-FR-367	Division 4 shall be capable of being manually reset as long as the trip condition(s) that initiated the trip has cleared **AND** the respective MSIV 120VAC pilot solenoid energized permissive **AND** the respective MSIV 125VDC pilot solenoid energized permissive are satisfied **AND** 1oo1 reset votes from CI18 input are received.	Original design feature	
N4S-FR-368	Division 1 shall provide a means to manually generate annunciation for N4S ISOLATION SYSTEM OUT OF SERVICE (INBOARD) and status light capability via the HMI.	Reg Guide 1.47 (BISI), IEEE Standard 279	
N4S-FR-369	Channel A shall provide a vote to annunciate to Division 1 when CI12 is satisfied (contact open).	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-370	Channel D shall provide a vote to annunciate to Division 4 when CI12 is satisfied (contact open).	Project design approach	
N4S-FR-371	Division 1 shall provide annunciation for N4S ISOLATION SYSTEM OUT OF SERVICE (INBOARD) and status light capability via the HMI when 1oo1 annunciate votes are received for CI12 input.	Reg Guide 1.47 (BISI), IEEE Standard 279	
N4S-FR-372	Division 1 shall provide annunciation for N4S ISOLATION SYSTEM OUT OF SERVICE (INBOARD) and status light capability via the HMI for any loss of power condition or logic test condition.	Reg Guide 1.47 (BISI), IEEE Standard 279	
N4S-FR-373	Division 4 shall provide means to manually generate annunciation for N4S ISOLATION SYSTEM OUT OF SERVICE (OUTBOARD) and status light capability via the HMI.	Reg Guide 1.47 (BISI), IEEE Standard 279	
N4S-FR-374	Division 4 shall provide annunciation for N4S ISOLATION SYSTEM OUT OF SERVICE (OUTBOARD) and status light capability via the HMI when 1oo1 annunciate votes are received for CI12 input.	Reg Guide 1.47 (BISI), IEEE Standard 279	
N4S-FR-375	Division 4 shall provide annunciation for N4S ISOLATION SYSTEM OUT OF SERVICE (OUTBOARD) and status light capability via the HMI for any loss of power condition or logic test condition.	Reg Guide 1.47 (BISI), IEEE Standard 279	
N4S-FR-376	PPS/N4S shall provide the capability to manually test all channels, divisions and the isolation valves.	GDC 21, GDC 54,. Reg Guide 1.22, Reg Guide 1.62	
N4S-FR-377	PPS/N4S shall provide the means to perform functional tests during normal plant operation.	IEEE Std. 603/IEEE Std. 7-4.3.2	
N4S-FR-378	Each channel and each division shall provide sufficient features and documented evaluations to support elimination of most Technical Specification Surveillance Tests, and minimize the requirements for manual calibration checks.	Project design approach	

N4S FUNCTIONAL REQUIREMENTS			
ID #	**PPS/N4S Requirement**	**PPS/N4S Source / Basis**	**Notes / Clarification**
N4S-FR-379	For all PPS inputs that have the potential to require manual test insertion or external measurement of input values (i.e., use of an external digital multi meter by a technician), test jacks are provided in the cabinets.	Project design approach	
N4S-FR-380	For all inputs that have the potential to require manual multi-point calibration checks with external calibration equipment, knife edge disconnects along with test jacks are incorporated in the field termination panels.	Project design approach	

C

C.1 HPCI Design Requirements

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-1	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. 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. 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.	GDC 1 - Quality standards and records
HPCI-DR-2	Structures, systems, and components important to safety shall be designed to withstand the effect of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions.	GDC 2 - Design Bases for Protection Against Natural Phenomena
HPCI-DR-3	Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions.	GDC 3 - Fire protection
HPCI-DR-4	Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents (LOCAs).	GDC 4 - Environmental and dynamic effects design bases
HPCI-DR-5	The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.	GDC 10 - Reactor design

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-6	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.	GDC 13 - Instrumentation and control
HPCI-DR-7	A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. 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 I&C 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.	GDC 19 - Control Room
HPCI-DR-8	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.	GDC 20 - Protection system functions

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-9	The protection system shall be designed for high functional reliability and in-service 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.	GDC 21 - Protection system reliability and testability
HPCI-DR-10	The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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.	GDC 22- Protection system independence
HPCI-DR-11	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.	GDC 23 - Protection system failure modes
HPCI-DR-12	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.	GDC 24 - Separation of protection and control systems

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-13	The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.	GDC 29 - Protection against anticipated operational occurrences
HPCI-DR-14	A system to supply reactor coolant makeup for protection against small breaks in the reactor coolant pressure boundary shall be provided. The system safety function shall be to assure that specified acceptable fuel design limits are not exceeded as a result of reactor coolant loss due to leakage from the reactor coolant pressure boundary and rupture of small piping or other small components which are part of the boundary. The system shall be designed to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished using the piping, pumps, and valves used to maintain coolant inventory during normal reactor operation.	GDC 33 - Reactor Coolant Makeup
HPCI-DR-15	A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts.	GDC 35 - Emergency Core Cooling
HPCI-DR-16	The emergency core cooling system shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leak tight integrity of its components, (2) the operability and performance of the active components of the system, and (3) the operability of the system as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.	GDC 37 - Testing of Emergency Core Cooling System

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-17	The protection system shall be designed to permit periodic testing of its initiation functions inclusive of the actuation devices and actuated equipment when the reactor is in operation.	Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions (Safety Guide 22)
HPCI-DR-18	Those structures, systems, and components (SSC) that should be designed to remain functional if the Safe Shutdown Earthquake (SSE) occurs shall be designated as Seismic Category I. (This includes Systems or portions of systems that are required for reactor shutdown; all electric and mechanical devices and circuitry between the process and the input terminals of the actuator systems involved in generating signals that initiate protective action; systems or portions of systems that are required for (1) monitoring of systems important to safety and (2) actuation of systems important to safety.)	Regulatory Guide 1.29 - Seismic Design Classification
HPCI-DR-19	The HPCI shall comply with the requirements of Appendix B to 10 CFR Part 50 for the installation, inspection, and testing of nuclear power plant instrumentation and electric equipment.	Regulatory Guide 1.30 - Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment (Safety Guide 30)
HPCI-DR-20	The HPCI shall meet the requirements for design, operation and testing of safety-related power systems within nuclear power plants as defined within IEEE Std. 308.	Regulatory Guide 1.32 - Criteria for Power Systems for Nuclear Power Plants
HPCI-DR-21	The HPCI shall meet the requirements for indicating the bypass or inoperable status of portions of the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the system it actuates to perform their safety-related functions:	Regulatory Guide 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
HPCI-DR-22	The HPCI shall comply with the IEEE Std. 279 requirement that any single failure within the protection system shall not prevent proper protective action at the system level when required, by using the guidance in IEEE Std. 379-1972 for applying the single-failure criterion to the design and analysis of nuclear power plant protection systems.	Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Safety Systems

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-23	The HPCI shall provide a means for manual initiation of protective actions.	Regulatory Guide 1.62 - Manual Initiation of Protective Actions
HPCI-DR-24	The HPCI shall meet the requirements for physical independence of the circuits and electric equipment comprising or associated with the Class 1E power system, the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety related functions.	Regulatory Guide 1.75 - Physical Independence of Electric Systems
HPCI-DR-25	The HPCI shall comply with design verification requirements to verify adequacy of design under the most adverse design conditions.	Regulatory Guide 1.89 - Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants
HPCI-DR-26	The HPCI shall comply with the requirement to: (1) provide information required to permit the operator to take preplanned manual actions to accomplish safe plant shutdown; (2) determine whether the reactor trip, engineered safety feature systems, and manually initiated safety systems and other systems important to safety are performing their intended functions (i.e., reactivity control, core cooling, maintaining reactor coolant system integrity, and maintaining containment integrity); (3) provide information to the operators that will enable them to determine the potential for causing a gross breach of the" barriers to radioactivity release (i.e., fuel cladding, reactor coolant pressure boundary, and containment) and to determine if a gross breach of a barrier has occurred.	Regulatory Guide 1.97 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants
HPCI-DR-27	The HPCI shall comply with design verification requirements to verify the seismic adequacy of electric equipment.	Regulatory Guide 1.100 - Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-28	The HPCI shall design shall implement setpoints that assure sufficient margin between Technical Specification limits and the trip setpoint to account for instrument inaccuracy, calibration uncertainties and instrument drift. Consideration of instrument span and range as well as environmental influences must be included.	Regulatory Guide 1.105 - Instrument Setpoint
HPCI-DR-29	The HPCI shall comply with the requirements for periodic testing of electric power and protection systems.	Regulatory Guide 1.118 - Periodic Testing of Electric Power and Protection Systems
HPCI-DR-30	The HPCI shall, with precision and reliability, initiate the startup of a steam driven turbine pump and alignment of valves to support a flow injection pathway to the reactor vessel.	IEEE Std. 603, Section 5.0 Safety System Criteria and 6.1 Automatic Control
HPCI-DR-31	The HPCI shall initiate when the monitored plant parameter exceeds the following trip setpoint: Reactor Vessel Water Level 2 < -38 inches Drywell Pressure > 1.68 psig	IEEE Std. 603, Section 6.1 Automatic Control
HPCI-DR-32	The HPCI signal input to actuation output propagation time shall be less than 100 milliseconds.	IEEE Std. 603, Section 4.10
HPCI-DR-33	The HPCI shall be capable of initiating under all required modes of reactor operation.	IEEE Std. 603, Section 4.1
HPCI-DR-34	The HPCI shall ensure that the protective action, once started, continues to completion.	IEEE Std. 603, Section 5.2 Completion of Protective Action
HPCI-DR-35	HPCI shall not be required to be single failure proof, but should be designed to provide the highest degree of protective action at the system level when required.	IEEE Std. 603, Section 5.1 Single Failure Criterion and IEEE Std. 7-4.3.2 Section 5.1 Single Failure Criterion

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-36	Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.	IEEE Std. 603 section 5.3 Quality and IEEE Std. 7-4.3.2 section 5.3 Quality
HPCI-DR-37	Type test data or reasonable engineering extrapolation based on test data shall be available to verify that protection system equipment shall meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements.	IEEE Std. 603 section 5.4 Equipment Qualification and IEEE Std. 7-4.3.2 section 5.4 Equipment Qualification
HPCI-DR-38	All protection system channels shall be designed to maintain necessary functional capability under extremes of conditions (as applicable) relating to environment, energy supply, malfunctions and accidents.	IEEE Std. 603 section 5.5 System Integrity and IEEE Std. 7-4.3.2 and section 5.5 Independence
HPCI-DR-39	Channels that provide signals for the same protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 System Integrity
HPCI-DR-40	Any equipment that is used for both protective and control functions shall be classified as part of the protection system and shall meet all the applicable requirements.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence
HPCI-DR-41	The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system and shall meet all the applicable requirements. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-42	Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
HPCI-DR-43	Provisions shall be included so that the protective action can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
HPCI-DR-44	Where a credible single event can cause a control system action that results in a condition requiring protective action and can concurrently prevent the protective action from those protection system channels designated to provide principal protection against the condition, then alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design bases.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
HPCI-DR-45	To the extent feasible and practical, protection system inputs shall be derived from signals that are direct measures of the desired variables.	IEEE Std. 603 section 6.4 Derivation of System Inputs
HPCI-DR-46	Means shall be provided for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
HPCI-DR-47	Capability shall be provided for testing and calibrating channels and the devices used to derive the final system output signal from the various channel signals.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
HPCI-DR-48	For those parts of the system where the required interval between testing will be less than the normal time interval between generating station shutdowns, there shall be capability for testing during power operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-49	The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective action at the systems level.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
HPCI-DR-50	During such operation, the active parts of the system shall of themselves continue to meet the single failure criterion.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
HPCI-DR-51	Where operating requirements necessitate automatic or manual bypass of a protective function, the design shall be such that the bypass will be removed automatically whenever permissive conditions are not met.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
HPCI-DR-52	Devices used to achieve automatic removal of the bypass of a protective function are part of the protection system and shall be designed in accordance with these criteria.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
HPCI-DR-53	If the protective action of some part of the system has been bypassed or deliberately rendered inoperative for any purpose, this fact shall be continuously indicated in the control room.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
HPCI-DR-54	The design shall permit the administrative control of the means for manually bypassing channels or protective functions.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
HPCI-DR-55	Where it is necessary to change to a more restrictive set point to provide adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of assuring that the more restrictive set point is used.	IEEE Std. 603 section 6.8 Setpoints
HPCI-DR-56	The devices used to prevent improper use of less restrictive set points shall be considered a part of the protection system and shall be designed in accordance with the other provisions of these criteria regarding performance and reliability.	IEEE Std. 603 section 6.8 Setpoints
HPCI-DR-57	The protection system shall be so designed that, once initiated, a protective action at the system level shall go to completion.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-58	Return to operation shall require subsequent deliberate operator action.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action
HPCI-DR-59	The protection system shall include means for manual initiation of each protective action at the system level (for example, reactor trip, containment isolation, safety injection, core spray, etc).	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
HPCI-DR-60	No single failure within the manual, automatic, or common portions of the protection system shall prevent initiation of protective action by manual or automatic means.	IEEE Std. 603 section 7.2 Manual Control
HPCI-DR-61	Manual initiation should depend upon the operation of a minimum of equipment.	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
HPCI-DR-62	The design shall permit the administrative control of access to all set point adjustments, module calibration adjustments, and test points.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
HPCI-DR-63	Protective actions shall be indicated and identified down to the channel level.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
HPCI-DR-64	The protection system shall be designed to provide the operator with accurate, complete, and timely information pertinent to its own status and to generating station safety.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
HPCI-DR-65	The design shall minimize the development of conditions which would cause meters, annunciators, recorders, alarms, etc, to give anomalous indications confusing to the operator.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
HPCI-DR-66	The system shall be designed to facilitate the recognition, location, replacement, repair, and adjustment of malfunctioning components or modules.	IEEE Std. 603 section 5.10 Repair

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-67	In order to provide assurance that the requirements given in this document can be applied during the design, construction, maintenance, and operation of the plant, the protection system equipment (for example, interconnecting wiring, components, modules, etc), shall be identified distinctively as being in the protection system.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
HPCI-DR-68	This identification shall distinguish between redundant portions of the protection system. (In the installed equipment, components, or modules mounted in assemblies that are clearly identified as being in the protection system do not themselves require identification.) All software, firmware, and programmable logic shall be identified in accordance with IEEE Std. 7-4.3.2 Clause 5.11.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
HPCI-DR-69	HPCI shall conform to the design criteria and features for Class 1E electric systems to ensure that functional requirements under the conditions produced by design basis events are met.	IEEE Std. 308 - Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations
HPCI-DR-70	HPCI shall conform to the methods for demonstrating the qualification of Class 1E equipment including components or equipment of any interface whose failure could adversely affect the performance of Class 1E systems and electronic equipment.	IEEE Std. 323 - Qualifying Class 1E Equipment for Nuclear Power Generating Stations
HPCI-DR-71	HPCI shall conform to the design and operational criteria for the performance of periodic testing of nuclear power generating station safety systems.	IEEE Std. 338 - Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems
HPCI-DR-72	HPCI shall meet its Class 1E performance requirements during and following one SSE (safe shutdown earthquake) preceeded by a number of OBEs (operating basis earthquakes).	IEEE Std. 344 - Guide for Seismic Qualification of Class 1 Electric Equipment for Nuclear Power Generating Stations
HPCI-DR-73	HPCI shall meet the single failure criterion as described and classified in IEEE Std. 379.	IEEE Std. 379 - Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

HPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
HPCI-DR-74	HPCI shall meet the criteria and requirements for establishing and maintaining the independence of Class 1E equipment and circuits and auxiliary supporting features by physical separation and electrical isolation.	IEEE Std. 384 - Criteria for Independence of Class 1E Equipment and Circuits

C.2 HPCI Functional Requirements

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-1	PPS/HPCI shall be capable of providing signals to start the steam turbine pump and align valves for delivering water to the reactor as well as to initiate other SR equipment either automatically when any of the monitored parameters exceeds a pre-established value, or by manual initiation.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-2	PPS/HPCI shall be comprised of two (2) independent and separate divisions (Division 2 and Division 4) to perform the following: • Initiate a HPCI turbine pump start • Provide HPCI turbine flow Control • Trip the HPCI turbine • Isolate the HPCI turbine	GDC 22, Reg Guide 1.62	
HPCI-FR-4	PPS/HPCI shall have four (4) independent channels (Channel A, Channel B, Channel C and Channel D) that each provide votes / signals to each of the divisions.	Reg Guide 1.53	The four channels are common to both divisions.
HPCI-FR-5	PPS/HPCI shall be capable of being powered by 125VDC power.	Original design feature	
HPCI-FR-6	Each division shall provide outputs that are capable of interfacing with 125VDC loads.	Original design feature	
HPCI-FR-7	Each channel shall receive an input from each of the following monitored parameters that are provided as common inputs to the PPS platform and are shared by each of the PPS functions: • Reactor Vessel Water Level 2 (Low) (RWL2) • Reactor Vessel Water Level 8 (High) (RWL8) • Drywell High Pressure (DHP) • Reactor Vessel Pressure (RVP)	IEEE Std. 603/IEEE Std. 7-4.3.2	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-8	Each channel shall receive an input from each of the following monitored parameters (4-20 mA sensor): • Steam Line Pressure (SLP) • Rupture Diaphragm High Pressure (RDHP)	Original design feature	
HPCI-FR-9	Channel B and Channel D shall receive a 4-20 mA input from each of the following monitored parameters: • Condensate Storage Tank Level (CSTL) • Suppression Chamber Level (SCL) • HPCI Turbine Exhaust Pressure (HTEP) • HPCI Steam Flow (HSF) (forward and reverse)	Original design feature	
HPCI-FR-10	Channel B shall receive a 4-20 mA input from each of the following monitored parameters: • HPCI Pump Discharge Pressure (HPDP) • HPCI Pump Flow 1 (HPF1) • HPCI Pump Flow 2 (HPF2) • HPCI Turbine Steam Supply Pressure (HTSSP) • HPCI Pump Suction Pressure (HPSP1) • HPCI Pump Suction Pressure (HPSP2)	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-11	Channel B shall receive the following contact inputs: • E41-F072 LS9 (CI1) • E41-F001 LS13 (CI2) • Turbine stop valve LS4 (CI3) • E41-F041 LS2 (CI4) • E41-F042 LS2 (CI5) • E41-F072 LS10 (CI6) • E51-F029 LS2 (CI7) (RCIC valve) • E51-F031 LS2 (CI8) (RCIC valve) • E41-F006 LS16 (CI9) • E41-F006 LS13 (CI10) • Barometric Condenser Vacuum Tank PP Start H1/H2 (CI11) • E41-F003 LS11 (CI13) • E41-F100 LS15 (CI14) • E41-N014 LSH (CI15) • E41-F003 74 (CI17) • E41-F072 74 (CI18) • E41-F072 LS11 (CI19) • AOP 49X (CI24) • E41-F001 LS15 (CI25) • Turbine bearing oil pressure PSL (CI26)	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-12	Channel B shall receive the following contact inputs (cont'd): • Vacuum tank vacuum PSH (CI27) • HPCI oil temperature TS DT-1 (CI28) • HPCI oil filter high diff pressure DPI (CI29) • HPCI oil tank level LSL/LSH (CI30) • Vacuum tank condensate pump / BCVP 49X (CI31) • Vacuum Tank level LSH56-120 H1/H2 (CI32) • E41-F093 LS11 (CI33) • Associated HPCI valve motor overcurrent (CI35) • Vacuum tank level LSL56-121 LSL (CI37)	Original design feature	
HPCI-FR-13	Channel D shall receive the following contact inputs: • E41-F002 LS11 (CI12) • E41-F002 74 (CI16) • E41-F095 LS11 (CI34) • Associated HPCI valve motor overcurrent (CI36)	Original design feature	
HPCI-FR-14	Channels B and D shall receive the following inputs from PPS/N4S: • HPCI area temperatures (isolate) (DI1)	Original design feature	
HPCI-FR-15	Channel B shall provide a vote to close to each division when CI1 is satisfied (contact closed)	Project design approach	
HPCI-FR-16	Channel B shall provide a condition vote to each division when CI2 is satisfied (contact open)	Project design approach	
HPCI-FR-17	Channel B shall provide a condition vote to each division when CI3 is satisfied (contact closed)	Project design approach	
HPCI-FR-18	Channel B shall provide a condition vote to each division when CI4 is satisfied (contact open)	Project design approach	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-19	Channel B shall provide a condition vote to each division when CI5 is satisfied (contact closed)	Project design approach	
HPCI-FR-20	Channel B shall provide a condition vote to each division when CI6 is satisfied (contact closed)	Project design approach	
HPCI-FR-21	Channel B shall provide a condition vote to each division when CI7 is satisfied (contact closed)	Project design approach	
HPCI-FR-22	Channel B shall provide a condition vote to each division when CI8 is satisfied (contact closed)	Project design approach	
HPCI-FR-23	Channel B shall provide a condition vote to each division when CI9 is satisfied (contact closed)	Project design approach	
HPCI-FR-24	Channel B shall provide a condition vote to each division when CI10 is satisfied (contact closed)	Project design approach	
HPCI-FR-25	Channel B shall provide a condition vote to each division when CI11 is satisfied (contact closed)	Project design approach	
HPCI-FR-26	Channel D shall provide an annunciate vote to each division when CI12 is satisfied (contact closed)	Project design approach	
HPCI-FR-27	Channel B shall provide an annunciate vote to each division when CI13 is satisfied (contact closed)	Project design approach	
HPCI-FR-28	Channel B shall provide an annunciate vote to each division when CI14 is satisfied (contact closed)	Project design approach	
HPCI-FR-29	Channel B shall provide an open vote to each division when CI15 is satisfied (contact closed)	Project design approach	
HPCI-FR-30	Channel B shall provide an annunciate vote to each division when CI15 is satisfied (contact closed)	Project design approach	
HPCI-FR-31	Channel D shall provide an annunciate vote to each division when CI16 is satisfied (contact closed)	Project design approach	
HPCI-FR-32	Channel B shall provide an annunciate vote to each division when CI17 is satisfied (contact closed)	Project design approach	
HPCI-FR-33	Channel B shall provide an annunciate vote to each division when CI18 is satisfied (contact closed)	Project design approach	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-34	Channel B shall provide an annunciate vote to each division when CI19 is satisfied (contact closed)	Project design approach	
HPCI-FR-35	Channel B shall provide a vote to annunciate to each division when CI24 is satisfied (contact closed).	Project design approach	
HPCI-FR-36	Channel B shall provide an annunciate vote to each division when CI25 is satisfied (contact closed) after a 15 second time delay	Project design approach	
HPCI-FR-37	Channel B shall provide a annunciate vote to each division when CI26 is satisfied (contact closed)	Project design approach	
HPCI-FR-38	Channel B shall provide a annunciate vote to each division when CI27 is satisfied (contact closed)	Project design approach	
HPCI-FR-39	Channel B shall provide a annunciate vote to each division when CI28 is satisfied (contact closed)	Project design approach	
HPCI-FR-40	Channel B shall provide a annunciate vote to each division when CI29 is satisfied (contact closed)	Project design approach	
HPCI-FR-41	Channel B shall provide a annunciate vote to each division when CI30 is satisfied (contact closed)	Project design approach	
HPCI-FR-42	Channel B shall provide a annunciate vote to each division when CI31 is satisfied (contact closed)	Project design approach	
HPCI-FR-43	Channel B shall provide a annunciate vote to each division when CI32 is satisfied (contact closed)	Project design approach	
HPCI-FR-44	Channel B shall provide a annunciate vote to each division when CI33 is satisfied (contact closed)	Project design approach	
HPCI-FR-45	Channel D shall provide a annunciate vote to each division when CI34 is satisfied (contact closed)	Project design approach	
HPCI-FR-46	Channel B shall provide a annunciate vote to each division when CI35 is satisfied (contact closed)	Project design approach	
HPCI-FR-47	Channel D shall provide a annunciate vote to each division when CI36 is satisfied (contact closed)	Project design approach	
HPCI-FR-48	Channel B shall provide a annunciate vote to each division when CI37 is satisfied (contact closed)	Project design approach	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-49	Channel B shall provide an isolate vote to each division when DI1 is satisfied.	Project design approach	
HPCI-FR-50	Channel D shall provide an isolate vote to each division when DI1 is satisfied.	Project design approach	
HPCI-FR-51	Each input to a channel (ma, contact input or digital signal) shall be voted on by the channel based on the condition (condition met or not met).	Project design approach	The term "shall be voted on" indicates that the channel performs a bi-stable comparison against a pre-determined configurable setpoint to determine whether the input is at or above/below the setpoint value.
HPCI-FR-52	Each channel shall provide the status of the vote (e.g. vote to not function if condition not met; vote to function if condition met; vote to annunciate) to each of the divisions.	Project design approach	The terms “not function”, “function”, “annunciate” describe different types of votes that may be provided by a channel (Note - others may be specified within the requirements). A particular vendor solution may combine one or more of the vote types into a single channel vote based on the capabilities of the platform.
HPCI-FR-53	Each division shall determine whether the votes to function for each type of input satisfy the voting criteria (e.g. 2oo4).	Project design approach	
HPCI-FR-54	Each division shall execute a function when the voting criteria is satisfied.	Project design approach	
HPCI-FR-55	Each input to a channel shall have an associated voter (e.g. 2oo4) within each division to ensure that trip inputs are voted separately.	Project design approach	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-56	Each division shall generate an output for an isolation, trip or initiation, when the required voting has been satisfied.	Project design approach	As an example, the RWL2 input to Channels A, B, C and D shall be sent to a 2oo4 voter in each of the divisions (Division 2 and Division 4). When at least two of the four RWL2 inputs to the 2oo4 voter achieves a trip state, the associated division generates an output. The generated output may be dependent on additional voting to be satisfied. Some outputs require different voting schemes which are described within the requirement.
HPCI-FR-57	Channel B shall include a manual initiation feature located in the control room that requires two distinct actions (e.g. arming prior to functioning) to be completed.	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
HPCI-FR-58	Channel B shall provide a vote to annunciate to Division 2 upon the first distinct action for the associated manual initiation feature being satisfied.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-59	Division 2 shall provide annunciation for MANUAL INITIATION SWITCH ARMED via the HMI when 1oo1 annunciate votes are received for the first distinct action for the manual initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-60	Channel B shall provide a vote for manual initiation to Division 2 on the second distinct action being satisfied.	Project design approach	
HPCI-FR-61	Each channel shall provide a vote for HPCI pump start to each division when RWL2 input reaches setpoint.	Project design approach	
HPCI-FR-62	Each channel shall provide a vote for HPCI pump start to each division when DHP input reaches setpoint	Project design approach	
HPCI-FR-63	Division 2 shall initiate a HPCI turbine pump start when 2oo4 start votes for RWL2 input are received.	GDC 35	
HPCI-FR-64	Division 2 shall initiate a HPCI turbine pump start when 2oo4 start votes for DHP input are received.	GDC 35	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-65	Division 2 shall initiate a HPCI turbine pump start when 1oo1 manual initiation votes is received.	GDC 35	
HPCI-FR-66	On a HPCI start, Division 2 shall provide an output to start the barometric condenser vacuum pump (BCVP).	Original design feature	
HPCI-FR-67	On a HPCI start, Division 2 shall provide an output to an indicating light via the HMI.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-68	Division 2 shall provide the capability to manually reset the indicating light (HMI) unless the HPCI turbine pump start condition is present.	Original design feature	
HPCI-FR-69	Division 2 shall seal in the output to start the barometric condenser vacuum pump (BCVP).	Original design feature	
HPCI-FR-70	Division 2 shall provide the capability to manually reset the BCVP sealed in output unless the HPCI turbine pump start condition is present.	Original design feature	
HPCI-FR-71	Division 2 shall provide a means to manually introduce a momentary signal to start or stop the BCVP by providing a signal to the pump control circuit.	Original design feature	
HPCI-FR-72	On a HPCI start, Division 2 shall provide an output to start the auxiliary oil pump (AOP).	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-73	Division 2 shall seal in the output to start the auxiliary oil pump (AOP).	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-74	Division 2 shall provide the capability to manually reset the AOP sealed in output unless the HPCI turbine pump start condition is present.	Original design feature	
HPCI-FR-75	Division 2 shall provide a means to manually start or stop the AOP by providing a signal to the pump control circuit.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-76	Division 2 shall provide AOP operating status indication via the HMI based on contact inputs from the associated pump control circuit.	IEEE Std. 603/IEEE Std. 7-4.3.2	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-77	Division 2 shall provide annunciation for HPCI OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI24 input are received.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-78	Division 2 shall provide AOP Overload / Power Loss alarm capability via the HMI when 1oo1 annunciate votes for CI24 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-79	On a HPCI start, Division 2 shall provide an output to open valve E41-F001 when 1oo1 condition votes for CI1 input is received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-80	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E41-F001 or terminate valve motion midstream from the control room.	Original design feature	
HPCI-FR-81	Division 2 shall provide valve E41-F001 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-82	On a HPCI start, Division 2 shall provide an output to open valve E41-F006 when 1oo1 condition votes for CI2 and 1oo1 condition votes for CI3 are satisfied.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-83	Division 2 shall provide an output to close valve E41-F006 (and inhibit opening) when 0oo1 condition votes for CI2 input are received.	Original design feature	
HPCI-FR-84	Division 2 shall provide an output to close valve E41-F006 (and inhibit opening) when 0oo1 condition votes for CI3 input are received.	Original design feature	
HPCI-FR-85	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E41-F006 or terminate valve motion midstream from the control room.	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-86	Division 2 shall provide valve E41-F006 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-87	On a HPCI start, Division 2 shall provide an output to open valve E41-F105 when 1oo1 condition votes for CI2 and 1oo1 condition votes for CI3 are satisfied.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-88	Division 2 shall provide an output to close valve E41-F105 (and inhibit opening) when 0oo1 condition votes for CI2 input are received.	Original design feature	
HPCI-FR-89	Division 2 shall provide an output to close valve E41-F105 (and inhibit opening) when 0oo1 condition votes for CI3 input are received.	Original design feature	
HPCI-FR-90	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E41-F105 or terminate valve motion midstream from the control room.	Original design feature	
HPCI-FR-91	Division 2 shall provide valve E41-F105 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-92	Division 2 shall provide a means to manually test the closing of valves E41-F006 and E41-F105 together.	Original design feature	
HPCI-FR-93	Division 2 shall provide annunciation for HPCI OUT OF SERVICE via the HMI when valves E41-F006 and E41-F105 are in test.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-94	On a HPCI start, Division 2 shall provide an output to open valve E41-F007.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-95	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E41-F007 or terminate valve motion midstream from the control room.	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-96	Division 2 shall provide valve E41-F007 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-97	Division 2 shall provide a means to manually test the closing of valve E41-F007.	Original design feature	
HPCI-FR-98	Division 2 shall provide annunciation for HPCI OUT OF SERVICE via the HMI when valve E41-F007 is in test.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-99	On a HPCI start, Division 2 shall provide an output to open valve E41-F004 when 1oo1 condition votes for CI4 input is received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-100	Division 2 shall provide an output to close valve E41-F004 when 0oo1 condition votes for CI4 and 1oo1 condition votes for CI5 are satisfied.	Original design feature	
HPCI-FR-101	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E41-F004 or terminate valve motion midstream from the control room.	Original design feature	
HPCI-FR-102	Division 2 shall provide valve E41-F004 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-103	On a HPCI start, Division 2 shall provide an output to close valve E41-F011.	GDC 37, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-104	Division 2 shall provide an output to close valve E41-F011 when 0oo1 condition votes for CI4 input are received.	Original design feature	
HPCI-FR-105	Division 2 shall provide an output to close valve E41-F011 when 1oo1 condition votes for CI7 input are received.	Original design feature	
HPCI-FR-106	Division 2 shall provide an output to close valve E41-F011 when 1oo1 condition votes for CI8 input are received.	Original design feature	
HPCI-FR-107	Division 2 shall provide a means to manually open and close valve E41-F011 or terminate valve motion midstream from the control room.	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-108	Division 2 shall provide valve E41-F011 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-109	On a HPCI start, Division 2 shall provide an output to close valve E41-F008.	GDC 37, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-110	Division 2 shall provide a signal to close valve E41-F008 when 1oo1 condition votes for CI9 input is received.	Original design feature	
HPCI-FR-111	Division 2 shall provide a means to manually introduce a momentary signal to close valve E41-F008 or terminate valve motion midstream from the control room.	Original design feature	
HPCI-FR-112	Division 2 shall provide a means to manually introduce a momentary signal to open valve E41-F008 when 1oo1 condition votes for CI10 input is received.	Original design feature	
HPCI-FR-113	Division 2 shall provide valve E41-F008 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-114	On a HPCI start, Division 2 shall provide an output to close valve E41-F071.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-115	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E41-F071 or terminate valve motion midstream from the control room.	Original design feature	
HPCI-FR-116	Division 2 shall provide valve E41-F071 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-117	Channel B shall provide the HPDP signal to Division 2.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-118	Division 2 shall provide the HPDP signal for indicator display via the HMI.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-119	Channel B shall provide a vote to open to each division when HPF1 exceeds setpoint low.	IEEE Std. 603/IEEE Std. 7-4.3.2	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-120	A 15 second timer shall start when HPF1 exceeds setpoint low.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-121	When the timer expires Channel B shall provide a vote to annunciate for to each division.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-122	Channel B shall provide a vote to open to each division when HPDP exceeds setpoint high.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-123	Division 2 shall provide an output to open valve E41-F012 when 1oo1 open votes for HPF1 input is received and 1oo1 open votes for HPDP input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-124	Division 2 shall provide annunciation for HPCI PUMP LO FLOW via the HMI when 1oo1 annunciate votes for HPF1 input is received and 1oo1 annunciate votes for CI25 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-125	Division 2 shall provide an output to close valve E41-F012 when 0oo1 open votes for HPF1 input is received.	Original design feature	
HPCI-FR-126	Division 2 shall provide an output to close valve E41-F012 when 0oo1 condition votes for CI2 input is received.	Original design feature	
HPCI-FR-127	Division 2 shall provide an output to close valve E41-F012 when 0oo1 condition votes for CI3 input is received.	Original design feature	
HPCI-FR-128	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E41-F012 or terminate valve motion midstream from the control room.	Original design feature	
HPCI-FR-129	Division 2 shall provide valve E41-F012 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-130	Division 2 shall provide two (2) outputs for HPCI compartment cooling when 1oo1 open votes for HPDP input is received.	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-131	Division 2 shall provide a signal to open valve E41-F059 when 1oo1 condition votes for CI3 input is received and 1oo1 condition votes for CI6 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-132	Division 2 shall provide a signal to close valve E41-F059 when 0oo1 condition votes for CI3 input is received.	Original design feature	
HPCI-FR-133	Division 2 shall provide a means to manually introduce a momentary signal to close valve E41-F059 or terminate valve motion midstream from the control room.	Original design feature	
HPCI-FR-134	Division 2 shall provide a means to manually introduce a momentary signal to open valve E41-F059 when 1oo1 condition votes for CI6 input is received.	Original design feature	
HPCI-FR-135	Division 2 shall provide valve E41-F059 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-136	Division 2 shall provide an output to close valve E41-F028 when 1oo1 condition votes for CI2 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-137	Division 2 shall provide a means to manually open valve E41-F028 when 0oo1 condition votes for CI2 input is received.	Original design feature	
HPCI-FR-138	Division 2 shall provide a means to manually close valve E41-F028.	Original design feature	
HPCI-FR-139	Division 2 shall provide valve E41-F028 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-140	Division 2 shall provide a signal to close valve E41-F029 when 1oo1 condition votes for CI2 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-141	Division 2 shall provide a means to manually open valve E41-F029 when 0oo1 condition votes for CI2 input is received.	Original design feature	
HPCI-FR-142	Division 2 shall provide a means to manually close valve E41-F029.	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-143	Division 2 shall provide valve E41-F029 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-144	Division 2 shall provide a signal to close valve E41-F026 when 1oo1 condition votes for CI2 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-145	Division 2 shall provide a signal to close valve E41-F026 when 1oo1 condition votes for CI11 is received.	Original design feature	
HPCI-FR-146	Division 2 shall provide a signal to open valve E41-F026 if 0oo1 condition votes for CI11 input is received and 0oo1 condition votes for CI2 is received.	Original design feature	
HPCI-FR-147	Division 2 shall provide a means to manually open valve E41-F026 when 0oo1 condition votes for CI2 input is received.	Original design feature	
HPCI-FR-148	Division 2 shall provide a means to manually close valve E41-F026.	Original design feature	
HPCI-FR-149	Division 2 shall provide valve E41-F026 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-150	Division 2 shall provide an output to close valve E41-F025 when 1oo1 condition votes for CI2 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-151	Division 2 shall provide a means to manually open valve E41-F025 when 0oo1 condition votes for CI2 input is received.	Original design feature	
HPCI-FR-152	Division 2 shall provide a means to manually close valve E41-F025.	Original design feature	
HPCI-FR-153	Division 2 shall provide valve E41-F025 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-154	Division 2 shall provide a signal to the turbine control ramp/signal generator when 1oo1 condition votes for CI3 input is received.	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-155	Channel B shall provide the RWL2 signal to Division 2.	Original design feature	
HPCI-FR-156	Channel B shall provide the RVP signal to Division 2.	Original design feature	
HPCI-FR-157	Channel B shall condition the HPF2 signal through a square root converter and convert dP to a flow signal.	Reg Guide 1.97	
HPCI-FR-158	Channel B shall provide the resultant flow signal to Division 2.	Reg Guide 1.97	
HPCI-FR-159	Division 2 shall provide the HPCI pump flow signal to the flow controller.	Reg Guide 1.97	
HPCI-FR-160	Division 2 shall provide the HPCI pump flow signal for indicator capability via the HMI.	Reg Guide 1.97	
HPCI-FR-161	Division 2 flow controller shall compare the flow signal to a flow setpoint and provide a speed demand signal to the turbine control ramp/signal generator.	Original design feature	
HPCI-FR-162	Division 2 flow controller shall be capable of providing PID flow control.	Project design approach	
HPCI-FR-163	Division 2 shall provide a means to manually adjust the flow setpoint of the flow controller.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-164	Division 2 shall provide the means to manually transfer from flow control mode to a level control mode.	Stakeholder design item	
HPCI-FR-165	Division 2 shall provide the RWL2 input signal to a level controller.	Stakeholder design item	
HPCI-FR-166	Division 2 shall provide the RWL2 signal for indicator capability via the HMI and transmit computer data to the non-SR DCS platform.	Stakeholder design item	
HPCI-FR-167	Division 2 level controller shall compare the RWL2 level signal to a level setpoint and provide a speed demand signal to the turbine control ramp/signal generator and transmit computer data to the non-SR DCS platform.	Stakeholder design item	
HPCI-FR-168	Division 2 level controller shall be capable of providing PID level control.	Stakeholder design item	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-169	Division 2 shall provide a means to manually adjust the level setpoint of the level controller.	Stakeholder design item	
HPCI-FR-170	Division 2 shall provide the means to manually transfer from flow control mode to a pressure control mode.	Stakeholder design item	
HPCI-FR-171	Division 2 shall provide the RVP input signal to a pressure controller.	Stakeholder design item	
HPCI-FR-172	Division 2 shall provide the RVP signal for indicator capability via the HMI and transmit computer data to the non-SR DCS platform.	Stakeholder design item	
HPCI-FR-173	Division 2 level controller shall compare the RVP pressure signal to a pressure setpoint and provide a speed demand signal to the turbine control ramp/signal generator and transmit computer data to the non-SR DCS platform.	Stakeholder design item	
HPCI-FR-174	Division 2 pressure controller shall be capable of providing PID pressure control.	Stakeholder design item	
HPCI-FR-175	Division 2 shall provide a means to manually adjust the pressure setpoint of the pressure controller.	Stakeholder design item	
HPCI-FR-176	Division 2 shall be capable of receiving a 0-1 mA turbine speed signal from the turbine EGM control box and providing it for indicator capability via the HMI.	Original design feature	
HPCI-FR-177	Channel B shall provide the HTSSP signal to Division 2.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-178	Division 2 shall provide the HTSSP signal for indicator capability via the HMI.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-179	Channel B shall provide a vote to transfer to each division when SCL exceeds setpoint high.	Project design approach	
HPCI-FR-180	Channel B shall provide a vote to annunciate to each division when SCL exceeds setpoint high.	Project design approach	
HPCI-FR-181	Channel B shall initiate a 12 second timer when CSTL exceeds setpoint low.	Project design approach	
HPCI-FR-182	When the timer expires, Channel B shall provide a vote to transfer to each division.	Project design approach	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-183	When the timer expires, Channel B shall provide a vote to annunciate to each division.	Project design approach	
HPCI-FR-184	Channel B shall reset the timer if CSTL no longer exceeds setpoint before the timer expires.	Project design approach	
HPCI-FR-185	Channel D shall provide a vote to transfer to each division when SCL exceeds setpoint high.	Project design approach	
HPCI-FR-186	Channel D shall provide a vote to annunciate to each division when SCL exceeds setpoint high.	Project design approach	
HPCI-FR-187	Channel D shall initiate a 12 second timer when CSTL exceeds setpoint low.	Project design approach	
HPCI-FR-188	When the timer expires, Channel D shall provide a vote to transfer to each division.	Project design approach	
HPCI-FR-189	When the timer expires, Channel D shall provide a vote to annunciate to each division.	Project design approach	
HPCI-FR-190	Division 2 shall initiate a transfer of the HPCI pump suction source from the CST to the suppression chamber when 1oo2 transfer votes for SCL input is received.	Original design feature	
HPCI-FR-191	Division 2 shall initiate a transfer of the HPCI pump suction source from the CST to the suppression chamber when 1oo2 transfer votes for CSTL input is received.	Original design feature	
HPCI-FR-192	Division 2 shall provide annunciation for COND STORAGE TANK LO LEVEL / SUCTION TRANSFER via the HMI when 1oo2 annunciate votes for CSTL input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-193	Division 2 shall provide annunciation for SUPPRESSION POOL HI LEVEL via the HMI when 1oo2 annunciate votes for SCL input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-194	On a suction transfer, Division 2 shall provide an output to open valves E41-F041 and E41-F042 to transfer the suction source.	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-195	Division 2 shall provide the capability to trip the HPCI turbine by providing an output to energize the turbine trip solenoid SV1.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-196	On a turbine trip, Division 2 shall provide annunciation for HPCI OUT OF SERVICE and a HPCI turbine trip alarm via the HMI.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-197	Each channel shall provide a vote to trip to each division when RWL8 exceeds setpoint high	Project design approach	
HPCI-FR-198	Each channel shall seal in the RWL8 input when setpoint is exceeded.	Original design feature	
HPCI-FR-199	Division 2 shall initiate a HPCI turbine trip when 2oo4 trip votes for RWL8 input are received.	GDC 35	
HPCI-FR-200	Each channel shall interrupt RWL8 seal-in when the RWL2 exceeds setpoint low.	Original design feature	
HPCI-FR-201	Division 2 shall provide a means to manually introduce a momentary signal to trip the HPCI turbine.	Original design feature	
HPCI-FR-202	Channel B shall provide a vote to trip to each division when HPSP1 exceeds setpoint low.	Project design approach	
HPCI-FR-203	Channel B shall provide a vote to annunciate to each division when HPSP1 exceeds setpoint low.	Project design approach	
HPCI-FR-204	Channel B shall provide the HPSP2 signal to Division 2.	Project design approach	
HPCI-FR-205	Channel B shall provide a vote to annunciate to each division when HPSP2 exceeds setpoint high.	Project design approach	
HPCI-FR-206	Channel B shall provide a vote to trip to each division when HTEP exceeds setpoint.	Project design approach	
HPCI-FR-207	Channel B shall provide a vote to annunciate to each division when HTEP exceeds setpoint.	Project design approach	
HPCI-FR-208	Channel B shall provide the HTEP signal to Division 2.	Project design approach	
HPCI-FR-209	Channel D shall provide a vote to trip to each division when HTEP exceeds setpoint.	Project design approach	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-210	Channel D shall provide a vote to annunciate to each division when HTEP exceeds setpoint.	Project design approach	
HPCI-FR-211	Division 2 shall initiate a HPCI turbine trip when 1oo1 trip vote for HPSP1 input is received.	Original design feature	There are two transmitters that sense suction pressure. One that monitors pressure above setpoint (for indicator and annunciator) and one that monitors pressure below setpoint for tripping turbine. Consider one transmitter for both, or make use of both for reliability.
HPCI-FR-212	Division 2 shall provide the HPSP2 signal for indicator capability via the HMI.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-213	Division 2 shall provide annunciation for HPCI PUMP SUCTION HI PRESS via the HMI when 1oo1 annunciate votes for HPSP2 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-214	Division 2 shall provide annunciation for HPCI PUMP SUCTION LO PRESS via the HMI when 1oo1 annunciate votes for HPSP1 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-215	Division 2 shall initiate a HPCI turbine trip when 1oo2 trip votes for HTEP input are received.	Original design feature	
HPCI-FR-216	Division 2 shall provide annunciation for HPCI TURBINE EXHAUST HI PRESS via the HMI when 1oo2 annunciate votes for HTEP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-217	Division 2 shall provide the HTEP signal for indicator capability via the HMI.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-218	Division 2 shall provide annunciation for HPCI OIL LO PRESS via the HMI when 1oo1 annunciate votes for CI26 input is received and 1oo1 annunciate votes for CI25 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-219	Division 2 shall provide annunciation for HPCI VACUUM TANK LO VACUUM via the HMI when 1oo1 annunciate votes for CI27 input is received and 1oo1 annunciate votes for CI25 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-220	Division 2 shall provide annunciation for HPCI OIL HI TEMP via the HMI when 1oo1 annunciate votes for CI28 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-221	Division 2 shall provide annunciation for HPCI FILTER HI Δ PRESS via the HMI when 1oo1 annunciate votes for CI29 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-222	Division 2 shall provide annunciation for HPCI OIL TANK LEVEL HI/LO via the HMI when 1oo1 annunciate votes for CI30 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-223	Division 2 shall provide annunciation for HPCI VACUUM PUMP / COND PUMP / MOTOR OVLD / LOSS OF POWER the HMI when 1oo1 annunciate votes for CI31 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-224	Division 2 shall provide annunciation for HPCI VACUUM TANK HI/LO LEVEL via the HMI when 1oo1 annunciate votes for CI32 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-225	Division 2 shall provide annunciation for HPCI VACUUM TANK HI/LO LEVEL via the HMI when 1oo1 annunciate votes for CI37 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-226	Division 2 shall initiate an isolation signal when conditions for monitored parameters are satisfied.	Reg Guide 1.53, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-227	Division 4 shall initiate an isolation signal when conditions for monitored parameters are satisfied.	Reg Guide 1.53, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-228	The Division 2 isolation signal (whether automatic or manually initiated) shall remain sealed in until manually reset.	Original design feature	
HPCI-FR-229	The Division 4 isolation signal (whether automatic or manually initiated) shall remain sealed in until manually reset.	Original design feature	
HPCI-FR-230	Each division shall provide annunciation for HPCI OUT OF SERVICE via the HMI when the isolation signal is initiated.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-231	Each division shall provide HPCI Isolation Initiated alarm capability via the HMI when an isolation signal is initiated.	Original design feature	
HPCI-FR-232	The HSF input shall be used to monitor forward steam flow and reverse steam flow.	Original design feature	
HPCI-FR-233	Channel B shall provide a vote to isolate to each division when HSF exceeds setpoint high after a three (3) second time delay.	Project design approach	
HPCI-FR-234	Channel B shall provide a vote to annunciate to each division when HSF exceeds setpoint high after a three (3) second time delay.	Project design approach	
HPCI-FR-235	Channel B shall provide a vote to isolate to each division when HSF exceeds setpoint low after a three (3) second time delay.	Project design approach	
HPCI-FR-236	Channel B shall provide a vote to annunciate to each division when HSF exceeds setpoint low after a three (3) second time delay.	Project design approach	
HPCI-FR-237	Channel D shall provide a vote to isolate to each division when HSF exceeds setpoint high after a three (3) second time delay.	Project design approach	
HPCI-FR-238	Channel D shall provide a vote to annunciate to each division when HSF exceeds setpoint high after a three (3) second time delay.	Project design approach	
HPCI-FR-239	Channel D shall provide a vote to isolate to each division when HSF exceeds setpoint low after a three (3) second time delay.	Project design approach	
HPCI-FR-240	Channel D shall provide a vote to annunciate to each division when HSF exceeds setpoint low after a three (3) second time delay.	Project design approach	
HPCI-FR-241	Each channel shall provide a vote to isolate to each division when SLP exceeds setpoint low.	Project design approach	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-242	Each channel shall provide a vote to annunciate to each division when SLP exceeds setpoint low.	Project design approach	
HPCI-FR-243	Each channel shall provide a vote to isolate to each division when RDHP exceeds setpoint high.	Project design approach	
HPCI-FR-244	Each channel shall provide a vote to annunciate to each division when RDHP exceeds setpoint high.	Project design approach	
HPCI-FR-245	Division 2 shall provide annunciation for HI HPCI STEAM LINE FLOW via the HMI when 2oo4 annunciate votes for HSF high input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-246	Division 2 shall provide annunciation for HI HPCI STEAM LINE FLOW via the HMI when 2oo4 annunciate votes for HSF low input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-247	Division 4 shall provide annunciation for HI HPCI STEAM LINE FLOW via the HMI when 2oo4 annunciate votes for HSF high input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-248	Division 4 shall provide annunciation for HI HPCI STEAM LINE FLOW via the HMI when 2oo4 annunciate votes for HSF low input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-249	Division 2 shall initiate a HPCI solation signal when 2oo4 isolate votes for HSF input are received.	GDC 55, GDC 56	
HPCI-FR-250	Division 4 shall initiate a HPCI solation signal when 2oo4 isolate votes for HSF input are received.	GDC 55, GDC 56	
HPCI-FR-251	Division 2 shall initiate a HPCI solation signal when 1oo2 isolate votes for DI1 input are received.	GDC 35, GDC 55, GDC 56, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-252	Division 4 shall initiate a HPCI solation signal when 1oo2 isolate votes for DI1 input are received.	GDC 55, GDC 56, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-253	Division 2 shall initiate HPCI solation signal when 2oo4 isolate votes for SLP input are received.	GDC 55, GDC 56, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-254	Division 4 shall initiate HPCI solation signal when 2oo4 isolate votes for SLP input are received.	GDC 55, GDC 56, IEEE Std. 603/IEEE Std. 7-4.3.2	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-255	Division 2 shall initiate HPCI solation signal when 2oo4 isolate votes for RDHP input are received.	GDC 55, GDC 56, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-256	Division 4 shall initiate HPCI solation signal when 2oo4 isolate votes for RDHP input are received.	GDC 55, GDC 56, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-257	Each division shall provide annunciation for HPCI TURBINE EXHAUST DIAPHRAGM RUPTURED via the HMI when 1oo2 annunciate votes for RDHP input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-258	Each division shall provide a means to manually initiate an isolation signal from the control room.	Reg Guide 1.62	
HPCI-FR-259	Each division shall include an interlock which prohibits manual isolation of the HPCI turbine unless a HPCI turbine pump start signal (automatic or manual) is present.	Original design feature	
HPCI-FR-260	Division 2 HPCI isolation signal shall provide outputs to close the following outboard valves: • E41-F041 • E41-F042 • E41-F003 • E41-F100	GDC 56	
HPCI-FR-261	Division 2 HPCI isolation signal shall provide outputs to trip the HPCI turbine.	GDC 56	
HPCI-FR-262	Division 4 HPCI isolation signal shall provide an output to close the following inboard valve: • E41-F002 • Trip the HPCI turbine.	GDC 56	
HPCI-FR-263	Division 4 HPCI isolation signal shall provide an output to trip the HPCI turbine.	GDC 56	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-264	In addition to the isolation signal, Division 2 shall provide a duplicate signal to close the following outboard valves when 2oo4 isolate votes for SLP input are received: • E41-F041 • E41-F042 • E41-F100	GDC 55, GDC 56, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-265	Division 2 shall provide interlocks that prohibit valves E41-F041 and E41-F042 from automatically opening if an isolation signal is present.	Original design feature	
HPCI-FR-266	Division 2 shall provide interlocks that prohibit valves E41-F041 and E41-F042 from automatically opening if an SLP initiated signal is present.	Original design feature	
HPCI-FR-267	Division 2 shall provide interlocks that prohibit valves E41-F041 and E41-F042 from being manually opened if an isolation signal is present.	Original design feature	
HPCI-FR-268	Division 2 shall provide interlocks that prohibit valves E41-F041 and E41-F042 from being manually opened if an SLP initiated signal is present.	Original design feature	
HPCI-FR-269	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E41-F041 or terminate valve motion midstream from the control room.	Original design feature	
HPCI-FR-270	Division 2 shall provide valve E41-F041 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-271	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E41-F042 or terminate valve motion midstream from the control room.	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-272	Division 2 shall provide valve E41-F042 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-273	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E41-F100 or terminate valve motion midstream from the control room.	Original design feature	
HPCI-FR-274	Division 2 shall provide an interlock to prevent valve E41-F100 from being manually opened if an isolation signal is present.	Original design feature	
HPCI-FR-275	Division 2 shall provide an interlock to prevent valve E41-F100 from being manually opened if an SLP initiated signal is present.	Original design feature	
HPCI-FR-276	Division 2 shall provide valve E41-F100 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-277	Division 2 shall provide annunciation for HPCI WARMUP LINE ISOLATION VALVE OPEN via the HMI when 1oo1 annunciate votes for CI14 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-278	Division 4 shall provide a means to manually open or close valve E41-F002, under administrative control, from the control room.	Original design feature	
HPCI-FR-279	Division 4 shall provide valve E41-F002 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-280	Division 4 shall provide an interlock to prevent valve E41-F002 from being manually opened if an isolation signal is present.	Original design feature	
HPCI-FR-281	Division 4 shall provide alarm capability via the HMI when valve E41-F002 is manually closed.	Reg Guide 1.47	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-282	Division 4 shall provide alarm capability via the HMI when 1oo1 annunciate votes for CI12 input is received.	Reg Guide 1.47	
HPCI-FR-283	Division 4 shall provide annunciation for HPCI OUT OF SERVICE via the HMI when valve E41-F002 is manually closed.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-284	Division 2 shall provide a means to manually open or close valve E41-F003, under administrative control, from the control room.	Original design feature	
HPCI-FR-285	Division 2 shall provide valve E41-F003 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-286	Division 2 shall provide an interlock to prevent valve E41-F003 from being manually opened if an isolation signal is present.	Original design feature	
HPCI-FR-287	Division 2 shall provide alarm capability via the HMI when valve E41-F003 is manually closed.	Reg Guide 1.47	
HPCI-FR-288	Division 2 shall provide alarm capability via the HMI when 1oo1 annunciate votes for CI13 is received.	Original design feature	
HPCI-FR-289	Division 2 shall provide annunciation for HPCI OUT OF SERVICE via the HMI when valve E41-F003 is manually closed.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-290	Division 2 shall provide an output to close valve E41-F093 when 2oo4 start votes for DHP input and 2oo4 isolate votes for SLP input are received.	Original design feature	
HPCI-FR-291	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E41-F093 or terminate valve motion midstream from the control room.	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-292	Division 2 shall provide an interlock to prevent valve E41-F093 from being manually opened when 2oo4 start votes for DHP input and 2oo4 isolate votes for SLP input are received.	Original design feature	
HPCI-FR-293	Division 2 shall provide valve E41-F093 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-294	Division 4 shall provide an output to close valve E41-F095 when 2oo4 start votes for DHP input and 2oo4 isolate votes for SLP input are received.	Original design feature	
HPCI-FR-295	Division 4 shall provide a means to manually introduce a momentary signal to open or close valve E41-F095 or terminate valve motion midstream from the control room.	Original design feature	
HPCI-FR-296	Division 4 shall provide valve E41-F095 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-297	Division 4 shall provide an interlock to prevent valve E41-F095 from being manually opened when 2oo4 start votes for DHP input and 2oo4 isolate votes for SLP input are received.	Original design feature	
HPCI-FR-298	Division 2 shall provide annunciation for HPCI VACUUM BREAKER ISOLATION VALVES NOT FULLY OPEN via the HMI when 1oo1 annunciate votes for CI33 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-299	Division 4 shall provide annunciation for HPCI VACUUM BREAKER ISOLATION VALVES NOT FULLY OPEN via the HMI when 1oo1 annunciate votes for CI34 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-300	Division 2 shall provide a signal to open valve E41-F054 when 1oo1 open votes for CI15 input is received.	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-301	Division 2 shall provide annunciation for HPCI TURBINE INLET DRAIN POT HI LEVEL via the HMI when 1oo1 annunciate votes for CI15 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-302	Division 2 shall provide a means to manually open or close valve E41-F054 from the control room.	Original design feature	
HPCI-FR-303	Division 2 shall provide valve E41-F054 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-304	Division 2 shall provide a means to manually open or close valve E41-F072, under administrative control, from the control room.	Original design feature	
HPCI-FR-305	Division 2 shall provide valve E41-F072 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-306	Division 2 shall provide alarm capability via the HMI when valve E41-F072 is manually closed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-307	Division 2 shall provide alarm capability via the HMI when 1oo1 annunciate votes for CI19 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-308	Division 2 shall provide annunciation for HPCI OUT OF SERVICE via the HMI when valve E41-F072 is manually closed.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-309	Division 2 shall provide annunciation for HPCI OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI17 input is received.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-310	Division 2 shall provide annunciation for HPCI OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI18 input is received.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-311	Division 2 shall provide annunciation for HPCI OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI35 inputs is received.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-312	Division 4 shall provide annunciation for HPCI OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI16 input is received.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-313	Division 4 shall provide annunciation for HPCI OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI36 input is received.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-314	Each division shall provide a means to manually provide annunciation for HPCI OUT OF SERVICE and alarm capability via the HMI.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-315	Division 2 shall provide MOV Overload / Power Loss alarm capability via the HMI when 1oo1 annunciate votes for CI35 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-316	Division 2 shall provide MOV Overload / Power Loss alarm capability via the HMI when 1oo1 annunciate votes for CI36 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-317	Division 2 shall provide turbine governor valve position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-318	Division 2 shall provide turbine stop valve position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-319	Each division shall provide the means to manually test the logic system for loss of power.	Original design feature	
HPCI-FR-320	Each division shall provide annunciation and alarm capability via the HMI for any logic anomaly or loss of power condition.	Project design approach	
HPCI-FR-321	Each division shall provide the means to perform functional tests during normal plant operation.	GDC 37, Reg Guide 1.22, IEEE Std. 603/IEEE Std. 7-4.3.2	
HPCI-FR-322	Each division shall be capable of automatically returning to a coolant injection mode from a test mode when an automatic initiation condition occurs.	Original design feature	

HPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/HPCI Requirement**	**PPS/HPCI Source / Basis**	**Notes / Clarification**
HPCI-FR-323	Each channel and each division shall provide sufficient features and documented evaluations to support elimination of most Technical Specification Surveillance Tests, and minimize the requirements for manual calibration checks.	Project design approach	
HPCI-FR-324	For all PPS inputs that have the potential to require manual test insertion or external measurement of input or output values (i.e., use of an external digital multi meter by a technician), test jacks are provided in the cabinets.	Project design approach	
HPCI-FR-325	For all inputs that have the potential to require manual multi-point calibration checks with external calibration equipment, knife edge disconnects along with test jacks are incorporated in the field termination panels.	Project design approach	
HPCI-FR-326	For the analog output, knife edge disconnects along with test jacks are incorporated in the field termination panels.	Project design approach	

D

D.1 ADS Design Requirements

ADS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
ADS-DR-1	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. 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. 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.	GDC 1 - Quality standards and records
ADS-DR-2	Structures, systems, and components important to safety shall be designed to withstand the effect of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions.	GDC 2 - Design Bases for Protection Against Natural Phenomena
ADS-DR-3	Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions.	GDC 3 - Fire protection
ADS-DR-4	Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents (LOCAs).	GDC 4 - Environmental and dynamic effects design bases
ADS-DR-5	The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.	GDC 10 - Reactor design

ADS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
ADS-DR-6	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.	GDC 13 - Instrumentation and control
ADS-DR-7	A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. 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 I&C 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.	GDC 19 - Control Room
ADS-DR-8	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.	GDC 20 - Protection system functions

ADS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
ADS-DR-9	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.	GDC 21 - Protection system reliability and testability
ADS-DR-10	The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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.	GDC 22- Protection system independence
ADS-DR-11	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.	GDC 23 - Protection system failure modes
ADS-DR-12	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.	GDC 24 - Separation of protection and control systems

ADS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
ADS-DR-13	The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.	GDC 29 - Protection against anticipated operational occurrences
ADS-DR-14	A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts.	GDC 35 - Emergency Core Cooling
ADS-DR-15	The emergency core cooling system shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leak tight integrity of its components, (2) the operability and performance of the active components of the system, and (3) the operability of the system as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.	GDC 37 - Testing of Emergency Core Cooling System
ADS-DR-16	The protection system shall be designed to permit periodic testing of its initiation functions inclusive of the actuation devices and actuated equipment when the reactor is in operation.	Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions (Safety Guide 22)
ADS-DR-17	Those structures, systems, and components (SSC) that should be designed to remain functional if the Safe Shutdown Earthquake (SSE) occurs shall be designated as Seismic Category I. (This includes Systems or portions of systems that are required for reactor shutdown; all electric and mechanical devices and circuitry between the process and the input terminals of the actuator systems involved in generating signals that initiate protective action; systems or portions of systems that are required for (1) monitoring of systems important to safety and (2) actuation of systems important to safety.)	Regulatory Guide 1.29 - Seismic Design Classification

ADS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
ADS-DR-18	The ADS shall comply with the requirements of Appendix B to 10 CFR Part 50 for the installation, inspection, and testing of nuclear power plant instrumentation and electric equipment.	Regulatory Guide 1.30 - Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment (Safety Guide 30)
ADS-DR-19	The ADS shall meet the requirements for design, operation, and testing of safety-related power systems within nuclear power plants as defined within IEEE Std. 308.	Regulatory Guide 1.32 - Criteria for Power Systems for Nuclear Power Plants
ADS-DR-20	The ADS shall meet the requirements for indicating the bypass or inoperable status of portions of the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the system it actuates to perform their safety-related functions:	Regulatory Guide 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
ADS-DR-21	The ADS shall comply with the IEEE Std. 279 requirement that any single failure within the protection system shall not prevent proper protective action at the system level when required, by utilizing the guidance in IEEE Std. 379-1972 for applying the single-failure criterion to the design and analysis of nuclear power plant protection systems.	Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Safety Systems
ADS-DR-22	The ADS shall provide a means for manual initiation of protective actions.	Regulatory Guide 1.62 - Manual Initiation of Protective Actions
ADS-DR-23	The ADS shall meet the requirements for physical independence of the circuits and electric equipment comprising or associated with the Class 1E power system, the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety related functions.	Regulatory Guide 1.75 - Physical Independence of Electric Systems
ADS-DR-24	The ADS shall comply with design verification requirements to verify adequacy of design under the most adverse design conditions.	Regulatory Guide 1.89 - Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants

ADS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
ADS-DR-25	The ADS shall comply with the requirement to: (1) provide information required to permit the operator to take preplanned manual actions to accomplish safe plant shutdown; (2) determine whether the reactor trip, engineered safety feature systems, and manually initiated safety systems and other systems important to safety are performing their intended functions (i.e., reactivity control, core cooling, maintaining reactor coolant system integrity, and maintaining containment integrity); (3) provide information to the operators that will enable them to determine the potential for causing a gross breach of the" barriers to radioactivity release (i.e., fuel cladding, reactor coolant pressure boundary, and containment) and to determine if a gross breach of a barrier has occurred.	Regulatory Guide 1.97 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants
ADS-DR-26	The ADS shall comply with design verification requirements to verify the seismic adequacy of electric equipment.	Regulatory Guide 1.100 - Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants
ADS-DR-27	The ADS shall design shall implement setpoints that assure sufficient margin between Technical Specification limits and the trip setpoint to account for instrument inaccuracy, calibration uncertainties and instrument drift. Consideration of instrument span and range as well as environmental influences must be included.	Regulatory Guide 1.105 - Instrument Setpoint
ADS-DR-28	The ADS shall comply with the requirements for periodic testing of electric power and protection systems.	Regulatory Guide 1.118 - Periodic Testing of Electric Power and Protection Systems
ADS-DR-29	The ADS shall, with precision and reliability, actuate Main Steam Relief Valves (SRVs) to depressurize the reactor pressure vessel so that injection flow to the vessel can occur in adequate time to cool the core and limit excessive fuel temperatures.	IEEE Std. 603, Section 5.0 Safety System Criteria and 6.1 Automatic Control

ADS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
ADS-DR-30	The ADS shall initiate when the monitored plant parameter exceeds the following trip setpoint: Reactor Vessel Water Level 1 < -129 inches Drywell Pressure > 1.68 psig Core Spray Pump Discharge Pressure ≥ 145 psig RHR LPCI Mode Pump Discharge Pressure ≥ 125psig Reactor Vessel Water Level-3 < 12.5 inches	IEEE Std. 603, Section 6.1 Automatic Control
ADS-DR-31	The ADS shall be capable of actuating SRVs under all required modes of reactor operation.	IEEE Std. 603, Section 4.1
ADS-DR-32	The ADS shall ensure that the protective action, once started, continues to completion.	IEEE Std. 603, Section 5.2 Completion of Protective Action
ADS-DR-33	Any single failure within the ADS shall not prevent proper protective action at the system level when required.	IEEE Std. 603, Section 5.1 Single Failure Criterion and IEEE Std. 7-4.3.2 Section 5.1 Single Failure Criterion
ADS-DR-34	Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.	IEEE Std. 603 section 5.3 Quality and IEEE Std. 7-4.3.2 section 5.3 Quality
ADS-DR-35	Type test data or reasonable engineering extrapolation based on test data shall be available to verify that protection system equipment shall meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements.	IEEE Std. 603 section 5.4 Equipment Qualification and IEEE Std. 7-4.3.2 section 5.4 Equipment Qualification
ADS-DR-36	All protection system channels shall be designed to maintain necessary functional capability under extremes of conditions (as applicable) relating to environment, energy supply, malfunctions and accidents.	IEEE Std. 603 section 5.5 System Integrity and IEEE Std. 7-4.3.2 and section 5.5 Independence

ADS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
ADS-DR-37	Channels that provide signals for the same protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 System Integrity
ADS-DR-38	Any equipment that is used for both protective and control functions shall be classified as part of the protection system and shall meet all the applicable requirements.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence
ADS-DR-39	The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system and shall meet all the applicable requirements. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence
ADS-DR-40	Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
ADS-DR-41	Provisions shall be included so that the protective action can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems

ADS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
ADS-DR-42	Where a credible single event can cause a control system action that results in a condition requiring protective action and can concurrently prevent the protective action from those protection system channels designated to provide principal protection against the condition, then alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design bases.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
ADS-DR-43	To the extent feasible and practical, protection system inputs shall be derived from signals that are direct measures of the desired variables.	IEEE Std. 603 section 6.4 Derivation of System Inputs
ADS-DR-44	Means shall be provided for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
ADS-DR-45	Capability shall be provided for testing and calibrating channels and the devices used to derive the final system output signal from the various channel signals.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
ADS-DR-46	For those parts of the system where the required interval between testing will be less than the normal time interval between generating station shutdowns, there shall be capability for testing during power operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
ADS-DR-47	The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective action at the systems level.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
ADS-DR-48	During such operation, the active parts of the system shall of themselves continue to meet the single failure criterion.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
ADS-DR-49	Where operating requirements necessitate automatic or manual bypass of a protective function, the design shall be such that the bypass will be removed automatically whenever permissive conditions are not met.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
ADS-DR-50	Devices used to achieve automatic removal of the bypass of a protective function are part of the protection system and shall be designed in accordance with these criteria.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses

ADS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
ADS-DR-51	If the protective action of some part of the system has been bypassed or deliberately rendered inoperative for any purpose, this fact shall be continuously indicated in the control room.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
ADS-DR-52	The design shall permit the administrative control of the means for manually bypassing channels or protective functions.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
ADS-DR-53	Where it is necessary to change to a more restrictive set point to provide adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of assuring that the more restrictive set point is used.	IEEE Std. 603 section 6.8 Setpoints
ADS-DR-54	The devices used to prevent improper use of less restrictive set points shall be considered a part of the protection system and shall be designed in accordance with the other provisions of these criteria regarding performance and reliability.	IEEE Std. 603 section 6.8 Setpoints
ADS-DR-55	The protection system shall be so designed that, once initiated, a protective action at the system level shall go to completion.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action
ADS-DR-56	Return to operation shall require subsequent deliberate operator action.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action
ADS-DR-57	The protection system shall include means for manual initiation of each protective action at the system level (for example, reactor trip, containment isolation, safety injection, core spray, etc).	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
ADS-DR-58	No single failure within the manual, automatic, or common portions of the protection system shall prevent initiation of protective action by manual or automatic means.	IEEE Std. 603 section 7.2 Manual Control
ADS-DR-59	Manual initiation should depend upon the operation of a minimum of equipment.	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
ADS-DR-60	The design shall permit the administrative control of access to all set point adjustments, module calibration adjustments, and test points.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access

ADS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
ADS-DR-61	Protective actions shall be indicated and identified down to the channel level.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
ADS-DR-62	The protection system shall be designed to provide the operator with accurate, complete, and timely information pertinent to its own status and to generating station safety.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
ADS-DR-63	The design shall minimize the development of conditions which would cause meters, annunciators, recorders, alarms, etc, to give anomalous indications confusing to the operator.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
ADS-DR-64	The system shall be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.	IEEE Std. 603 section 5.10 Repair
ADS-DR-65	In order to provide assurance that the requirements given in this document can be applied during the design, construction, maintenance, and operation of the plant, the protection system equipment (for example, interconnecting wiring, components, modules, etc), shall be identified distinctively as being in the protection system.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
ADS-DR-66	This identification shall distinguish between redundant portions of the protection system. (In the installed equipment, components, or modules mounted in assemblies that are clearly identified as being in the protection system do not themselves require identification.) All software, firmware, and programmable logic shall be identified in accordance with IEEE Std. 7-4.3.2 Clause 5.11.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
ADS-DR-67	ADS shall conform to the design criteria and features for Class 1E electric systems to ensure that functional requirements under the conditions produced by design basis events are met.	IEEE Std. 308 - Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations

ADS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
ADS-DR-68	ADS shall conform to the methods for demonstrating the qualification of Class 1E equipment including components or equipment of any interface whose failure could adversely affect the performance of Class 1E systems and electronic equipment.	IEEE Std. 323 - Qualifying Class 1E Equipment for Nuclear Power Generating Stations
ADS-DR-69	ADS shall conform to the design and operational criteria for the performance of periodic testing of nuclear power generating station safety systems.	IEEE Std. 338 - Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems
ADS-DR-70	ADS shall meet its Class 1E performance requirements during and following one SSE (safe shutdown earthquake) preceeded by a number of OBEs (operating basis earthquakes).	IEEE Std. 344 - Guide for Seismic Qualification of Class 1 Electric Equipment for Nuclear Power Generating Stations
ADS-DR-71	ADS shall meet the single failure criterion as described and classified in IEEE Std. 379.	IEEE Std. 379 - Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems
ADS-DR-72	ADS shall meet the criteria and requirements for establishing and maintaining the independence of Class 1E equipment and circuits and auxiliary supporting features by physical separation and electrical isolation.	IEEE Std. 384 - Criteria for Independence of Class 1E Equipment and Circuits

D.2 ADS Functional Requirements

ADS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/ADS Requirement Revised**	**PPS/ADS Source / Basis**	**Notes / Clarification**
ADS-FR-1	The PPS/ADS shall be capable of initiating a signal to actuate Main Steam Relief Valves (SRVs) either automatically when monitored parameters exceed a pre-established value, or by manual initiation.	GDC 13 , GDC 20, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-2	The PPS/ADS shall be comprised of two independent and separate divisions (Division 1 and Division 3)	GDC 22, GDC 24, Reg Guide 1.53, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-3	PPS/ADS shall have four (4) independent channels: (Channel A, Channel B, Channel C, and Channel D) that each provide votes/signals to each of the divisions.	GDC 22, GDC 24, Reg Guide 1.53, IEEE Std. 603/IEEE Std. 7-4.3.2	The four channels are common to both divisions.
ADS-FR-4	Each channel shall receive an input from each of the following monitored parameters that are provided as common inputs to the PPS platform and are shared by each of the PPS functions: • Reactor Vessel Low Water Level (Level 1) (RWL 1) • Drywell High Pressure (DHP) • Reactor Vessel Low Water Level (Level 3) (RWL 3)	GDC 13, GDC 20, GDC 35, IEEE 279	
ADS-FR-5	Each channel shall receive a 4-20 mA input from each of the following monitored parameters: • RHR Pump A Discharge Pressure (RDPA) • Core Spray Pump A Discharge Pressure (CSDPA) • RHR Pump B Discharge Pressure (RDPB) • Core Spray Pump B Discharge Pressure (CSDPB) • RHR Pump C Discharge Pressure (RDPC) • Core Spray Pump C Discharge Pressure (CSDPC) • RHR Pump D Discharge Pressure (RDPD) • Core Spray Pump D Discahrge Pressure (CSDPD)	GDC 20, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

ADS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/ADS Requirement Revised**	**PPS/ADS Source / Basis**	**Notes / Clarification**
ADS-FR-6	Each input to a channel (ma or contact input) shall be voted on by the channel based on the condition (condition met or not met).	Project design approach	The term "shall be voted on" indicates that the channel performs a bi-stable comparison against a pre-determined configurable setpoint to determine whether the input is at or above/below the setpont value.
ADS-FR-7	Each channel shall provide the status of the vote (e.g. vote to not function if condition not met; vote to function if condition met; vote to annunciate) to each of the divisions.	Project design approach	The terms “not function”, “function”, “annunciate” describe different types of votes that may be provided by a channel (Note -others may be specified within the requirements). A particular vendor solution may combine one or more of the vote types into a single channel vote based on the capabilities of the platform.
ADS-FR-8	Each division shall determine whether the votes to function for each type of input satisfy the voting criteria (e.g. 2oo4)	Project design approach	
ADS-FR-9	Each division shall execute a function when the voting criteria is satisfied.	Project design approach	As an example, the RWL1 input to Channels A, B, C, and D shall be sent to a 2oo4 voter in each of the divisions (Division 1 and Division 3). When at least two of the four RWL1 inputs to the 2oo4 voter are satisfied, the associated division generates an output. The generated output may be dependent on additional voting to be satisfied. Some outputs require different voting schemes which are described within the requirement.
ADS-FR-10	Each input to a channel shall have an associated voter (e.g. 2oo4) within each division to ensure that trip inputs are voted separately.	Project design approach	
ADS-FR-11	Each channel shall provide a vote to annunciate to each division when RWL3 exceeds setpoint low.	Project design approach	

ADS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/ADS Requirement Revised**	**PPS/ADS Source / Basis**	**Notes / Clarification**
ADS-FR-12	Division 1 shall provide annunciation for REACTOR LEVEL 3 ADS PERMISSIVE via the HMI when 2oo4 annunciate votes for RWL3 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-13	Division 3 shall provide annunciation for REACTOR LEVEL 3 ADS PERMISSIVE via the HMI when 2oo4 annunciate votes for RWL3 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-14	Each channel shall initiate an ADS timer of 117 seconds when RWL1 exceeds setpoint low **and** DHP exceeds setpoint high **and** RWL3 exceeds setpoint.	GDC 13, GDC 19, GDC 20, GDC 35, Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-15	Each channel shall provide a vote to annunciate to each division when the ADS timer starts.	Project design approach	
ADS-FR-16	Division 1 shall provide annunciation for ADS TIMER INITIATED via the HMI when 2oo4 annunciate votes for ADS timer initiated are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-17	Division 1 shall provide a displayed ADS timer countdown via the HMI when 2oo4 annunciate votes for ADS timer initiated are received.	Project design approach	
ADS-FR-18	Division 3 shall provide annunciation for ADS TIMER INITIATED via the HMI when 2oo4 annunciate votes for ADS timer initiated are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-19	Division 3 shall provide a displayed ADS timer countdown via the HMI when 2oo4 annunciate votes for ADS timer initiated are received.	Project design approach	
ADS-FR-20	Each channel shall reset the ADS 117 second timer and provide a vote to not annunciate if the RWL1 input drops below setpoint before the timer times out.	Original design feature	
ADS-FR-21	Each channel shall seal in the DHP input when the setpoint is exceeded and shall provide a vote to annunciate to each division.	IEEE Std. 603/IEEE Std. 7-4.3.2, project design approach	
ADS-FR-22	Division 1 shall provide annunciation and an indicating light via the HMI when the DHP input is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	

ADS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/ADS Requirement Revised**	**PPS/ADS Source / Basis**	**Notes / Clarification**
ADS-FR-23	Division 3 shall provide annunciation and an indicating light via the HMI when the DHP input is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-24	Each channel shall provide a means for manually resetting the DHP seal in feature.	GDC 13, Reg Guide 1.62 IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-25	Each channel shall initiate a 450 second timer when RWL1 exceeds setpoint and shall provide a vote to annunciate to each division.	NUREG 0737, IEEE 279	
ADS-FR-26	Division 1 shall provide annunciation via the HMI when 2oo4 annunciate votes for ADS high drywell pressure bypass timer initiated.	NUREG 0737, IEEE 279	
ADS-FR-27	Division 3 shall provide annunciation via the HMI when 2oo4 annunciate votes for ADS high drywell pressure bypass timer initiated.	NUREG 0737, IEEE 279	
ADS-FR-28	Each channel shall bypass the DHP input when the 450 second timer has expired.	NUREG 0737, IEEE 279	
ADS-FR-29	Each channel shall reset the 450 second timer if the RWL1 input drops below setpoint before the timer times out and shall provide a vote to not annunciate to each division.	NUREG 0737	
ADS-FR-30	Each channel shall seal in the RWL1 and DHP inputs when 117 second timer has expired.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-31	When the timer expires, Channel A shall provide a vote to initiate ADS to each division when CSDPA input exceeds setpoint high **or** RDPA input exceeds setpoint high **or** RDPC exceeds setpoint high.	Project design approach	
ADS-FR-32	When the timer expires, Channel B shall provide a vote to initiate ADS to each division when CSDPB input exceeds setpoint high **or** RDPB input exceeds setpoint high **or** RDPD exceeds setpoint high.	Project design approach	

ADS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/ADS Requirement Revised**	**PPS/ADS Source / Basis**	**Notes / Clarification**
ADS-FR-33	When the timer expires, Channel C shall provide a vote to initiate ADS to each division when CSDPC input exceeds setpoint high **or** RDPA input exceeds setpoint high **or** RDPC exceeds setpoint high.	Project design approach	
ADS-FR-34	When the timer expires, Channel D shall provide a vote to initiate ADS to each division when CSDPD input exceeds setpoint high **or** RDPB input exceeds setpoint high **or** RDPB exceeds setpoint high.	Project design approach	
ADS-FR-35	Channel A shall provide a condition vote to Division 1 when RDPA exceeds setpoint.	Project design approach	
ADS-FR-36	Channel A shall provide a condition vote to Division 1 when CSDPA exceeds setpoint.	Project design approach	
ADS-FR-37	Channel B shall provide a condition vote to Division 3 when RDPB exceeds setpoint.	Project design approach	
ADS-FR-38	Channel B shall provide a condition vote to Division 3 when CSDPB exceeds setpoint.	Project design approach	
ADS-FR-39	Channel C shall provide a condition vote to Division 1 when RDPC exceeds setpoint.	Project design approach	
ADS-FR-40	Channel C shall provide a condition vote to Division 1 when CSDPC exceeds setpoint.	Project design approach	
ADS-FR-41	Channel D shall provide a condition vote to Division 3 when RDPD exceeds setpoint.	Project design approach	
ADS-FR-42	Channel D shall provide a condition vote to Division 3 when CSDPD exceeds setpoint.	Project design approach	
ADS-FR-43	Division 1 shall initiate an ADS output signal when 2oo4 votes to initiate ADS are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-44	The Division 1 ADS output signal shall energize the 125VDC "A" solenoid on each of five (5) SRVs.	Original deign feature	
ADS-FR-45	Division 1 shall provide annunciation via the HMI when the ADS sealed in trip condition is satisfied.	IEEE Std. 603/IEEE Std. 7-4.3.2	

ADS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/ADS Requirement Revised**	**PPS/ADS Source / Basis**	**Notes / Clarification**
ADS-FR-46	Division 1 shall provide indicating light capability via the HMI to indicate that the "A" solenoid for each of five (5) SRVs is **NOT** energized.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-47	Division 1 shall provide indicating light capability via the HMI to indicate that each of five (5) SRVs is in a closed position when the ADS is **NOT** in a sealed in trip condition.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-48	Division 3 shall initiate an ADS output signal when 2oo4 votes to initiate ADS are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-49	The Division 3 ADS output signal shall energize the 125VDC "B" solenoid on each of five (5) SRVs.	Original deign feature	
ADS-FR-50	Division 3 shall provide annunciation via the HMI when the ADS sealed in trip condition is satisfied.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-51	Division 3 shall provide indicating light capability via the HMI to indicate that the "B" solenoid for each of five (5) SRVs is **NOT** energized.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-52	Division 3 shall provide indicating light capability via the HMI to indicate that each of five (5) SRVs is in a closed position when the ADS is **NOT** in a sealed in trip condition.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-53	Each division shall include a manual ADS initiation feature that requires two distinct actions (e.g. arming prior to functioning) to be completed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-54	Each division shall provide annunciation via the HMI upon completing the first distinct switch action.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-55	Each division shall complete the manual ADS initiation by performing the second distinct switch action.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-56	Each division manual ADS initiation shall bypass all channel timer functions.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-57	Each division manual ADS initiation shall seal in.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-58	Each division shall provide annunciation via the HMI when the ADS manual initiation is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	

ADS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/ADS Requirement Revised**	**PPS/ADS Source / Basis**	**Notes / Clarification**
ADS-FR-59	Division 1 shall initiate an ADS output signal when the ADS manual initiation is sealed in **AND** 1oo1 condition votes for CSDPA input **AND** 1oo1 condition votes for CSDPC input are received.	GDC 13, GDC 35, Reg Guide 1.47, Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-60	Division 1 shall initiate an ADS output signal when the ADS manual initiation is sealed in **AND** 1oo1 condition votes for RDPA input are received.	GDC 13, GDC 35, Reg Guide 1.47, Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-61	Division 1 shall initiate an ADS output signal when the ADS manual initiation is sealed in **AND** 1oo1 condition votes for RDPC input are received.	GDC 13, GDC 35, Reg Guide 1.47, Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-62	The Division 1 manual ADS output signal shall energize the 125VDC "A" solenoid on each of five (5) SRVs.	GDC 13, GDC 35, Reg Guide 1.47, Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-63	Division 3 shall initiate an ADS output signal when the ADS manual initiation is sealed in **AND** 1oo1 condition votes for CSDPB input **AND** 1oo1 condition votes for CSDPD input are received.	GDC 13, GDC 35, Reg Guide 1.47, Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-64	Division 3 shall initiate an ADS output signal when the ADS manual initiation is sealed in **AND** 1oo1 condition votes for RDPB input are received.	GDC 13, GDC 35, Reg Guide 1.47, Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-65	Division 3 shall initiate an ADS output signal when the ADS manual initiation is sealed in **AND** 1oo1 condition votes for RDPD input are received.	GDC 13, GDC 35, Reg Guide 1.47, Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-66	The Division 3 manual ADS output signal shall energize the 125VDC "B" solenoid on each of five (5) SRVs.	GDC 13, GDC 35, Reg Guide 1.47, Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-67	Each division shall provide a manual inhibit feature to preclude the initiation of ADS actuation.	GDC 13, NUREG 0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-68	Each division shall provide annunciation via the HMI when the inhibit feature is in force.	IEEE Std. 603/IEEE Std. 7-4.3.2	

ADS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/ADS Requirement Revised**	**PPS/ADS Source / Basis**	**Notes / Clarification**
ADS-FR-69	The inhibit feature shall not be capable of defeating the ADS actuation if initiation logic is sealed in.	Original design feature	
ADS-FR-70	Each division shall provide a manual reset feature that simultaneously resets the channels and voting logic, thereby removing the ADS output signal from the actuated SRVs.	GDC 13, Reg Guide 1.62 IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-71	The reset of both divisions shall be required to enable the actuated SRVs to return to the normal (closed) position.	Original design feature	
ADS-FR-72	Division 3 shall include soft controls to support manually overriding the automatic actuation function and individually energize the solenoid "B" on each ADS SRV.	GDC 13, GDC 35, Reg Guide 1.47, Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	This switch exists at Panel 631 in the AER. This will be migrated to an HMI interface via soft controls.
ADS-FR-73	Division 1 shall include soft controls to support manually overriding the automatic actuation function and individually energize the “A” solenoid on each ADS SRV.	GDC 19, Reg Guide 1.62 and IEEE Std. 603/IEEE Std. 7-4.3.2	This switch is identified on drawing M-1-B21-1060-E-004 but is not described in L-S-31.
ADS-FR-74	Division 1 shall include soft controls to support manually energizing the solenoid on each of nine (9) non-ADS SRVs.	GDC 19, Reg Guide 1.62 and IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-75	Each division shall provide the means to functionally test during normal plant operation without initiating an inadvertent protective action.	GDC 12, GDC 37, Reg Guide 1.22, Reg Guide 1.105, Reg Guide 1.118, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-76	An ADS initiation by either division shall result in the SRVs being actuated.	Original design feature	
ADS-FR-77	The PPS/ADS shall interface with a 125 VDC power source to support actuation of the SRVs.	GDC 22	
ADS-FR-78	Each division shall be capable of being powered by 125VDC power.	GDC 22	
ADS-FR-79	Each division shall be clearly identified to reduce the possibility of personnel causing inadvertent trips or undesired operating conditions.	IEEE Std. 603/IEEE Std. 7-4.3.2	

ADS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/ADS Requirement Revised**	**PPS/ADS Source / Basis**	**Notes / Clarification**
ADS-FR-80	All physical switches and soft controls shall provide both electrical and physical separation between the divisions for the PPS/ADS.	GDC 24, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-81	Failure of a single channel (sensor and associated equipment) shall not prevent normal protective action of the safety system.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-82	Failure of a single system component shall neither prevent normal protective action of the safety system nor result in an inadvertent actuation.	IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-83	Redundant sensor circuits associated with each trip system (sensors, wiring, transmitter, amplifier. etc.) shall be electrically, mechanically, and physically independent so that they are unlikely to be disabled by a common cause.	GDC 21, GDC 23, Reg Guide 1.53, IEEE Std. 603/IEEE Std. 7-4.3.2	
ADS-FR-84	Each channel and each division shall provide sufficient features and documented evaluations to support elimination of most Technical Specification Surveillance Tests, and minimize the requirements for manual calibration checks.	Project design approach	
ADS-FR-85	For all PPS inputs that have the potential to require manual test insertion or external measurement of input values (i.e., use of an external digital multi meter by a technician), test jacks are provided in the cabinets.	Project design approach	
ADS-FR-86	For all inputs that have the potential to require manual multi-point calibration checks with external calibration equipment, knife edge disconnects along with test jacks are incorporated in the field termination panels.	Project design approach	

E

E.1 CS Design Requirements

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-1	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. 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. 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.	GDC 1 - Quality standards and records
CS-DR-2	Structures, systems, and components important to safety shall be designed to withstand the effect of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions.	GDC 2 - Design Bases for Protection Against Natural Phenomena
CS-DR-3	Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions.	GDC 3 - Fire protection
CS-DR-4	Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents (LOCAs).	GDC 4 - Environmental and dynamic effects design bases
CS-DR-5	The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.	GDC 10 - Reactor design

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-6	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.	GDC 13 - Instrumentation and control
CS-DR-7	A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. 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 I&C 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.	GDC 19 - Control Room
CS-DR-8	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.	GDC 20 - Protection system functions

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-9	The protection system shall be designed for high functional reliability and in-service 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.	GDC 21 - Protection system reliability and testability
CS-DR-10	The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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.	GDC 22- Protection system independence
CS-DR-11	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.	GDC 23 - Protection system failure modes
CS-DR-12	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.	GDC 24 - Separation of protection and control systems

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-13	The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.	GDC 29 - Protection against anticipated operational occurrences
CS-DR-14	A system to supply reactor coolant makeup for protection against small breaks in the reactor coolant pressure boundary shall be provided. The system safety function shall be to assure that specified acceptable fuel design limits are not exceeded as a result of reactor coolant loss due to leakage from the reactor coolant pressure boundary and rupture of small piping or other small components which are part of the boundary. The system shall be designed to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished using the piping, pumps, and valves used to maintain coolant inventory during normal reactor operation.	GDC 33 - Reactor Coolant Makeup
CS-DR-15	A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts.	GDC 35 - Emergency Core Cooling
CS-DR-16	The emergency core cooling system shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leak tight integrity of its components, (2) the operability and performance of the active components of the system, and (3) the operability of the system as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.	GDC 37 - Testing of Emergency Core Cooling System

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-17	The protection system shall be designed to permit periodic testing of its initiation functions inclusive of the actuation devices and actuated equipment when the reactor is in operation.	Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions (Safety Guide 22)
CS-DR-18	Those structures, systems, and components (SSC) that should be designed to remain functional if the Safe Shutdown Earthquake (SSE) occurs shall be designated as Seismic Category I. (This includes Systems or portions of systems that are required for reactor shutdown; all electric and mechanical devices and circuitry between the process and the input terminals of the actuator systems involved in generating signals that initiate protective action; systems or portions of systems that are required for (1) monitoring of systems important to safety and (2) actuation of systems important to safety.)	Regulatory Guide 1.29 - Seismic Design Classification
CS-DR-19	The CS shall comply with the requirements of Appendix B to 10 CFR Part 50 for the installation, inspection, and testing of nuclear power plant instrumentation and electric equipment.	Regulatory Guide 1.30 - Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment (Safety Guide 30)
CS-DR-20	The CS shall meet the requirements for design, operation and testing of safety-related power systems within nuclear power plants as defined within IEEE Std. 308.	Regulatory Guide 1.32 - Criteria for Power Systems for Nuclear Power Plants
CS-DR-21	The CS shall meet the requirements for indicating the bypass or inoperable status of portions of the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the system it actuates to perform their safety-related functions:	Regulatory Guide 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
CS-DR-22	The CS shall comply with the IEEE Std. 279 requirement that any single failure within the protection system shall not prevent proper protective action at the system level when required, by utilizing the guidance in IEEE Std. 379-1972 for applying the single-failure criterion to the design and analysis of nuclear power plant protection systems.	Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Safety Systems

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-23	The CS shall provide a means for manual initiation of protective actions.	Regulatory Guide 1.62 - Manual Initiation of Protective Actions
CS-DR-24	The CS shall meet the requirements for physical independence of the circuits and electric equipment comprising or associated with the Class 1E power system, the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety related functions.	Regulatory Guide 1.75 - Physical Independence of Electric Systems
CS-DR-25	The CS shall comply with design verification requirements to verify adequacy of design under the most adverse design conditions.	Regulatory Guide 1.89 - Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants
CS-DR-26	The CS shall comply with the requirement to: (1) provide information required to permit the operator to take preplanned manual actions to accomplish safe plant shutdown; (2) determine whether the reactor trip, engineered safety feature systems, and manually initiated safety systems and other systems important to safety are performing their intended functions (i.e., reactivity control, core cooling, maintaining reactor coolant system integrity, and maintaining containment integrity); (3) provide information to the operators that will enable them to determine the potential for causing a gross breach of the" barriers to radioactivity release (i.e., fuel cladding, reactor coolant pressure boundary, and containment) and to determine if a gross breach of a barrier has occurred.	Regulatory Guide 1.97 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants
CS-DR-27	The CS shall comply with design verification requirements to verify the seismic adequacy of electric equipment.	Regulatory Guide 1.100 - Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-28	The CS shall design shall implement setpoints that assure sufficient margin between Technical Specification limits and the trip setpoint to account for instrument inaccuracy, calibration uncertainties and instrument drift. Consideration of instrument span and range as well as environmental influences must be included.	Regulatory Guide 1.105 - Instrument Setpoint
CS-DR-29	The CS shall comply with the requirements for periodic testing of electric power and protection systems.	Regulatory Guide 1.118 - Periodic Testing of Electric Power and Protection Systems
CS-DR-30	The CS shall, with precision and reliability, energize pumps and align valves to cool the fuel by spraying water on the core.	IEEE Std. 603, Section 5.0 Safety System Criteria and 6.1 Automatic Control
CS-DR-31	The CS shall initiate when the monitored plant parameter exceeds the following trip setpoint: Reactor Vessel Water Level 1 < -129 inches Drywell Pressure > 1.68 psig Reactor Vessel Pressure < 455 psig	IEEE Std. 603, Section 6.1 Automatic Control
CS-DR-32	The CS signal input to actuation output propagation time shall be less than 100 milliseconds.	IEEE Std. 603, Section 4.10
CS-DR-33	The CS shall be capable of initiating under all required modes of reactor operation.	IEEE Std. 603, Section 4.1
CS-DR-34	The CS shall ensure that the protective action, once started, continues to completion.	IEEE Std. 603, Section 5.2 Completion of Protective Action
CS-DR-35	Any single failure within the CS shall not prevent proper protective action at the system level when required.	IEEE Std. 603, Section 5.1 Single Failure Criterion and IEEE Std. 7-4.3.2 Section 5.1 Single Failure Criterion

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-36	Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.	IEEE Std. 603 section 5.3 Quality and IEEE Std. 7-4.3.2 section 5.3 Quality
CS-DR-37	Type test data or reasonable engineering extrapolation based on test data shall be available to verify that protection system equipment shall meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements.	IEEE Std. 603 section 5.4 Equipment Qualification and IEEE Std. 7-4.3.2 section 5.4 Equipment Qualification
CS-DR-38	All protection system channels shall be designed to maintain necessary functional capability under extremes of conditions (as applicable) relating to environment, energy supply, malfunctions and accidents.	IEEE Std. 603 section 5.5 System Integrity and IEEE Std. 7-4.3.2 and section 5.5 Independence
CS-DR-39	Channels that provide signals for the same protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 System Integrity
CS-DR-40	Any equipment that is used for both protective and control functions shall be classified as part of the protection system and shall meet all the applicable requirements.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence
CS-DR-41	The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system and shall meet all the applicable requirements. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-42	Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
CS-DR-43	Provisions shall be included so that the protective action can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
CS-DR-44	Where a credible single event can cause a control system action that results in a condition requiring protective action and can concurrently prevent the protective action from those protection system channels designated to provide principal protection against the condition, then alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design bases.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
CS-DR-45	To the extent feasible and practical, protection system inputs shall be derived from signals that are direct measures of the desired variables.	IEEE Std. 603 section 6.4 Derivation of System Inputs
CS-DR-46	Means shall be provided for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
CS-DR-47	Capability shall be provided for testing and calibrating channels and the devices used to derive the final system output signal from the various channel signals.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
CS-DR-48	For those parts of the system where the required interval between testing will be less than the normal time interval between generating station shutdowns, there shall be capability for testing during power operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-49	The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective action at the systems level.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
CS-DR-50	During such operation, the active parts of the system shall of themselves continue to meet the single failure criterion.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
CS-DR-51	Where operating requirements necessitate automatic or manual bypass of a protective function, the design shall be such that the bypass will be removed automatically whenever permissive conditions are not met.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
CS-DR-52	Devices used to achieve automatic removal of the bypass of a protective function are part of the protection system and shall be designed in accordance with these criteria.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
CS-DR-53	If the protective action of some part of the system has been bypassed or deliberately rendered inoperative for any purpose, this fact shall be continuously indicated in the control room.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
CS-DR-54	The design shall permit the administrative control of the means for manually bypassing channels or protective functions.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
CS-DR-55	Where it is necessary to change to a more restrictive set point to provide adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of assuring that the more restrictive set point is used.	IEEE Std. 603 section 6.8 Setpoints
CS-DR-56	The devices used to prevent improper use of less restrictive set points shall be considered a part of the protection system and shall be designed in accordance with the other provisions of these criteria regarding performance and reliability.	IEEE Std. 603 section 6.8 Setpoints
CS-DR-57	The protection system shall be so designed that, once initiated, a protective action at the system level shall go to completion.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-58	Return to operation shall require subsequent deliberate operator action.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action
CS-DR-59	The protection system shall include means for manual initiation of each protective action at the system level (for example, reactor trip, containment isolation, safety injection, core spray, etc).	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
CS-DR-60	No single failure within the manual, automatic, or common portions of the protection system shall prevent initiation of protective action by manual or automatic means.	IEEE Std. 603 section 7.2 Manual Control
CS-DR-61	Manual initiation should depend upon the operation of a minimum of equipment.	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
CS-DR-62	The design shall permit the administrative control of access to all set point adjustments, module calibration adjustments, and test points.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
CS-DR-63	Protective actions shall be indicated and identified down to the channel level.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
CS-DR-64	The protection system shall be designed to provide the operator with accurate, complete, and timely information pertinent to its own status and to generating station safety.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
CS-DR-65	The design shall minimize the development of conditions which would cause meters, annunciators, recorders, alarms, etc, to give anomalous indications confusing to the operator.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
CS-DR-66	The system shall be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.	IEEE Std. 603 section 5.10 Repair

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-67	In order to provide assurance that the requirements given in this document can be applied during the design, construction, maintenance, and operation of the plant, the protection system equipment (for example, interconnecting wiring, components, modules, etc), shall be identified distinctively as being in the protection system.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
CS-DR-68	This identification shall distinguish between redundant portions of the protection system. (In the installed equipment, components, or modules mounted in assemblies that are clearly identified as being in the protection system do not themselves require identification.) All software, firmware, and programmable logic shall be identified in accordance with IEEE Std. 7-4.3.2 Clause 5.11.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
CS-DR-69	CS shall conform to the design criteria and features for Class 1E electric systems to ensure that functional requirements under the conditions produced by design basis events are met.	IEEE Std. 308 - Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations
CS-DR-70	CS shall conform to the methods for demonstrating the qualification of Class 1E equipment including components or equipment of any interface whose failure could adversely affect the performance of Class 1E systems and electronic equipment.	IEEE Std. 323 - Qualifying Class 1E Equipment for Nuclear Power Generating Stations
CS-DR-71	CS shall conform to the design and operational criteria for the performance of periodic testing of nuclear power generating station safety systems.	IEEE Std. 338 - Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems
CS-DR-72	CS shall meet its Class 1E performance requirements during and following one SSE (safe shutdown earthquake) preceeded by a number of OBEs (operating basis earthquakes).	IEEE Std. 344 - Guide for Seismic Qualification of Class 1 Electric Equipment for Nuclear Power Generating Stations
CS-DR-73	CS shall meet the single failure criterion as described and classified in IEEE Std. 379.	IEEE Std. 379 - Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

CS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
CS-DR-74	CS shall meet the criteria and requirements for establishing and maintaining the independence of Class 1E equipment and circuits and auxiliary supporting features by physical separation and electrical isolation.	IEEE Std. 384 - Criteria for Independence of Class 1E Equipment and Circuits

E.2 CS Functional Requirements

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-1	PPS/CS shall be capable of providing signals to start pumps and align valves for delivering water to the reactor as well as to initiate other SR equipment either automatically when any of the monitored parameters exceeds a pre-established value, or by manual initiation.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-2	PPS/CS shall be comprised of four (4) independent and separate divisions (Division 1, Division 2, Division 3, and Division 4)	GDC 22, Reg Guide 1.53, Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-3	Each division shall be capable of being powered by 125VDC power.	Original design feature	
CS-FR-4	Each division shall provide outputs that are capable of interfacing with 120VAC loads.	Original design feature	
CS-FR-5	PPS/CS shall have four (4) independent channels (Channel A, Channel B, Channel C and Channel D) that each provide votes / signals to each of the divisions.	GDC 22, Reg Guide 1.53, Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	The four channels are common to each of the divisions.
CS-FR-6	Each channel shall receive an input from each of the following monitored parameters that are provided as common inputs to the PPS platform and are shared by each of the PPS functions: • Reactor Vessel Low Water Level (Level 1) (RWL 1) • Drywell High Pressure (DHP) • Reactor Low Pressure (RLP)	GDC 13, GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-7	Channel A and Channel B shall receive additional 4-20mA inputs from the associated monitored parameters: • CS Loop Flow (CSF1) • CS Loop Flow (CSF2) • CS Loop Discharge Pressure (CSP)	Original design feature	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-8	Channel A shall receive an additional 4-20mA input from the associated monitored parameter: • CS DP (CSDP)	Original design feature	
CS-FR-9	Each channel shall receive the following contact inputs: • Power available at the associated CS pump motor bus (CI1) • Associated EDG breaker closes. (CI2) • Associated E21-F001 LS12 (CI6) (qty 2) • Associated CS pump motor auto trip (CI7) (qty 2) • Associated CS pump breaker not in operate position (CI8) (qty 2) • Associated CS pump motor overcurrent (CI9) • Associated CS pump motor breaker in operating position (CI10)	Original design feature	
CS-FR-10	Channel C and Channel D shall receive the following additional contact inputs: • Associated CS pump running (CI3) • Associated E21-F001 49X (CI11) (qty 2)	Original design feature	
CS-FR-11	Channel A and Channel B shall receive the following additional contact inputs: • Associated CS pump motor breaker auxiliary switch (CI4) • Associated Outboard Injection valve limit switch (CI5)	Original design feature	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-12	Each input to a channel (ma or contact input) shall be voted on by the channel based on the condition (condition met or not met).	Project design approach	The term "shall be voted on" indicates that the channel performs a bi-stable comparison against a pre-determined configurable setpoint to determine whether the input is at or above/below the setpoint value.
CS-FR-13	Each channel shall provide the status of the vote (e.g. vote to not function if condition not met; vote to function if condition met) to each of the divisions.	Project design approach	
CS-FR-14	Each division shall determine whether the votes to function for each type of input satisfy the voting criteria (e.g. 2oo4).	Project design approach	
CS-FR-15	Each division shall execute a function when the voting criteria is satisfied.	Project design approach	As an example, the RWL1 input to Channels A, B, C and D shall be sent to a 2oo4 voter in each of the divisions (Division 1, Division 2, Division 3 and Division 4). When at least two of the four RWL1 inputs to the 2oo4 voter are satisfied, the associated division generates an output. The generated output may be dependent on additional voting to be satisfied. Some outputs require different voting schemes which are described within the requirement.
CS-FR-16	Each input to a channel shall have an associated voter (e.g. 2oo4) within each division to ensure that trip inputs are voted separately.	Project design approach	
CS-FR-17	Each channel shall provide a vote for LOCA signal to each division when RWL1 input reaches setpoint.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-18	Each channel shall provide a vote for LOCA signal to each division when DHP input and RLP input reach setpoint	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-19	Each channel shall provide a vote to actuate to each division when RLP input reaches setpoint.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-20	Each channel shall include a manual CS initiation feature located in the control room that requires two distinct actions (e.g. arming prior to functioning) to be completed.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-21	Channel A shall provide a status to annunciate to Division 1 upon the first distinct action for the associated manual CS initiation feature being satisfied.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-22	Channel B shall provide a status to annunciate to Division 2 upon the first distinct action for the associated manual CS initiation feature being satisfied.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-23	Channel C shall provide a status to annunciate to Division 3 upon the first distinct action for the associated manual CS initiation feature being satisfied.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-24	Channel D shall provide a status to annunciate to Division 4 upon the first distinct action for the associated manual CS initiation feature being satisfied.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-25	Division 1 shall provide annunciation via the HMI when annunciate status is received for the first distinct action for the manual CS initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-26	Division 2 shall provide annunciation via the HMI when annunciate status is received for the first distinct action for the manual CS initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-27	Division 3 shall provide annunciation via the HMI when annunciate status is received for the first distinct action for the manual CS initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-28	Division 4 shall provide annunciation via the HMI when annunciate status is received for the first distinct action for the manual CS initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-29	Channel A shall provide a vote for manual initiation to Division 1 on the second distinct action being satisfied.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-30	Channel B shall provide a vote for manual initiation to Division 2 on the second distinct action being satisfied.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-31	Channel C shall provide a vote for manual initiation to Division 3 on the second distinct action being satisfied.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-32	Channel D shall provide a vote for manual initiation to Division 4 on the second distinct action being satisfied.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-33	Each channel shall seal in the RWL1, DHP/RLP and manual initiation inputs until manually reset.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-34	Division 1 shall provide a signal to start Emergency Diesel Generator A (EDGA) when 2oo4 LOCA votes for RWL1 input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-35	Division 1 shall provide a signal to start EDGA when 2oo4 LOCA votes for DHP / RLP input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-36	Division 1 shall provide a signal to start EDGA when 1oo1 votes are received for the second distinct action for the manual CS initiation.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-37	Division 1 shall provide two (2) outputs (one to EDGA 4kV breaker control and one to EDGA undervoltage logic circuits at the Safeguard Bus) when 2oo4 LOCA votes for RWL1 input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-38	Division 1 shall provide two (2) outputs (one to EDGA 4kV breaker control and one to EDGA undervoltage logic circuits at the Safeguard Bus) when 2oo4 LOCA votes for DHP / RLP input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-39	Division 1 shall provide two (2) outputs (one to EDGA 4kV breaker control and one to EDGA undervoltage logic circuits at the Safeguard Bus) when 1oo1 votes are received for the second distinct action for the manual CS initiation.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-40	Division 2 shall provide a signal to start EDGB when 2oo4 LOCA votes for RWL1 input are received	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-41	Division 2 shall provide a signal to start EDGB when 2oo4 LOCA votes for DHP / RLP input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-42	Division 2 shall provide a signal to start EDGB when 1oo1 votes are received for the second distinct action for the manual CS initiation.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-43	Division 2 shall provide two (2) outputs (one to EDGB 4kV breaker control and one to EDGB undervoltage logic circuits at the Safeguard Bus) when 2oo4 LOCA votes RWL1 input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-44	Division 2 shall provide two (2) outputs (one to EDGB 4kV breaker control and one to EDGB undervoltage logic circuits at the Safeguard Bus) when 2oo4 LOCA votes for DHP / RLP input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-45	Division 2 shall provide two (2) outputs (one to EDGB 4kV breaker control and one to EDGB undervoltage logic circuits at the Safeguard Bus) when 1oo1 votes are received for the second distinct action for the manual CS initiation.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-46	Division 3 shall provide a signal to start EDGC when 2oo4 LOCA votes for RWL1 input are received	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-47	Division 3 shall provide a signal to start EDGC when 2oo4 LOCA votes for DHP / RLP input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-48	Division 3 shall provide a signal to start EDGC when 1oo1 votes are received for the first distinct action for the manual CS initiation.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-49	Division 3 shall provide two (2) outputs (one to EDGC 4kV breaker control and one to EDGC undervoltage logic circuits at the Safeguard Bus) when 2oo4 LOCA votes RWL1 input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-50	Division 3 shall provide two (2) outputs (one to EDGC 4kV breaker control and one to EDGC undervoltage logic circuits at the Safeguard Bus) when 2oo4 LOCA votes for DHP / RLP input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-51	Division 3 shall provide two (2) outputs (one to EDGC 4kV breaker control and one to EDGC undervoltage logic circuits at the Safeguard Bus) when 1oo1 votes are received for the second distinct action for the manual CS initiation.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-52	Division 4 shall provide a signal to start EDGD when 2oo4 LOCA votes for RWL1 input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-53	Division 4 shall provide a signal to start EDGD when 2oo4 LOCA votes for DHP / RLP input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-54	Division 4 shall provide a signal to start EDGD when 1oo1 votes are received for the first distinct action for the manual CS initiation.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-55	Division 4 shall provide two (2) outputs (one to EDGD 4kV breaker control and one to EDGD undervoltage logic circuits at the Safeguard Bus) when 2oo4 LOCA votes RWL1 input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-56	Division 4 shall provide two (2) outputs (one to EDGD 4kV breaker control and one to EDGD undervoltage logic circuits at the Safeguard Bus) when 2oo4 LOCA votes for DHP / RLP input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-57	Division 4 shall provide two (2) outputs (one to EDGD 4kV breaker control and one to EDGD undervoltage logic circuits at the Safeguard Bus) when 1oo1 votes are received for the second distinct action for the manual CS initiation.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-58	Each division and channel shall be capable of being manually reset.	Original design capability	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-59	Channel A shall provide a start vote to Division 1 after a 10 second time delay if CI1 is satisfied (contact closed).	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-60	Division 1 shall provide a signal to start CS Pump "A" when 2oo4 LOCA votes for RWL1 input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-61	Division 1 shall provide a signal to start CS Pump "A" when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-62	Division 1 shall provide a signal to start CS Pump "A" when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-63	Channel C shall provide a start vote to Division 3 after a 10 second time delay if CI1 is satisfied (contact closed).	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-64	Division 3 shall provide a signal to start CS Pump "C" when 2oo4 LOCA votes for RWL1 input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-65	Division 3 shall provide a signal to start CS Pump "C" when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-66	Division 3 shall provide a signal to start CS Pump "C" when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-67	Channel B shall provide a start vote to Division 2 after a 15 second time delay if CI1 is satisfied (contact closed).	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-68	Division 2 shall provide a signal to start CS Pump "B" when 2oo4 LOCA votes for RWL1 input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-69	Division 2 shall provide a signal to start CS Pump "B" when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-70	Division 2 shall provide a signal to start CS Pump "B" when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-71	Channel D shall provide a start vote to Division 4 after a 15 second time delay if CI1 is satisfied (contact closed).	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-72	Division 4 shall provide a signal to start CS Pump "D" when 2oo4 LOCA votes for RWL1 input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-73	Division 4 shall provide a signal to start CS Pump "D" when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-74	Division 4 shall provide a signal to start CS Pump "D" when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-75	Channel A shall provide a start vote to Division 1 after a 7 second time delay if CI2 is satisfied (contact closed).	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-76	Division 1 shall provide a signal to start CS Pump "A" when 2oo4 LOCA votes for RWL1 input are received **AND** a 1oo1 start vote for CI2 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-77	Division 1 shall provide a signal to start CS Pump "A" when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI2 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-78	Division 1 shall provide a signal to start CS Pump "A" when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** a 1oo1 start vote for CI2 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-79	Channel B shall provide a start vote to Division 2 after a 7 second time delay if CI2 is satisfied (contact closed).	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-80	Division 2 shall provide a signal to start CS Pump "B" when 2oo4 LOCA votes for RWL1 input are received **AND** a 1oo1 start vote for CI2 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-81	Division 2 shall provide a signal to start CS Pump "B" when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI2 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-82	Division 2 shall provide a signal to start CS Pump "B" when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** a 1oo1 start vote for CI2 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-83	Channel C shall provide a start vote to Division 3 after a 7 second time delay if CI2 is satisfied (contact closed).	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-84	Division 3 shall provide a signal to start CS Pump "C" when 2oo4 LOCA votes for RWL1 input are received **AND** a 1oo1 start vote for CI2 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-85	Division 3 shall provide a signal to start CS Pump "C" when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI2 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-86	Division 3 shall provide a signal to start CS Pump "C" when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** a 1oo1 start vote for CI2 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-87	Channel D shall provide a start vote to Division 4 after a 7 second time delay if CI2 is satisfied (contact closed).	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-88	Division 4 shall provide a signal to start CS Pump "D" when 2oo4 LOCA votes for RWL1 input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-89	Division 4 shall provide a signal to start CS Pump "D" when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-90	Division 4 shall provide a signal to start CS Pump "D" when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** a 1oo1 start vote for CI1 is received.	GDC 20, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-91	Each division and associated channel shall be required to be manually reset, from any prior trip, in order to generate a manual or automatic start signal to the associated CS pump.	Original design feature	
CS-FR-92	Each division shall provide a means to manually start or stop the associated CS pump by providing a signal to the CS pump control circuit.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-93	Channel A shall provide a vote to annunciate to Division 1 when CI10 is satisfied (contact closed).	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-94	Division 1 shall provide annunciation via the HMI when 1oo1 annunciate votes are received for the CI10 input.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-95	Channel B shall provide a vote to annunciate to Division 2 when CI10 is satisfied (contact closed).	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-96	Division 2 shall provide annunciation via the HMI when 1oo1 annunciate votes are received for the CI10 input.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-97	Channel C shall provide a vote to annunciate to Division 3 when CI10 is satisfied (contact closed).	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-98	Division 3 shall provide annunciation via the HMI when 1oo1 annunciate votes are received for the CI10 input.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-99	Channel D shall provide a vote to annunciate to Division 4 when CI10 is satisfied (contact closed).	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-100	Division 4 shall provide annunciation via the HMI when 1oo1 annunciate votes are received for the CI10 input.	IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-101	Each division shall include interlocks to allow the associated CS Pump to be manually placed in "Stop" in the presence of an automatic start signal to the CS pump.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-102	Each division shall provide indicating light capability via the HMI when the associated CS Pump is placed in "Stop" in the presence of an automatic start signal to the CS pump.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-103	Each division shall allow the CS pump to be momentarily started by manually placing the associated CS Pump in "Start". (Note that this momentarily overrides the stop interlock of an automatic start signal to the CS pump.)	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-104	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E21-F004A or terminate valve motion midstream from the control room.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-105	Division 1 shall provide a signal to open valve E21-F004A when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 13, GDC 20, GDC 29, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-106	Division 1 shall provide a signal to open valve E21-F004A when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 13, GDC 20, GDC 29, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-107	Division 1 shall provide a signal to open valve E21-F004A when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 13, GDC 20, GDC 29, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-108	Division 1 shall provide an interlock to prevent valve E21-F004A from being manually closed when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 21, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-109	Division 1 shall provide an interlock to prevent valve E21-F004A from being manually closed when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 21, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-110	Division 1 shall provide an interlock to prevent valve E21-F004A from being manually closed when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 21, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-111	Division 1 shall provide valve E21-F004A position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-112	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E21-F005 or terminate valve motion midstream from the control room.	Reg Guide 1.22, Reg Guide 1.62, GDC 21, GDC 37, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-113	Division 1 shall provide valve E21-F005 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-114	Division 1 shall provide a signal to open valve E21-F005 when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 13, GDC 20, GDC 29, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-115	Division 1 shall provide a signal to open valve E21-F005 when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 13, GDC 20, GDC 29, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-116	Division 1 shall provide a signal to open valve E21-F005 when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	GDC 13, GDC 20, GDC 29, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-117	Division 1 shall provide an override to manually close valve E21-F005 from the control room when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-118	Division 1 shall provide indicating light capability via the HMI when a manual signal to close valve E21-F005 is initiated when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-119	Division 1 shall provide an override to manually close valve E21-F005 from the control room when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-120	Division 1 shall provide indicating light capability via the HMI when a manual signal to close valve E21-F005 is initiated when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-121	Division 1 shall provide an override to manually close valve E21-F005 from the control room when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-122	Division 1 shall provide indicating light capability via the HMI when a manual signal to close valve E21-F005 is initiated when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-123	Channel A shall provide a vote to interlock to Division 1 if CI5 is satisfied (contact open).	Project design approach	
CS-FR-124	Division 1 shall provide an interlock to prevent valve E21-F005 from being manually opened when 2oo4 LOCA votes for RWL1 input are received **AND** a 1oo1 start vote for CI1 is received.	Original design feature	
CS-FR-125	Division 1 shall provide an interlock to prevent valve E21-F005 from being manually opened when 1oo1 votes are received for the second distinct action for the manual CS initiation is received **AND** a 1oo1 start vote for CI1 is received.	Original design feature	
CS-FR-126	Division 1 shall provide an interlock to prevent valve E21-F005 from being manually opened when a 1oo1 interlock vote for CI5 is received.	Original design feature	
CS-FR-127	Division 1 shall provide an interlock to prevent valve E21-F005 from opening, if closed, when valve E21-F004A and the Division 1 initiation logic are being tested when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 21, GDC 35	
CS-FR-128	Division 1 shall provide an interlock to prevent valve E21-F005 from opening, if closed, when valve E21-F004A and the Division 1 initiation logic are being tested when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 21, GDC 35	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-129	Division 1 shall provide an interlock to prevent valve E21-F005 from opening, if closed, when valve E21-F004A and the Division 1 initiation logic are being tested when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	GDC 21, GDC 35	
CS-FR-130	Once valve E21-F005 has been manually closed after already being automatically opened, Division 1 shall provide an interlock that prevents the valve from being opened unless 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-131	Once valve E21-F005 has been manually closed after already being automatically opened, Division 1 shall provide an interlock that prevents the valve from being opened unless 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-132	Once valve E21-F005 has been manually closed after already being automatically opened, Division 1 shall provide an interlock that prevents the valve from being opened unless 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-133	Once valve E21-F005 has been manually closed, trip system Division 1 shall provide an interlock that prevents the valve from automatically opening when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-134	Once valve E21-F005 has been manually closed, trip system Division 1 shall provide an interlock that prevents the valve from automatically opening when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-135	Once valve E21-F005 has been manually closed, trip system Division 1 shall provide an interlock that prevents the valve from automatically opening when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-136	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E21-F004B or terminate valve motion midstream from the control room.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-137	Division 2 shall provide a signal to open valve E21-F004B when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 13, GDC 20, GDC 29, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-138	Division 2 shall provide a signal to open valve E21-F004B when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 13, GDC 20, GDC 29, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-139	Division 2 shall provide a signal to open valve E21-F004B when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	GDC 13, GDC 20, GDC 29, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-140	Division 2 shall provide an interlock to prevent valve E21-F004B from being manually closed when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 21, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-141	Division 2 shall provide an interlock to prevent valve E21-F004B from being manually closed when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 21, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-142	Division 2 shall provide an interlock to prevent valve E21-F004B from being manually closed when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 21, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-143	Division 2 shall provide valve E21-F004B position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-144	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E21-F037 or terminate valve motion midstream from the control room.	Reg Guide 1.22, Reg Guide 1.62, GDC 21, GDC 37, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-145	Division 2 shall provide valve E21-F037 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-146	Division 2 shall provide a signal to open valve E21-F037 when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 13, GDC 20, GDC 29, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-147	Division 2 shall provide a signal to open valve E21-F037 when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 13, GDC 20, GDC 29, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-148	Division 2 shall provide a signal to open valve E21-F037 when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	GDC 13, GDC 20, GDC 29, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-149	Division 2 shall provide an override to manually close valve E21-F037 from the control room when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-150	Division 2 shall provide indicating light capability via the HMI when a manual signal to close valve E21-F037 is initiated when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-151	Division 2 shall provide an override to manually close valve E21-F037 from the control room when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-152	Division 2 shall provide indicating light capability via the HMI when a manual signal to close valve E21-F037 is initiated when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-153	Division 2 shall provide an override to manually close valve E21-F037 from the control room when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-154	Division 2 shall provide indicating light capability via the HMI when a manual signal to close valve E21-F037 is initiated when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-155	Channel B shall provide a vote to interlock to Division 2 if CI5 is satisfied (contact open).	Project design approach	
CS-FR-156	Division 2 shall provide an interlock to prevent valve E21-F037 from being manually opened when 2oo4 LOCA votes for RWL1 input are received **AND** a 1oo1 start vote for CI1 is received.	Original design feature	
CS-FR-157	Division 2 shall provide an interlock to prevent valve E21-F037 from being manually opened when 1oo1 votes are received for the second distinct action for the manual CS initiation is received **AND** a 1oo1 start vote for CI1 is received.	Original design feature	
CS-FR-158	Division 2 shall provide an interlock to prevent valve E21-F037 from being manually opened when a 1oo1 interlock vote for CI5 is received.	Project design approach	
CS-FR-159	Division 2 shall provide an interlock to prevent valve E21-F037 from opening, if closed, when valve E21-F004B and the Division 2 initiation logic are being tested when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 21, GDC 35	
CS-FR-160	Division 2 shall provide an interlock to prevent valve E21-F037 from opening, if closed, when valve E21-F004B and the Division 2 initiation logic are being tested when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	GDC 21, GDC 35	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-161	Division 2 shall provide an interlock to prevent valve E21-F037 from opening, if closed, when valve E21-F004B and the Division 2 initiation logic are being tested when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	GDC 21, GDC 35	
CS-FR-162	Once valve E21-F037 has been manually closed after already being automatically opened, Division 2 shall provide an interlock that prevents the valve from being opened unless 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-163	Once valve E21-F037 has been manually closed after already being automatically opened, Division 2 shall provide an interlock that prevents the valve from being opened unless 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-164	Once valve E21-F037 has been manually closed after already being automatically opened, Division 2 shall provide an interlock that prevents the valve from being opened unless 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-165	Once valve E21-F037 has been manually closed, trip system Division 2 shall provide an interlock that prevents the valve from automatically opening when 2oo4 LOCA votes for RWL1 input are received **AND** 2oo4 actuate votes for RLP input are received **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-166	Once valve E21-F037 has been manually closed, trip system Division 2 shall provide an interlock that prevents the valve from automatically opening when 2oo4 LOCA votes for DHP / RLP input are received **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-167	Once valve E21-F037 has been manually closed, trip system Division 2 shall provide an interlock that prevents the valve from automatically opening when 1oo1 votes are received for the second distinct action for the manual CS initiation **AND** 2oo4 actuate votes are received for RLP input **AND** a 1oo1 start vote for CI1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-168	Division 1 shall provide a signal to close valve E21-F015A when 2oo4 LOCA votes for RWL1 input are received.	GDC 20, GDC 21, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-169	Division 1 shall provide a signal to close valve E21-F015A when 2oo4 LOCA votes for DHP / RLP input are received.	GDC 20, GDC 21, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-170	Division 1 shall provide a signal to close valve E21-F015A when 1oo1 votes are received for the second distinct action for the manual CS initiation.	GDC 20, GDC 21, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-171	Division 1 shall provide an interlock to prevent valve E21-F015A from being manually opened when 2oo4 LOCA votes for RWL1 input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-172	Division 1 shall provide an interlock to prevent valve E21-F015A from being manually opened when 2oo4 LOCA votes for DHP / RLP input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-173	Division 1 shall provide an interlock to prevent valve E21-F015A from being manually opened when 1oo1 votes are received for the second distinct action for the manual CS initiation.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-174	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E21-F015A or terminate valve motion midstream from the control room.	Reg Guide 1.22, Reg Guide 1.62, GDC 21, GDC 37, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-175	Division 1 shall provide valve E21-F015A position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-176	Division 2 shall provide a signal to close valve E21-F015B when 2oo4 LOCA votes for RWL1 input are received.	GDC 20, GDC 21, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-177	Division 2 shall provide a signal to close valve E21-F015B when 2oo4 LOCA votes for DHP / RLP input are received.	GDC 20, GDC 21, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-178	Division 2 shall provide a signal to close valve E21-F015B when 1oo1 votes are received for the second distinct action for the manual CS initiation.	GDC 20, GDC 21, GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-179	Division 2 shall provide an interlock to prevent valve E21-F015B from being manually opened when 2oo4 LOCA votes for RWL1 input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-180	Division 2 shall provide an interlock to prevent valve E21-F015B from being manually opened when 2oo4 LOCA votes for DHP / RLP input are received.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-181	Division 2 shall provide an interlock to prevent valve E21-F015B from being manually opened when 1oo1 votes are received for the second distinct action for the manual CS initiation.	GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-182	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E21-F015B or terminate valve motion midstream from the control room.	Reg Guide 1.22, Reg Guide 1.62, GDC 21, GDC 37, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-183	Division 2 shall provide valve E21-F015B position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-184	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E21-F031A or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-185	Channel A shall provide an actuate vote to Division 1 after a 3 second time delay once CSF1 exceeds setpoint.	Project design approach	
CS-FR-186	Division 1 shall provide a signal to close valve E21-F031A when a 1oo1 actuate vote for CSF1 is received.	GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-187	Channel C shall provide an actuate vote to Division 1 when CI3 is satisfied (contact closed).	Project design approach	
CS-FR-188	Channel A shall provide an actuate vote to Division 1 when CI4 is satisfied (contact closed).	Project design approach	
CS-FR-189	Division 1 shall provide a signal to open valve E21-F031A when a 1oo1 actuate vote from CI3 is received.	GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-190	Division 1 shall provide a signal to open valve E21-F031A when a 1oo1 actuate vote from CI4 is received.	GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-191	Division 1 shall provide valve E21-F031A position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-192	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E21-F031B or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-193	Channel B shall provide an actuate vote to Division 2 after a 3 second time delay once CSF1 exceeds setpoint.	Project design approach	
CS-FR-194	Division 2 shall provide a signal to close valve E21-F031B when a 1oo1 actuate vote for CSF1 is received.	GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-195	Channel D shall provide an actuate vote to Division 2 when CI3 is satisfied (contact closed).	Project design approach	
CS-FR-196	Channel B shall provide an actuate vote to Division 2 when CI4 is satisfied (contact closed).	Project design approach	
CS-FR-197	Division 2 shall provide a signal to open valve E21-F031B when a 1oo1 actuate vote from CI3 is received.	GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-198	Division 2 shall provide a signal to open valve E21-F031B when a 1oo1 actuate vote from CI4 is received.	GDC 33, GDC 35, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-199	Trip system Division 2 shall provide valve E21-F031B position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-200	Division 1 shall provide a means to manually test valves E21-F006A and E21-F039A via the HMI.	Reg Guide 1.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-201	Division 1 shall provide valve E21-F006A and E21-F039A position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-202	Division 1 shall provide valve E21-F007A position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-203	Division 2 shall provide a means to manually test valves E21-F006B and E21-F039B via the HMI.	Reg Guide 1.22, GDC 16, GDC 32, GDC 37, NUREG-0737	
CS-FR-204	Division 2 shall provide valve E21-F006B and E21-F039B position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-205	Division 2 shall provide valve E21-F007B position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-206	Division 1 shall provide a means to manually open or close valve E21-F001A, under administrative control, from the control room.	GDC 33, GDC 54, GDC 56	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-207	Division 1 shall provide annunciation and indicating light capability via the HMI when the signal to close valve E21-F001A has been initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-208	Channel A shall provide an actuate vote to Division 1 when CI6-1 is satisfied (contact closed).	Project design approach	
CS-FR-209	Channel A shall provide an actuate vote to Division 1 when CI6-2 is satisfied (contact closed).	Project design approach	
CS-FR-210	Division 1 shall provide annunciation via the HMI when a 1oo1 actuate vote for CI6-1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-211	Division 1 shall provide indicating light capability via the HMI when a 1oo1 actuate vote for CI6-2 is received.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-212	Division 1 shall provide valve E21-F001A position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-213	Division 2 shall provide a means to manually open or close valve E21-F001B, under administrative control, from the control room.	GDC 33, GDC 54, GDC 56	
CS-FR-214	Division 2 shall provide annunciation and indicating light capability via the HMI when the signal to close valve E21-F001B has been initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-215	Channel B shall provide an actuate vote to Division 2 when CI6-1 is satisfied (contact closed).	Project design approach	
CS-FR-216	Channel B shall provide an actuate vote to Division 2 when CI6-2 is satisfied (contact closed).	Project design approach	
CS-FR-217	Division 2 shall provide annunciation via the HMI a 1oo1 actuate vote for CI6-1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-218	Division 2 shall provide indicating light capability via the HMI when a 1oo1 actuate vote for CI6-2 is received.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-219	Division 2 shall provide valve E21-F001B valve position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-220	Division 3 shall provide a means to manually open or close valve E21-F001C, under administrative control, from the control room.	GDC 33, GDC 54, GDC 56	
CS-FR-221	Division 3 shall provide annunciation and indicating light capability via the HMI when the signal to close valve E21-F001C has been initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-222	Channel C shall provide an actuate vote to Division 3 when CI6-1 is satisfied (contact closed).	Project design approach	
CS-FR-223	Channel C shall provide an actuate vote to Division 3 when CI6-2 is satisfied (contact closed).	Project design approach	
CS-FR-224	Division 3 shall provide annunciation via the HMI a 1oo1 actuate vote for CI6-1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-225	Division 3 shall provide indicating light capability via the HMI when a 1oo1 actuate vote for CI6-2 is received.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-226	Division 3 shall provide valve E21-F001C valve position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-227	Division 4 shall provide a means to manually open or close valve E21-F001D, under administrative control, from the control room.	GDC 33, GDC 54, GDC 56	
CS-FR-228	Division 4 shall provide annunciation and indicating light capability via the HMI when the signal to close valve E21-F001D has been initiated.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-229	Channel D shall provide an actuate vote to Division 4 when CI6-1 is satisfied (contact closed).	Project design approach	
CS-FR-230	Channel D shall provide an actuate vote to Division 4 when CI6-2 is satisfied (contact closed).	Project design approach	
CS-FR-231	Division 4 shall provide annunciation via the HMI a 1oo1 actuate vote for CI6-1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-232	Division 4 shall provide indicating light capability via the HMI when a 1oo1 actuate vote for CI6-2 is received.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-233	Division 4 shall provide valve E21-F001D position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-234	Division 1 shall provide a means to manually open or close valve E21-F005 from the control room during normal operation.	GDC 37	
CS-FR-235	Division 2 shall provide a means to manually open or close valve E21-F037 from the control room during normal operation.	GDC 37	
CS-FR-236	Channel A shall provide a CSP signal to Division 1 for indicator capability via the HMI.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-237	Channel A shall provide a vote to annunciate to Division 1 when CSP exceeds setpoint high.	Project design approach	
CS-FR-238	Channel A shall provide a vote to annunciate to Division 1 when CSP exceeds setpoint low.	Project design approach	
CS-FR-239	Division 1 shall provide annunciation via the HMI when a 1oo1 annunciate vote for CSP high is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-240	Division 1 shall provide annunciation via the HMI when a 1oo1 annunciate vote for CSP low is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-241	Channel A shall provide a CSF2 signal to Division 1.	Project design approach	
CS-FR-242	Division 1 shall condition the CSF2 signal through a square root converter and provide the resultant signal for indicator capability via the HMI.	GDC 13, Reg. Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-243	Channel A shall provide a vote to annunciate to Division 1 when CSDP exceeds setpoint high.	Project design approach	
CS-FR-244	Channel A shall provide a vote to annunciate to Division 1 when CSDP exceeds setpoint low.	Project design approach	
CS-FR-245	Division 1 shall provide annunciation via the HMI when a 1oo1 annunciate vote for CSDP high is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-246	Division 1 shall provide annunciation via the HMI when a 1oo1 annunciate vote for CSDP low is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-247	Each division and channel shall provide the capability to perform functional tests of the CS initiation logic.	Reg Guide 1.22, GDC 16, GDC 32, GDC 37, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-248	Each division shall provide annunciation and indicating light capability via the HMI when the CS initiation logic is being tested.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-249	Division 1 shall provide the capability to functionally test valve E21-F004A.	Reg Guide 1.22, GDC 16, GDC 32, GDC 37, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-250	Division 1 shall provide annunciation and indicating light capability via the HMI when valve E21-F004A is in test.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-251	Division 1 shall provide the capability to functionally test valve E21-F005.	Reg Guide 1.22, GDC 16, GDC 32, GDC 37, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-252	Division 1 shall provide annunciation and indicating light capability via the HMI when valve E21-F005 is in test.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-253	Division 2 shall provide the capability to functionally test valve E21-F004B.	Reg Guide 1.22, GDC 16, GDC 32, GDC 37, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-254	Division 2 shall provide annunciation and indicating light capability via the HMI when valve E21-F004B is in test.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-255	Division 2 shall provide the capability to functionally test valve E21-F037.	Reg Guide 1.22, GDC 16, GDC 32, GDC 37, NUREG-0737, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-256	Division 2 shall provide annunciation and indicating light capability via the HMI when valve E21-F037 is in test.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-257	Division 2 shall provide the capability to functionally test valve E21-F038.	Reg Guide 1.22, GDC 16, GDC 32, GDC 37, NUREG-0737	
CS-FR-258	Division 2 shall provide valve E21-F038 position indication via the HMI based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-259	Each division shall provide annunciation and indicating light capability via the HMI when any power condition (overload / loss of power) or test mode makes the system unavailable.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-260	Channel A shall provide an annunciate vote to Division 1 when CI7-1 is satisfied (contact closed).	Project design approach	
CS-FR-261	Channel A shall provide an annunciate vote to Division 1 when CI7-2 is satisfied (contact closed).	Project design approach	
CS-FR-262	Channel A shall provide an annunciate vote to Division 1 when CI8-1 is satisfied (contact closed).	Project design approach	
CS-FR-263	Channel A shall provide an annunciate vote to Division 1 when CI8-2 is satisfied (contact closed).	Project design approach	
CS-FR-264	Channel B shall provide an annunciate vote to Division 2 when CI7-1 is satisfied (contact closed).	Project design approach	
CS-FR-265	Channel B shall provide an annunciate vote to Division 2 when CI7-2 is satisfied (contact closed).	Project design approach	
CS-FR-266	Channel B shall provide an annunciate vote to Division 2 when CI8-1 is satisfied (contact closed).	Project design approach	
CS-FR-267	Channel B shall provide an annunciate vote to Division 2 when CI8-2 is satisfied (contact closed).	Project design approach	
CS-FR-268	Channel C shall provide an annunciate vote to Division 3 when CI7-1 is satisfied (contact closed).	Project design approach	
CS-FR-269	Channel C shall provide an annunciate vote to Division 3 when CI7-2 is satisfied (contact closed).	Project design approach	
CS-FR-270	Channel C shall provide an annunciate vote to Division 3 when CI8-1 is satisfied (contact closed).	Project design approach	
CS-FR-271	Channel C shall provide an annunciate vote to Division 3 when CI8-2 is satisfied (contact closed).	Project design approach	
CS-FR-272	Channel D shall provide an annunciate vote to Division 4 when CI7-1 is satisfied (contact closed).	Project design approach	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-273	Channel D shall provide an annunciate vote to Division 4 when CI7-2 is satisfied (contact closed).	Project design approach	
CS-FR-274	Channel D shall provide an annunciate vote to Division 4 when CI8-1 is satisfied (contact closed).	Project design approach	
CS-FR-275	Channel D shall provide an annunciate vote to Division 4 when CI8-2 is satisfied (contact closed).	Project design approach	
CS-FR-276	Each division shall provide annunciation via the HMI when a 1oo1 annunciate vote for C17-1 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-277	Each division shall provide annunciation via the HMI when a 1oo1 annunciate vote for C18-1 is received.	Project design approach	
CS-FR-278	Each division shall provide a means to manually provide annunciation for CORE SPRAY OUT OF SERVICE and status lights via the HMI.	Reg Guide 1.47 (BISI), IEEE Standard 279	
CS-FR-279	Each division shall provide indicating light capability via the HMI when a 1oo1 annunciate vote for C17-2 is received.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-280	Each division shall provide indicating light capability via the HMI when a 1oo1 annunciate vote for C18-2 is received.	Reg Guide 1.47, IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-281	Channel A shall provide an annunciate vote to Division 1 when CI9 is satisfied (contact closed).	Project design approach	
CS-FR-282	Channel B shall provide an annunciate vote to Division 2 when CI9 is satisfied (contact closed).	Project design approach	
CS-FR-283	Channel C shall provide an annunciate vote to Division 3 when CI9 is satisfied (contact closed).	Project design approach	
CS-FR-284	Channel D shall provide an annunciate vote to Division 4 when CI9 is satisfied (contact closed).	Project design approach	
CS-FR-285	Each division shall provide annunciation via the HMI when a 1oo1 annunciate vote for CI9 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
CS-FR-286	Channel C shall provide an annunciate vote to Division 3 when CI11 is satisfied (contact closed).	Project design approach	

CS FUNCTIONAL REQUIREMENTS			
ID #	**PPS/CS Requirement Revised**	**PPS/CS Source / Basis**	**Notes / Clarification**
CS-FR-287	Channel D shall provide an annunciate vote to Division 4 when CI11 is satisfied (contact closed).	Project design approach	
CS-FR-288	Division 3 shall provide annunciation via the HMI when a 1oo1 annunciate vote for CI11 is received.	Project design approach	
CS-FR-289	Division 4 shall provide annunciation via the HMI when a 1oo1 annunciate vote for CI11 is received.	Project design approach	
CS-FR-290	The trip system shall provide the means to perform functional tests during normal plant operation.	GDC 16, GDC 32, GDC 37, Reg Guide 1.22, NUREG-0737	
CS-FR-291	Each channel and each division shall provide sufficient features and documented evaluations to support elimination of most Technical Specification Surveillance Tests, and minimize the requirements for manual calibration checks.	Project design approach	
CS-FR-292	For all PPS inputs that have the potential to require manual test insertion or external measurement of input values (i.e., use of an external digital multi meter by a technician), test jacks are provided in the cabinets.	Project design approach	
CS-FR-293	For all inputs that have the potential to require manual multi-point calibration checks with external calibration equipment, knife edge disconnects along with test jacks are incorporated in the field termination panels.	Project design approach	
CS-FR-294	Each division shall provide the means via soft controls on the HMI to automate valve sequencing, alignment and throttling and CS pump operation to support CS Flow Testing and other CS alignments.	Original design feature / Project design decision	
CS-FR-295	Each division shall provide the means via soft controls on the HMI to interrupt the automated valve sequencing, alignment and throttling and CS pump operation that have been initiated to support CS Flow Testing or other CS alignments.	Original design feature / Project design decision	

F

F.1 RHR Design Requirements

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-1	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. 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. 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.	GDC 1 - Quality standards and records
RHR-DR-2	Structures, systems, and components important to safety shall be designed to withstand the effect of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions.	GDC 2 - Design Bases for Protection Against Natural Phenomena
RHR-DR-3	Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions.	GDC 3 - Fire protection
RHR-DR-4	Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents (LOCAs).	GDC 4 - Environmental and dynamic effects design bases
RHR-DR-5	The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.	GDC 10 - Reactor design

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-6	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.	GDC 13 - Instrumentation and control
RHR-DR-7	A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. 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 I&C 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.	GDC 19 - Control Room
RHR-DR-8	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.	GDC 20 - Protection system functions

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-9	The protection system shall be designed for high functional reliability and in-service 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.	GDC 21 - Protection system reliability and testability
RHR-DR-10	The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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.	GDC 22- Protection system independence
RHR-DR-11	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.	GDC 23 - Protection system failure modes
RHR-DR-12	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.	GDC 24 - Separation of protection and control systems

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-13	The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.	GDC 29 - Protection against anticipated operational occurrences
RHR-DR-14	A system to supply reactor coolant makeup for protection against small breaks in the reactor coolant pressure boundary shall be provided. The system safety function shall be to assure that specified acceptable fuel design limits are not exceeded as a result of reactor coolant loss due to leakage from the reactor coolant pressure boundary and rupture of small piping or other small components which are part of the boundary. The system shall be designed to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished using the piping, pumps, and valves used to maintain coolant inventory during normal reactor operation.	GDC 33 - Reactor Coolant Makeup
RHR-DR-15	A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts.	GDC 35 - Emergency Core Cooling
RHR-DR-16	The emergency core cooling system shall be designed to permit appropriate periodic pressure and functional testing to assure (1) the structural and leak tight integrity of its components, (2) the operability and performance of the active components of the system, and (3) the operability of the system as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.	GDC 37 - Testing of Emergency Core Cooling System

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-17	The protection system shall be designed to permit periodic testing of its initiation functions inclusive of the actuation devices and actuated equipment when the reactor is in operation.	Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions (Safety Guide 22)
RHR-DR-18	Those structures, systems, and components (SSC) that should be designed to remain functional if the Safe Shutdown Earthquake (SSE) occurs shall be designated as Seismic Category I. (This includes Systems or portions of systems that are required for reactor shutdown; all electric and mechanical devices and circuitry between the process and the input terminals of the actuator systems involved in generating signals that initiate protective action; systems or portions of systems that are required for (1) monitoring of systems important to safety and (2) actuation of systems important to safety.)	Regulatory Guide 1.29 - Seismic Design Classification
RHR-DR-19	The RHR shall comply with the requirements of Appendix B to 10 CFR Part 50 for the installation, inspection, and testing of nuclear power plant instrumentation and electric equipment.	Regulatory Guide 1.30 - Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment (Safety Guide 30)
RHR-DR-20	The RHR shall meet the requirements for design, operation and testing of safety-related power systems within nuclear power plants as defined within IEEE Std. 308.	Regulatory Guide 1.32 - Criteria for Power Systems for Nuclear Power Plants
RHR-DR-21	The RHR shall meet the requirements for indicating the bypass or inoperable status of portions of the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the system it actuates to perform their safety-related functions:	Regulatory Guide 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
RHR-DR-22	The RHR shall comply with the IEEE Std. 279 requirement that any single failure within the protection system shall not prevent proper protective action at the system level when required, by utilizing the guidance in IEEE Std. 379-1972 for applying the single-failure criterion to the design and analysis of nuclear power plant protection systems.	Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Safety Systems

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-23	The RHR shall provide a means for manual initiation of protective actions.	Regulatory Guide 1.62 - Manual Initiation of Protective Actions
RHR-DR-24	The RHR shall meet the requirements for physical independence of the circuits and electric equipment comprising or associated with the Class 1E power system, the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety related functions.	Regulatory Guide 1.75 - Physical Independence of Electric Systems
RHR-DR-25	The RHR shall comply with design verification requirements to verify adequacy of design under the most adverse design conditions.	Regulatory Guide 1.89 - Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants
RHR-DR-26	The RHR shall comply with the requirement to: (1) provide information required to permit the operator to take preplanned manual actions to accomplish safe plant shutdown; (2) determine whether the reactor trip, engineered safety feature systems, and manually initiated safety systems and other systems important to safety are performing their intended functions (i.e., reactivity control, core cooling, maintaining reactor coolant system integrity, and maintaining containment integrity); (3) provide information to the operators that will enable them to determine the potential for causing a gross breach of the" barriers to radioactivity release (i.e., fuel cladding, reactor coolant pressure boundary, and containment) and to determine if a gross breach of a barrier has occurred.	Regulatory Guide 1.97 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants
RHR-DR-27	The RHR shall comply with design verification requirements to verify the seismic adequacy of electric equipment.	Regulatory Guide 1.100 - Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-28	The RHR shall design shall implement setpoints that assure sufficient margin between Technical Specification limits and the trip setpoint to account for instrument inaccuracy, calibration uncertainties and instrument drift. Consideration of instrument span and range as well as environmental influences must be included.	Regulatory Guide 1.105 - Instrument Setpoint
RHR-DR-29	The RHR shall comply with the requirements for periodic testing of electric power and protection systems.	Regulatory Guide 1.118 - Periodic Testing of Electric Power and Protection Systems
RHR-DR-30	The RHR shall, with precision and reliability, restore and maintain the reactor vessel water level by the use of the Low Pressure Coolant Injection (LPCI) mode after a Loss of Coolant Accident (LOCA)	IEEE Std. 603, Section 5.0 Safety System Criteria and 6.1 Automatic Control
RHR-DR-31	The RHR shall initiate when the monitored plant parameter exceeds the following trip setpoint: Reactor Vessel Water Level 1 < -129 inches Drywell Pressure > 1.68 psig	IEEE Std. 603, Section 6.1 Automatic Control
RHR-DR-32	The RHR signal input to actuation output propagation time shall be less than 100 milliseconds.	IEEE Std. 603, Section 4.10
RHR-DR-33	The RHR shall be capable of initiating under all required modes of reactor operation.	IEEE Std. 603, Section 4.1
RHR-DR-34	The RHR shall ensure that the protective action, once started, continues to completion.	IEEE Std. 603, Section 5.2 Completion of Protective Action
RHR-DR-35	Any single failure within the RHR shall not prevent proper protective action at the system level when required.	IEEE Std. 603, Section 5.1 Single Failure Criterion and IEEE Std. 7-4.3.2 Section 5.1 Single Failure Criterion

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-36	Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.	IEEE Std. 603 section 5.3 Quality and IEEE Std. 7-4.3.2 section 5.3 Quality
RHR-DR-37	Type test data or reasonable engineering extrapolation based on test data shall be available to verify that protection system equipment shall meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements.	IEEE Std. 603 section 5.4 Equipment Qualification and IEEE Std. 7-4.3.2 section 5.4 Equipment Qualification
RHR-DR-38	All protection system channels shall be designed to maintain necessary functional capability under extremes of conditions (as applicable) relating to environment, energy supply, malfunctions and accidents.	IEEE Std. 603 section 5.5 System Integrity and IEEE Std. 7-4.3.2 and section 5.5 Independence
RHR-DR-39	Channels that provide signals for the same protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 System Integrity
RHR-DR-40	Any equipment that is used for both protective and control functions shall be classified as part of the protection system and shall meet all the applicable requirements.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence
RHR-DR-41	The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system and shall meet all the applicable requirements. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-42	Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
RHR-DR-43	Provisions shall be included so that the protective action can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
RHR-DR-44	Where a credible single event can cause a control system action that results in a condition requiring protective action and can concurrently prevent the protective action from those protection system channels designated to provide principal protection against the condition, then alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design bases.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
RHR-DR-45	To the extent feasible and practical, protection system inputs shall be derived from signals that are direct measures of the desired variables.	IEEE Std. 603 section 6.4 Derivation of System Inputs
RHR-DR-46	Means shall be provided for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
RHR-DR-47	Capability shall be provided for testing and calibrating channels and the devices used to derive the final system output signal from the various channel signals.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
RHR-DR-48	For those parts of the system where the required interval between testing will be less than the normal time interval between generating station shutdowns, there shall be capability for testing during power operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-49	The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective action at the systems level.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
RHR-DR-50	During such operation, the active parts of the system shall of themselves continue to meet the single failure criterion.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
RHR-DR-51	Where operating requirements necessitate automatic or manual bypass of a protective function, the design shall be such that the bypass will be removed automatically whenever permissive conditions are not met.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
RHR-DR-52	Devices used to achieve automatic removal of the bypass of a protective function are part of the protection system and shall be designed in accordance with these criteria.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
RHR-DR-53	If the protective action of some part of the system has been bypassed or deliberately rendered inoperative for any purpose, this fact shall be continuously indicated in the control room.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RHR-DR-54	The design shall permit the administrative control of the means for manually bypassing channels or protective functions.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
RHR-DR-55	Where it is necessary to change to a more restrictive set point to provide adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of assuring that the more restrictive set point is used.	IEEE Std. 603 section 6.8 Setpoints
RHR-DR-56	The devices used to prevent improper use of less restrictive set points shall be considered a part of the protection system and shall be designed in accordance with the other provisions of these criteria regarding performance and reliability.	IEEE Std. 603 section 6.8 Setpoints
RHR-DR-57	The protection system shall be so designed that, once initiated, a protective action at the system level shall go to completion.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-58	Return to operation shall require subsequent deliberate operator action.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action
RHR-DR-59	The protection system shall include means for manual initiation of each protective action at the system level (for example, reactor trip, containment isolation, safety injection, core spray, etc).	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
RHR-DR-60	No single failure within the manual, automatic, or common portions of the protection system shall prevent initiation of protective action by manual or automatic means.	IEEE Std. 603 section 7.2 Manual Control
RHR-DR-61	Manual initiation should depend upon the operation of a minimum of equipment.	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
RHR-DR-62	The design shall permit the administrative control of access to all set point adjustments, module calibration adjustments, and test points.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
RHR-DR-63	Protective actions shall be indicated and identified down to the channel level.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RHR-DR-64	The protection system shall be designed to provide the operator with accurate, complete, and timely information pertinent to its own status and to generating station safety.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RHR-DR-65	The design shall minimize the development of conditions which would cause meters, annunciators, recorders, alarms, etc, to give anomalous indications confusing to the operator.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RHR-DR-66	The system shall be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.	IEEE Std. 603 section 5.10 Repair

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-67	In order to provide assurance that the requirements given in this document can be applied during the design, construction, maintenance, and operation of the plant, the protection system equipment (for example, interconnecting wiring, components, modules, etc), shall be identified distinctively as being in the protection system.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
RHR-DR-68	This identification shall distinguish between redundant portions of the protection system. (In the installed equipment, components, or modules mounted in assemblies that are clearly identified as being in the protection system do not themselves require identification.) All software, firmware, and programmable logic shall be identified in accordance with IEEE Std. 7-4.3.2 Clause 5.11.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
RHR-DR-69	RHR shall conform to the design criteria and features for Class 1E electric systems to ensure that functional requirements under the conditions produced by design basis events are met.	IEEE Std. 308 - Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations
RHR-DR-70	RHR shall conform to the methods for demonstrating the qualification of Class 1E equipment including components or equipment of any interface whose failure could adversely affect the performance of Class 1E systems and electronic equipment.	IEEE Std. 323 - Qualifying Class 1E Equipment for Nuclear Power Generating Stations
RHR-DR-71	RHR shall conform to the design and operational criteria for the performance of periodic testing of nuclear power generating station safety systems.	IEEE Std. 338 - Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems
RHR-DR-72	RHR shall meet its Class 1E performance requirements during and following one SSE (safe shutdown earthquake) preceeded by a number of OBEs (operating basis earthquakes).	IEEE Std. 344 - Guide for Seismic Qualification of Class 1 Electric Equipment for Nuclear Power Generating Stations
RHR-DR-73	RHR shall meet the single failure criterion as described and classified in IEEE Std. 379.	IEEE Std. 379 - Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

RHR/LPCI DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RHR-DR-74	RHR shall meet the criteria and requirements for establishing and maintaining the independence of Class 1E equipment and circuits and auxiliary supporting features by physical separation and electrical isolation.	IEEE Std. 384 - Criteria for Independence of Class 1E Equipment and Circuits

F.2 RHR Functional Requirements

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-1	PPS/RHR LPCI shall be capable of providing signals to start pumps and align valves for delivering water to the reactor as well as to support additional cooling functions either automatically when any of the monitored parameters exceeds a pre-established value, or by manual initiation. PPS/RHR shall also provide automation for other RHR modes that were previously performed manually.	GDC 35	
RHR-FR-2	RHR shall be comprised of four independent and separate divisions (Division 1, Division 2, Division 3 and Division 4).	Reg Guide 1.53, IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-3	PPS/RHR shall have four (4) independent channels (Channel A, Channel B, Channel C and Channel D) that each provide votes / signals to each of the divisions.	Project design approach	The four channels are common to each of the divisions.
RHR-FR-4	PPS/RHR shall be capable of being powered by 125VDC power.	Original design feature	
RHR-FR-5	Each division shall provide outputs that are capable of interfacing with 120VAC loads.	Original design feature	
RHR-FR-6	Each channel shall receive an input from each of the following monitored parameters that are provided as common inputs to the PPS platform and are shared by each of the PPS functions: • Reactor Vessel Water Level 1 (RWL1) • Drywell High Pressure (DHP) • Reactor Low Pressure (RLP)	GDC 13, GDC 20, GDC 29, IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-7	Each channel shall receive a 4-20 mA input from each of the following monitored parameters: • RHR Injection Valve DP (RIVDP) • RHR Loop Discharge Flow (RLDF) • RHR Pump Discharge Flow (RPDF) • RHR Pump Discharge Pressure (RPDP)	Original design feature	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-8	Channel B shall receive a 4-20 mA input from the following monitored parameter: • RHR Pump Suction Shutdown Cooling Pressure (RSSCP)	Original design feature	
RHR-FR-9	Channel A and Channel B shall receive a 4-20 mA input from the following monitored parameter: • LPCI Line Differential Pressure (LLDP)	Original design feature	
RHR-FR-10	Each channel shall receive the following contact inputs: • 144X from 4kV bus (CI1) • 152H/152S from Standby Diesel (CI2) • RHR Pump Breaker 52 (CI27) • RHR Pump Breaker in operating position (CI28) • Associated RHR valve motor overcurrent (CI29) • Loss of Logic Power (CI30)	Original design feature	
RHR-FR-11	Channel A shall receive the following contact inputs: • E11- F017A LS6 (CI3) • E11- F021A LS6 (CI5) • E11- F016A LS6 (CI6) • E11-F006A LS11 (CI9) • E11-F004A LS11 (CI10) • E11-F006A LS6 (CI19) • E11-F004A LS6 (CI21) • E11-F024A LS6 (CI22) • E11-F027A LS6 (CI23)	Original design feature	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-12	Channel B shall receive the following contact inputs: • E11- F017B LS6 (CI4) • E11- F021B LS6 (CI7) • E11- F016B LS6 (CI8) • E11-F006B LS11 (CI11) • E11-F004B LS11 (CI12) • E11-F006B LS6 (CI20) • E11-F004B LS6 (CI24) • E11-F024B LS6 (CI25) • E11-F027B LS6 (CI26)	Original design feature	
RHR-FR-13	Channel C shall receive the following contact inputs: • E11-F004C LS11 (CI13) • E11-F067A LS5 (CI15)	Original design feature	
RHR-FR-14	Channel D shall receive the following contact inputs: • E11-F004D LS11 (CI14) • E11-F067B LS5 (CI16)	Original design feature	
RHR-FR-15	Channel A and Channel B shall receive the following contact inputs: • E11-F009 LS11 (CI17) • E11-F008 LS11 (CI18)	Original design feature	
RHR-FR-16	Each input to a channel (ma, contact input or digital signal) shall be voted on by the channel based on the condition (condition met or not met).	Project design approach	The term "shall be voted on" indicates that the channel performs a bi-stable comparison against a pre-determined configurable setpoint to determine whether the input is at or above/below the setpoint value.

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-17	Each channel shall provide the status of the vote (e.g. vote to not function if condition not met; vote to function if condition met; vote to annunciate) to each of the divisions.	Project design approach	The terms “not function”, “function”, “annunciate” describe different types of votes that may be provided by a channel (Note - others may be specified within the requirements). A particular vendor solution may combine one or more of the vote types into a single channel vote based on the capabilities of the platform.
RHR-FR-18	Each division shall determine whether the votes to function for each type of input satisfy the voting criteria (e.g. 2oo4).	Project design approach	
RHR-FR-19	Each division shall execute a function when the voting criteria is satisfied.	Project design approach	
RHR-FR-20	Each input to a channel shall have an associated voter (e.g. 2oo4) within each division to ensure that trip inputs are voted separately.	Project design approach	
RHR-FR-21	Each division shall generate an output for an isolation trip initiation, when the required voting has been satisfied.	Project design approach	As an example, the RWL1 input to Channels A, B, C and D shall be sent to a 2oo4 voter in each of the divisions (Division 1, Division 2, Division 3 and Division 4). When at least two of the four RWL1 inputs to the 2oo4 voter achieves a trip state, the associated division generates an output. The generated output may be dependent on additional voting to be satisfied. Some outputs require different voting schemes which are described within the requirement.
RHR-FR-22	Channel A shall provide a condition vote to Division 1 when CI1 is satisfied (contact closed).	Project design approach	
RHR-FR-23	Channel A shall provide a delay vote to Division 1 when CI1 is satisfied (contact closed) after a 5 second delay.	Project design approach	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-24	Channel B shall provide a condition vote to Division 2 CI1 is satisfied (contact closed).	Project design approach	
RHR-FR-25	Channel B shall provide a delay vote to Division 1 when CI1 is satisfied (contact closed) after a 5 second delay.	Project design approach	
RHR-FR-26	Channel C shall provide a condition vote to Division 3 CI1 is satisfied (contact closed).	Project design approach	
RHR-FR-27	Channel D shall provide a condition vote to Division 4 CI1 is satisfied (contact closed).	Project design approach	
RHR-FR-28	Channel A shall provide a condition vote to Division 1 when CI2 is satisfied (contact closed).	Project design approach	
RHR-FR-29	Channel B shall provide a condition vote to Division 2 when CI2 is satisfied (contact closed).	Project design approach	
RHR-FR-30	Channel C shall provide a condition vote to Division 3 when CI2 is satisfied (contact closed).	Project design approach	
RHR-FR-31	Channel D shall provide a condition vote to Division 4 when CI2 is satisfied (contact closed).	Project design approach	
RHR-FR-32	Channel A shall provide a condition vote to Division 1 when CI3 is satisfied (contact closed).	Project design approach	
RHR-FR-33	Channel B shall provide a condition vote to Division 2 when CI4 is satisfied (contact closed).	Project design approach	
RHR-FR-34	Channel A shall provide a condition vote to Division 1 when CI5 is satisfied (contact closed).	Project design approach	
RHR-FR-35	Channel A shall provide a condition vote to Division 1 when CI6 is satisfied (contact closed).	Project design approach	
RHR-FR-36	Channel B shall provide a condition vote to Division 2 when CI7 is satisfied (contact closed).	Project design approach	
RHR-FR-37	Channel B shall provide a condition vote to Division 2 when CI8 is satisfied (contact closed).	Project design approach	
RHR-FR-38	Channel A shall provide a condition vote to Division 1 when CI9 is satisfied (contact closed).	Project design approach	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-39	Channel A shall provide a condition vote to Division 1 when CI10 is satisfied (contact closed).	Project design approach	
RHR-FR-40	Channel B shall provide a condition vote to Division 2 when CI11 is satisfied (contact closed).	Project design approach	
RHR-FR-41	Channel B shall provide a condition vote to Division 2 when CI12 is satisfied (contact closed).	Project design approach	
RHR-FR-42	Channel C shall provide a condition vote to Division 3 when CI13 is satisfied (contact closed).	Project design approach	
RHR-FR-43	Channel D shall provide a condition vote to Division 3 when CI14 is satisfied (contact closed).	Project design approach	
RHR-FR-44	Channel C shall provide a condition vote to Division 3 when CI15 is satisfied (contact open).	Project design approach	
RHR-FR-45	Channel D shall provide a condition vote to Division 4 when CI16 is satisfied (contact open).	Project design approach	
RHR-FR-46	Channel A shall provide a condition vote to Division 1 when CI17 is satisfied (contact closed).	Project design approach	
RHR-FR-47	Channel B shall provide a condition vote to Division 2 when CI17 is satisfied (contact closed).	Project design approach	
RHR-FR-48	Channel A shall provide a condition vote to Division 1 when CI18 is satisfied (contact closed).	Project design approach	
RHR-FR-49	Channel B shall provide a condition vote to Division 2 when CI18 is satisfied (contact closed).	Project design approach	
RHR-FR-50	Channel A shall provide a condition vote to Division 1 when CI19 is satisfied (contact open).	Project design approach	
RHR-FR-51	Channel B shall provide a condition vote to Division 2 when CI20 is satisfied (contact open).	Project design approach	
RHR-FR-52	Channel A shall provide a condition vote to Division 1 when CI21 is satisfied (contact open).	Project design approach	
RHR-FR-53	Channel A shall provide a condition vote to Division 1 when CI22 is satisfied (contact open).	Project design approach	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-54	Channel A shall provide a condition vote to Division 1 when CI23 is satisfied (contact open).	Project design approach	
RHR-FR-55	Channel B shall provide a condition vote to Division 2 when CI24 is satisfied (contact open).	Project design approach	
RHR-FR-56	Channel B shall provide a condition vote to Division 2 when CI25 is satisfied (contact open).	Project design approach	
RHR-FR-57	Channel B shall provide a condition vote to Division 2 when CI26 is satisfied (contact open).	Project design approach	
RHR-FR-58	Channel A shall provide a condition vote to Division 1 when CI27 is satisfied (contact closed) after a 10 second time delay.	Project design approach	
RHR-FR-59	Channel B shall provide a condition vote to Division 2 when CI27 is satisfied (contact closed) after a 10 second time delay.	Project design approach	
RHR-FR-60	Channel C shall provide a condition vote to Division 3 when CI27 is satisfied (contact closed) after a 10 second time delay.	Project design approach	
RHR-FR-61	Channel D shall provide a condition vote to Division 4 when CI27 is satisfied (contact closed) after a 10 second time delay.	Project design approach	
RHR-FR-62	Channel A shall provide an annunciate vote to Division 1 when CI28 is satisfied (contact closed).	Project design approach	
RHR-FR-63	Channel B shall provide an annunciate vote to Division 2 when CI28 is satisfied (contact closed).	Project design approach	
RHR-FR-64	Channel C shall provide an annunciate vote to Division 3 when CI28 is satisfied (contact closed).	Project design approach	
RHR-FR-65	Channel D shall provide an annunciate vote to Division 4 when CI28 is satisfied (contact closed).	Project design approach	
RHR-FR-66	Channel A shall provide an annunciate vote to Division 1 when CI29 is satisfied (contact closed).	Project design approach	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-67	Channel B shall provide an annunciate vote to Division 2 when CI29 is satisfied (contact closed).	Project design approach	
RHR-FR-68	Channel C shall provide an annunciate vote to Division 3 when CI29 is satisfied (contact closed).	Project design approach	
RHR-FR-69	Channel D shall provide an annunciate vote to Division 4 when CI29 is satisfied (contact closed).	Project design approach	
RHR-FR-70	Channel A shall provide an annunciate vote to Division 1 when CI30 is satisfied (contact closed).	Project design approach	
RHR-FR-71	Channel B shall provide an annunciate vote to Division 2 when CI30 is satisfied (contact closed).	Project design approach	
RHR-FR-72	Channel C shall provide an annunciate vote to Division 3 when CI30 is satisfied (contact closed).	Project design approach	
RHR-FR-73	Channel D shall provide an annunciate vote to Division 4 when CI30 is satisfied (contact closed).	Project design approach	
RHR-FR-74	Channel A shall provide a condition vote to Division 1 when RIVDP exceeds setpoint low.	Project design approach	
RHR-FR-75	Channel A shall provide an annunciate vote to Division 1 when RIVDP exceeds setpoint low.	Project design approach	
RHR-FR-76	Channel B shall provide a condition vote to Division 2 when RIVDP exceeds setpoint low.	Project design approach	
RHR-FR-77	Channel B shall provide an annunciate vote to Division 2 when RIVDP exceeds setpoint low.	Project design approach	
RHR-FR-78	Channel C shall provide a condition vote to Division 3 when RIVDP exceeds setpoint low.	Project design approach	
RHR-FR-79	Channel C shall provide an annunciate vote to Division 3 when RIVDP exceeds setpoint low.	Project design approach	
RHR-FR-80	Channel D shall provide a condition vote to Division 4 when RIVDP exceeds setpoint low.	Project design approach	
RHR-FR-81	Channel D shall provide an annunciate vote to Division 4 when RIVDP exceeds setpoint low.	Project design approach	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-82	Channel A shall provide a condition vote to Division 1 when RLDF exceeds setpoint high.	Project design approach	
RHR-FR-83	Channel A shall provide an annunciate vote to Division 1 when RLDF exceeds setpoint high.	Project design approach	
RHR-FR-84	Channel B shall provide a condition vote to Division 2 when RLDF exceeds setpoint high.	Project design approach	
RHR-FR-85	Channel B shall provide an annunciate vote to Division 2 when RLDF exceeds setpoint high.	Project design approach	
RHR-FR-86	Channel C shall provide a condition vote to Division 3 when RLDF exceeds setpoint high.	Project design approach	
RHR-FR-87	Channel C shall provide an annunciate vote to Division 3 when RLDF exceeds setpoint high.	Project design approach	
RHR-FR-88	Channel D shall provide a condition vote to Division 4 when RLDF exceeds setpoint high.	Project design approach	
RHR-FR-89	Channel D shall provide an annunciate vote to Division 4 when RLDF exceeds setpoint high.	Project design approach	
RHR-FR-90	Channel B shall provide an annunciate vote to Division 2 when RSSCP exceeds setpoint high.	Project design approach	
RHR-FR-91	Channel A shall provide an annunciate vote to Division 1 when RPDP exceeds setpoint high.	Project design approach	
RHR-FR-92	Channel A shall provide an annunciate vote to Division 1 when RPDP exceeds setpoint low.	Project design approach	
RHR-FR-93	Channel B shall provide an annunciate vote to Division 2 when RPDP exceeds setpoint high.	Project design approach	
RHR-FR-94	Channel B shall provide an annunciate vote to Division 2 when RPDP exceeds setpoint low.	Project design approach	
RHR-FR-95	Channel C shall provide an annunciate vote to Division 3 when RPDP exceeds setpoint high.	Project design approach	
RHR-FR-96	Channel C shall provide an annunciate vote to Division 3 when RPDP exceeds setpoint low.	Project design approach	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-97	Channel D shall provide an annunciate vote to Division 4 when RPDP exceeds setpoint high.	Project design approach	
RHR-FR-98	Channel D shall provide an annunciate vote to Division 4 when RPDP exceeds setpoint low.	Project design approach	
RHR-FR-99	Channel A shall provide an annunciate vote to Division 1 when LLDP exceeds setpoint high.	Project design approach	
RHR-FR-100	Channel A shall provide an annunciate vote to Division 1 when LLDP exceeds setpoint low.	Project design approach	
RHR-FR-101	Channel B shall provide an annunciate vote to Division 2 when LLDP exceeds setpoint high.	Project design approach	
RHR-FR-102	Channel B shall provide an annunciate vote to Division 2 when LLDP exceeds setpoint low.	Project design approach	
RHR-FR-103	Each division shall initiate the LPCI mode of RHR when a LOCA signal is present. LOCA signal: RWL1 reaches setpoint **OR** DHP and RLP both reach setpoint.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-104	Each channel shall provide a vote for LOCA signal to each division when RWL1 input exceeds setpoint low.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-105	Each channel shall provide a vote to annunciate to each division when RWL1 input exceeds setpoint low.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-106	Each channel shall provide a vote for LOCA signal to each division when DHP input exceeds setpoint high **AND** RLP input exceeds setpoint low.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-107	Each channel shall provide a condition vote to each division when DHP input exceeds setpoint high.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-108	Each channel shall provide a vote to annunciate to each division when DHP input exceeds setpoint high.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-109	Each channel shall provide a vote to annunciate to each division when RLP input exceeds setpoint low.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-110	Each channel shall include a manual LPCI initiation feature located in the control room that requires two distinct actions (e.g. arming prior to functioning) to be completed.	Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-111	Channel A shall provide a vote to annunciate to Division 1 upon the first distinct action for the associated manual initiation feature being satisfied.	Project design approach	
RHR-FR-112	Division 1 shall provide annunciation for RHR MANUAL INITIATION SWITCH ARMED via the HMI when 1oo1 annunciate votes are received for the first distinct action for the manual initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-113	Channel B shall provide a vote to annunciate to Division 2 upon the first distinct action for the associated manual initiation feature being satisfied.	Project design approach	
RHR-FR-114	Division 2 shall provide annunciation for RHR MANUAL INITIATION SWITCH ARMED via the HMI when 1oo1 annunciate votes are received for the first distinct action for the manual initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-115	Channel C shall provide a vote to annunciate to Division 3 upon the first distinct action for the associated manual initiation feature being satisfied.	Project design approach	
RHR-FR-116	Division 3 shall provide annunciation for RHR MANUAL INITIATION SWITCH ARMED via the HMI when 1oo1 annunciate votes are received for the first distinct action for the manual initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-117	Channel D shall provide a vote to annunciate to Division 4 upon the first distinct action for the associated manual initiation feature being satisfied.	Project design approach	
RHR-FR-118	Division 4 shall provide annunciation for RHR MANUAL INITIATION SWITCH ARMED via the HMI when 1oo1 annunciate votes are received for the first distinct action for the manual initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-119	Channel A shall provide a vote for manual initiation to Division 1 on the second distinct action being satisfied.	Project design approach	
RHR-FR-120	Channel B shall provide a vote for manual initiation to Division 2 on the second distinct action being satisfied.	Project design approach	
RHR-FR-121	Channel C shall provide a vote for manual initiation to Division 3 on the second distinct action being satisfied.	Project design approach	
RHR-FR-122	Channel D shall provide a vote for manual initiation to Division 4 on the second distinct action being satisfied.	Project design approach	
RHR-FR-123	Each channel shall seal in the RWL1, DHP/RLP and manual initiation inputs until manually reset.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-124	Each division shall provide indicating light capability via the HMI when 2oo4 LOCA votes for RWL1 input are received.	Original design feature	
RHR-FR-125	Each division shall provide indicating light capability via the HMI when 2oo4 LOCA votes for DHP/RLP input are received.	Original design feature	
RHR-FR-126	Division 1 shall provide indicating light capability via the HMI when 1oo1 manual initiation votes are received.	Original design feature	
RHR-FR-127	Each division shall provide annunciation for DRYWELL HI PRESS via the HMI when 2oo4 annunciate votes for DHP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-128	Each division shall provide annunciation for REACTOR LO-LO-LO LEVEL via the HMI when 2oo4 annunciate votes RWL1 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-129	Each division shall provide annunciation for LO REACTOR PRESS RHR PERMISSIVE TO START via the HMI when 2oo4 annunciate votes RLP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-130	Division 1 shall provide an output to start RHR Pump A when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 delay votes for CI1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-131	Division 1 shall provide an output to start RHR Pump A when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 delay votes for CI1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-132	Division 1 shall provide an output to start RHR Pump A when 1oo1 manual initiation votes **AND** 1oo1 delay votes for CI1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-133	Division 2 shall provide an output to start RHR Pump B when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 delay votes for CI1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-134	Division 2 shall provide an output to start RHR Pump B when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 delay votes for CI1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-135	Division 2 shall provide an output to start RHR Pump B when 1oo1 manual initiation votes **AND** 1oo1 delay votes for CI1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-136	Division 1 shall provide an output to start RHR Pump A when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for CI2 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-137	Division 1 shall provide an output to start RHR Pump A when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for CI2 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-138	Division 1 shall provide an output to start RHR Pump A when 1oo1 manual initiation votes and 1oo1 condition votes for CI1 input and 1oo1 condition votes for CI2 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-139	Division 2 shall provide an output to start RHR Pump B when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for CI2 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-140	Division 2 shall provide an output to start RHR Pump B when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI1 input and 1oo1 condition votes for CI2 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-141	Division 2 shall provide an output to start RHR Pump B when 1oo1 manual initiation votes and 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for CI2 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-142	Division 3 shall provide an output to start RHR Pump C when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 condition votes for CI1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-143	Division 3 shall provide an output to start RHR Pump C when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-144	Division 3 shall provide an output to start RHR Pump C when 1oo1 manual initiation votes **AND** 1oo1 condition votes for CI1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-145	Division 4 shall provide an output to start RHR Pump D when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 condition votes for CI1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-146	Division 4 shall provide an output to start RHR Pump D when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-147	Division 4 shall provide an output to start RHR Pump D when 1oo1 manual initiation votes **AND** 1oo1 condition votes for CI1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-148	Division 1 shall provide an output to open injection valve E11-F017A when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for RIVDP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-149	Division 1 shall provide an output to open injection valve E11-F017A when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for RIVDP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-150	Division 1 shall provide an output to open injection valve E11-F017A when 1oo1 manual initiation votes **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for RIVDP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-151	Division 1 shall provide annunciation for Division 1 LPCI INJECTION VALVE ΔP PERMISSIVE via the HMI when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 annunciate votes for RIVDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-152	Division 1 shall provide annunciation for Division 1 LPCI INJECTION VALVE ΔP PERMISSIVE via the HMI when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 annunciate votes for RIVDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-153	Division 1 shall provide annunciation for Division 1 LPCI INJECTION VALVE ΔP PERMISSIVE via the HMI when 1oo1 manual initiation votes **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 annunciate votes for RIVDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-154	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E11-F017A or terminate valve motion midstream from the control room.	Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-155	Division 1 shall provide valve E11-F017A position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-156	Division 1 shall inhibit valve E11-F017A from being manually opened if 0oo1 condition votes for RIDVP are received.	Original design feature	
RHR-FR-157	Division 1 shall be capable of manually overriding the any of the LPCI initiation signals (auto or manual) in order to close valve E11-F017A.	Original design feature	
RHR-FR-158	Division 1 shall provide indicating light capability via the HMI when the LPCI initiation signal is manually overridden to close valve E11-F017A.	Original design feature	
RHR-FR-159	Division 2 shall provide an output to open injection valve E11-F017B when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for RIVDP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-160	Division 2 shall provide an output to open injection valve E11-F017B when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for RIVDP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-161	Division 2 shall provide an output to open injection valve E11-F017B when 1oo1 manual initiation votes **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for RIVDP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-162	Division 2 shall provide annunciation for Division 2 LPCI INJECTION VALVE ΔP PERMISSIVE via the HMI when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 annunciate votes for RIVDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-163	Division 2 shall provide annunciation for Division 2 LPCI INJECTION VALVE ΔP PERMISSIVE via the HMI when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 annunciate votes for RIVDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-164	Division 2 shall provide annunciation for Division 2 LPCI INJECTION VALVE ΔP PERMISSIVE via the HMI when 1oo1 manual initiation votes **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 annunciate votes for RIVDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-165	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E11-F017B or terminate valve motion midstream from the control room.	Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-166	Division 2 shall provide valve E11-F017B position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-167	Division 2 shall inhibit valve E11-F017B from being manually opened if 0oo1 condition votes for RIDVP are received.	Original design feature	
RHR-FR-168	Division 2 shall be capable of manually overriding the any of the LPCI initiation signals (auto or manual) in order to close valve E11-F017B.	Original design feature	
RHR-FR-169	System Division 2 shall provide indicating light capability via the HMI when the LPCI initiation signal is manually overridden to close valve E11-F017B.	Original design feature	
RHR-FR-170	Division 3 shall provide an output to open injection valve E11-F017C when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for RIVDP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-171	Division 3 shall provide an output to open injection valve E11-F017C when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for RIVDP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-172	Division 3 shall provide an output to open injection valve E11-F017C when 1oo1 manual initiation votes **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for RIVDP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-173	Division 3 shall provide annunciation for Division 3 LPCI INJECTION VALVE ΔP PERMISSIVE via the HMI when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 annunciate votes for RIVDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-174	Division 3 shall provide annunciation for Division 3 LPCI INJECTION VALVE ΔP PERMISSIVE via the HMI when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 annunciate votes for RIVDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-175	Division 3 shall provide annunciation for Division 3 LPCI INJECTION VALVE ΔP PERMISSIVE via the HMI when 1oo1 manual initiation votes **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 annunciate votes for RIVDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-176	Division 3 shall provide a means to manually introduce a momentary signal to open or close valve E11-F017C or terminate valve motion midstream from the control room.	Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-177	Division 3 shall provide valve E11-F017C position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-178	Division 3 shall inhibit valve E11-F017C from being manually opened if 0oo1 condition votes for RIDVP are received.	Original design feature	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-179	Division 3 shall be capable of manually overriding the any of the LPCI initiation signals (auto or manual) in order to close valve E11-F017C.	Original design feature	
RHR-FR-180	System Division 3 shall provide indicating light capability via the HMI when the LPCI initiation signal is manually overridden to close valve E11-F017C.	Original design feature	
RHR-FR-181	Division 4 shall provide an output to open injection valve E11-F017D when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for RIVDP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-182	Division 4 shall provide an output to open injection valve E11-F017D when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for RIVDP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-183	Division 4 shall provide an output to open injection valve E11-F017D when 1oo1 manual initiation votes **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 condition votes for RIVDP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-184	Division 4 shall provide annunciation for Division 4 LPCI INJECTION VALVE ΔP PERMISSIVE via the HMI when 2oo4 LOCA votes for RWL1 input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 annunciate votes for RIVDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-185	Division 4 shall provide annunciation for Division 4 LPCI INJECTION VALVE ΔP PERMISSIVE via the HMI when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 annunciate votes for RIVDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-186	Division 4 shall provide annunciation for Division 4 LPCI INJECTION VALVE ΔP PERMISSIVE via the HMI when 1oo1 manual initiation votes **AND** 1oo1 condition votes for CI1 input **AND** 1oo1 annunciate votes for RIVDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-187	Division 4 shall provide a means to manually introduce a momentary signal to open or close valve E11-F017D or terminate valve motion midstream from the control room.	Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-188	Division 4 shall provide valve E11-F017D position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-189	Division 4 shall inhibit valve E11-F017D from being manually opened if 0oo1 condition votes for RIDVP are received.	Original design feature	
RHR-FR-190	Division 4 shall be capable of manually overriding the any of the LPCI initiation signals (auto or manual) in order to close valve E11-F017D.	Original design feature	
RHR-FR-191	System Division 4 shall provide indicating light capability via the HMI when the LPCI initiation signal is manually overridden to close valve E11-F017D.	Original design feature	
RHR-FR-192	Division 1 shall provide an output to open valve E11-F048A for 3 minutes when 2oo4 LOCA votes for RWL1 input are received.	GDC 13, GDC 20, GDC 29, GDC 38,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-193	Division 1 shall provide an output to open valve E11-F048A for 3 minutes when 2oo4 LOCA votes for DHP/RLP input are received.	GDC 13, GDC 20, GDC 29, GDC 38,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-194	Division 1 shall provide an output to open valve E11-F048A for 3 minutes when 1oo1 manual initiation votes is received.	GDC 13, GDC 20, GDC 29, GDC 38,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-195	Division 1 shall generate an output for alarm capability via the HMI to alert operators to close valve E11-F048A after 10 minutes following receipt of a LOCA signal.	Stakeholder comment	
RHR-FR-196	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E11-F048A or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-197	Division 1 shall provide valve E11-F048A position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-198	Division 1 shall provide an output to close valve E11-F024A when 2oo4 LOCA votes for RWL1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-199	Division 1 shall provide an output to close valve E11-F024A when 2oo4 LOCA votes for DHP/RLP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-200	Division 1 shall provide an output to close valve E11-F024A when 1oo1 manual initiation votes is received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-201	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E11-F024A or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-202	Division 1 shall provide valve E11-F024A position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-203	Division 1 shall be capable of manually overriding the LPCI initiation signal in order to open valve E11-F024A when 1oo1 condition votes for CI3 input is received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-204	Division 1 shall provide an output to close valve E11-F027A when 2oo4 LOCA votes for RWL1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-205	Division 1 shall provide an output to close valve E11-F027A when 2oo4 LOCA votes for DHP/RLP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-206	Division 1 shall provide an output to close valve E11-F027A when 1oo1 manual initiation votes is received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-207	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E11-F027A or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-208	Division 1 shall provide valve E11-F027A position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-209	Division 1 shall be capable of manually overriding the LPCI initiation signal in order to open valve E11-F027A when 1oo1 condition votes for CI3 input is received.	GDC 38,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-210	Division 1 shall provide an output to close valve E11-F103A when 2oo4 LOCA votes for RWL1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-211	Division 1 shall provide an output to close valve E11-F103A when 2oo4 LOCA votes for DHP/RLP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-212	Division 1 shall provide an output to close valve E11-F103A when 1oo1 manual initiation votes is received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-213	Division 1 shall provide valve E11-F103A position indication by computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-214	Division 1 shall provide an output to close valve E11-F104A when 2oo4 LOCA votes for RWL1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-215	Division 1 shall provide an output to close valve E11-F104A when 2oo4 LOCA votes for DHP/RLP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-216	Division 1 shall provide an output to close valve E11-F104A when 1oo1 manual initiation votes is received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-217	Division 2 shall provide an output to open valve E11-F048B for 3 minutes when 2oo4 LOCA votes for RWL1 input are received.	GDC 38,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-218	Division 2 shall provide an output to open valve E11-F048B for 3 minutes when 2oo4 LOCA votes for DHP/RLP input are received.	GDC 38,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-219	Division 2 shall provide an output to open valve E11-F048B for 3 minutes when 1oo1 manual initiation votes is received.	GDC 38,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-220	Division 2 shall generate an output for alarm capability via the HMI to alert operators to close valve E11-F048B after 10 minutes following receipt of a LOCA signal.	Stakeholder comment	
RHR-FR-221	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E11-F048B or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-222	Division 2 shall provide valve E11-F048B position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-223	Division 2 shall provide an output to close valve E11-F024B when 2oo4 LOCA votes for RWL1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-224	Division 2 shall provide an output to close valve E11-F024B when 2oo4 LOCA votes for DHP/RLP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-225	Division 2 shall provide an output to close valve E11-F024B when 1oo1 manual initiation votes is received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-226	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E11-F024B or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-227	Division 2 shall provide valve E11-F024B position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-228	Division 2 shall be capable of manually overriding the LPCI initiation signal in order to open valve E11-F024B when 1oo1 condition votes for CI4 input is received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-229	Division 2 shall provide an output to close valve E11-F027B when 2oo4 LOCA votes for RWL1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-230	Division 2 shall provide an output to close valve E11-F027B when 2oo4 LOCA votes for DHP/RLP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-231	Division 2 shall provide an output to close valve E11-F027B when 1oo1 manual initiation votes is received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-232	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E11-F027B or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-233	Division 2 shall provide valve E11-F027B position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-234	Division 2 shall be capable of manually overriding the LPCI initiation signal in order to open valve E11-F027B when 1oo1 condition votes for CI3 input is received.	GDC 38,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-235	Division 2 shall provide an output to close valve E11-F103B when 2oo4 LOCA votes for RWL1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-236	Division 2 shall provide an output to close valve E11-F103B when 2oo4 LOCA votes for DHP/RLP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-237	Division 2 shall provide an output to close valve E11-F103B when 1oo1 manual initiation votes is received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-238	Division 2 shall provide an output to close valve E11-F104B when 2oo4 LOCA votes for RWL1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-239	Division 2 shall provide an output to close valve E11-F104B when 2oo4 LOCA votes for DHP/RLP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-240	Division 2 shall provide an output to close valve E11-F104B when 1oo1 manual initiation votes is received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-241	Division 2 shall provide computer data to the non-SR DCS platform for valve E11-F104B position indication based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-242	Division 3 shall provide an output to close valve E11-F010A and an output to inhibit the manual opening of valve E11-F010A when 2oo4 LOCA votes for RWL1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-243	Division 3 shall provide an output to close valve E11-F010A and an output to inhibit the manual opening of valve E11-F010A when 2oo4 LOCA votes for DHP/RLP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-244	Division 3 shall provide an output to close valve E11-F010A and an output to inhibit the manual opening of valve E11-F010A when 1oo1 manual initiation votes is received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-245	Division 3 shall provide a means to manually introduce a momentary signal to open or close valve E11-F010A or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-246	Division 3 shall provide valve E11-F010A position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-247	Division 4 shall provide an output to close valve E11-F010B and an output to inhibit the manual opening of valve E11-F010B when 2oo4 LOCA votes for RWL1 input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-248	Division 4 shall provide an output to close valve E11-F010B and an output to inhibit the manual opening of valve E11-F010B when 2oo4 LOCA votes for DHP/RLP input are received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-249	Division 4 shall provide an output to close valve E11-F010B and an output to inhibit the manual opening of valve E11-F010B when 1oo1 manual initiation votes is received.	GDC 13, GDC 20, GDC 29,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-250	Division 4 shall provide a means to manually introduce a momentary signal to open or close valve E11-F010B or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-251	Division 4 shall provide valve E11-F010B position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-252	Division 1 shall provide an output to open valve E11-F007A when 1oo1 condition votes for CI27 input **AND** 0oo1 condition votes for RLDF input are received	Original design feature	
RHR-FR-253	Division 1 shall provide an output to close valve E11-F007A when 1oo1 condition votes for RLDF input is received.	Original design feature	
RHR-FR-254	Division 1 shall provide indicating light capability via the HMI when 1oo1 annunciate votes for RLDF input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-255	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E11-F007A or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-256	Division 1 shall provide valve E11-F007A position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-257	Division 2 shall provide an output to open valve E11-F007B when 1oo1 condition votes for CI27 input **AND** 0oo1 condition votes for RLDF input are received.	Original design feature	
RHR-FR-258	Division 2 shall provide an output to close valve E11-F007B when 1oo1 condition votes for RLDF input is received.	Original design feature	
RHR-FR-259	Division 2 shall provide indicating light capability via the HMI when 1oo1 annunciate votes for RLDF input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-260	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E11-F007B or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-261	Division 2 shall provide valve E11-F007B position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-262	Division 3 shall provide an output to open valve E11-F007C when 1oo1 condition votes for CI27 input **AND** 0oo1 condition votes for RLDF input are received.	Original design feature	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-263	Division 3 shall provide an output to close valve E11-F007C when 1oo1 condition votes for RLDF input is received.	Original design feature	
RHR-FR-264	Division 3 shall provide indicating light capability via the HMI when 1oo1 annunciate votes for RLDF input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-265	Division 3 shall provide a means to manually introduce a momentary signal to open or close valve E11-F007C or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-266	Division 3 shall provide valve E11-F007C position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-267	Division 4 shall provide an output to open valve E11-F007D when 1oo1 condition votes for CI27 input **AND** 0oo1 condition votes for RLDF input are received.	Original design feature	
RHR-FR-268	Division 4 shall provide an output to close valve E11-F007D when 1oo1 condition votes for RLDF input is received.	Original design feature	
RHR-FR-269	Division 4 shall provide indicating light capability via the HMI when 1oo1 annunciate votes for RLDF input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-270	Division 4 shall provide a means to manually introduce a momentary signal to open or close valve E11-F007D or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-271	Division 4 shall provide valve E11-F007D position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-272	Each division shall provide the capability to manually reset the LPCI initiation once the initiating condition has cleared.	Original design feature	
RHR-FR-273	Each division shall provide a means to manually introduce a momentary signal to the pump control circuit to start or stop the associated RHR pump.	Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-274	Each division shall provide RHR pump operating status capability via the HMI based on contact inputs from the associated pump control circuit.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-275	Each division shall seal in a block signal when the RHR pump is manually stopped that prevents the LPCI initiation signal from restarting the RHR Pump until a manual start signal is provided to the pump control circuit.	Original design feature	
RHR-FR-276	Each division shall provide indicating light capability via the HMI when the block signal seal in is present.	Original design feature	
RHR-FR-277	Division 1 shall provide a stop command to the RHR pump A control circuit when 1oo1 condition votes for CI9 input **AND** 1oo1 condition votes for CI10 input are received.	Original design feature	
RHR-FR-278	Division 1 shall provide a stop command to the RHR pump A control circuit when 1oo1 condition votes for CI17 input **AND** 1oo1 condition votes for CI10 input are received.	Original design feature	
RHR-FR-279	Division 1 shall provide a stop command to the RHR pump A control circuit when 1oo1 condition votes for CI18 input **AND** 1oo1 condition votes for CI10 input are received.	Original design feature	
RHR-FR-280	Division 2 shall provide a stop command to the RHR pump B control circuit when 1oo1 condition votes for CI11 input **AND** 1oo1 condition votes for CI12 input are received.	Original design feature	
RHR-FR-281	Division 2 shall provide a stop command to the RHR pump B control circuit when 1oo1 condition votes for CI17 input **AND** 1oo1 condition votes for CI12 input are received.	Original design feature	
RHR-FR-282	Division 2 shall provide a stop command to the RHR pump B control circuit when 1oo1 condition votes for CI18 input **AND** 1oo1 condition votes for CI12 input are received.	Original design feature	
RHR-FR-283	Division 3 shall provide a stop command to the RHR pump C control circuit when 1oo1 condition votes for CI13 input is received.	Original design feature	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-284	Division 4 shall provide a stop command to the RHR pump D control circuit when 1oo1 condition votes for CI13 input is received.	Original design feature	
RHR-FR-285	Division 1 shall provide a means to manually open or close valve E11-F016A, under administrative control, from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-286	Division 1 shall provide valve E11-F016A position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-287	Division 1 shall be capable of manually opening valve E11-F016A when 2oo4 LOCA votes for RWL1 input **AND** 2oo4 condition votes for DHP input **AND** 1oo1 condition votes for CI3 input are received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-288	Division 1 shall be capable of manually opening valve E11-F016A when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI3 input are received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-289	Division 1 shall be capable of manually opening valve E11-F016A when 1oo1 condition votes for CI5 input is received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-290	Division 1 shall provide a means to manually open or close valve E11-F021A, under administrative control, from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-291	Division 1 shall provide valve E11-F021A position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-292	Division 1 shall be capable of manually opening valve E11-F021A when 2oo4 LOCA votes for RWL1 input **AND** 2oo4 condition votes for DHP input **AND** 1oo1 condition votes for CI3 input are received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-293	Division 1 shall be capable of manually opening valve E11-F021A when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI3 input are received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-294	Division 1 shall be capable of manually opening valve E11-F021A when 1oo1 condition votes for CI6 input is received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-295	Division 2 shall provide a means to manually open or close valve E11-F016B, under administrative control, from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-296	Division 2 shall provide valve E11-F016B position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-297	Division 2 shall be capable of manually opening valve E11-F016B when 2oo4 LOCA votes for RWL1 input **AND** 2oo4 condition votes for DHP input **AND** 1oo1 condition votes for CI4 input are received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-298	Division 2 shall be capable of manually opening valve E11-F016B when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI4 input are received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-299	Division 2 shall be capable of manually opening valve E11-F016B when 1oo1 condition votes for CI7 input is received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-300	Division 2 shall provide a means to manually open or close valve E11-F021B, under administrative control, from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-301	Division 2 shall provide valve E11-F021B position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-302	Division 2 shall be capable of manually opening valve E11-F021B when 2oo4 LOCA votes for RWL1 input **AND** 2oo4 condition votes for DHP input **AND** 1oo1 condition votes for CI4 input are received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-303	Division 2 shall be capable of manually opening valve E11-F021B when 2oo4 LOCA votes for DHP/RLP input **AND** 1oo1 condition votes for CI4 input are received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-304	Division 2 shall be capable of manually opening valve E11-F021B when 1oo1 condition votes for CI8 input is received.	GDC 38, Reg Guide 1.62,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-305	Division 1 shall provide a means to manually open or close valve E11-F004A, under administrative control, from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-306	Division 1 shall provide annunciation for SUCTION VALVE FULLY CLOSED CONTROL SW IN CLOSE POSITION and status light capability via the HMI when valve E11-F004A is manually closed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-307	Division 1 shall inhibit the opening of valve E11-F004A when 1oo1 condition votes for CI19 input is received.	GDC 34	
RHR-FR-308	Division 1 shall provide valve E11-F004A position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-309	Division 2 shall provide a means to manually open or close valve E11-F004B, under administrative control, from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-310	Division 2 shall provide annunciation for SUCTION VALVE FULLY CLOSED CONTROL SW IN CLOSE POSITION and status light capability via the HMI when valve E11-F004B is manually closed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-311	Division 2 shall inhibit the opening of valve E11-F004B when 1oo1 condition votes for CI20 input is received.	GDC 34	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-312	Division 2 shall provide valve E11-F004B position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-313	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E11-F006A or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-314	Division 1 shall provide valve E11-F006A position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-315	Division 1 shall inhibit the opening of valve E11-F004A when 1oo1 condition votes for CI21 input is received.	Original design feature	
RHR-FR-316	Division 1 shall inhibit the opening of valve E11-F004A when 1oo1 condition votes for CI22 input is received.	Original design feature	
RHR-FR-317	Division 1 shall inhibit the opening of valve E11-F004A when 1oo1 condition votes for CI23 input is received.	Original design feature	
RHR-FR-318	Division 1 shall provide valve E11-F060A position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-319	Division 1 shall provide valve E11-F065A position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-320	Division 2 shall provide a means to manually introduce a momentary signal to open or close valve E11-F006B or terminate valve motion midstream from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-321	Division 2 shall provide valve E11-F006B position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-322	Division 2 shall inhibit the opening of valve E11-F004B when 1oo1 condition votes for CI24 input is received.	Original design feature	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-323	Division 2 shall inhibit the opening of valve E11-F004B when 1oo1 condition votes for CI25 input is received.	Original design feature	
RHR-FR-324	Division 2 shall inhibit the opening of valve E11-F004B when 1oo1 condition votes for CI26 input is received.	Original design feature	
RHR-FR-325	Division 2 shall provide valve E11-F060B position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-326	Division 2 shall provide valve E11-F065B position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-327	Division 3 shall provide a means to manually open or close valve E11-F004C, under administrative control, from the control room.	GDC 34	
RHR-FR-328	Division 3 shall provide annunciation for RHR OR SLC OUT OF SERVICE and status light capability via the HMI when valve E11-F004C is manually closed.	Reg Guide 1.47 (BISI), IEEE Standard 279	
RHR-FR-329	Division 3 shall inhibit the opening of valve E11-F004C when 1oo1 condition votes for CI15 input is received.	GDC 34	
RHR-FR-330	Division 3 shall provide valve E11-F004C position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-331	Division 3 shall provide valve E11-F065C position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-332	Division 4 shall provide a means to manually open or close valve E11-F004D, under administrative control, from the control room.	GDC 34	
RHR-FR-333	Division 4 shall provide annunciation for RHR OR SLC OUT OF SERVICE and status light capability via the HMI when valve E11-F004D is manually closed.	Reg Guide 1.47 (BISI), IEEE Standard 279	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-334	Division 4 shall inhibit the opening of valve E11-F004D when 1oo1 condition votes for CI16 input is received.	GDC 34	
RHR-FR-335	Division 4 shall provide valve E11-F004D position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-336	Division 3 shall provide valve E11-F065D position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-337	Division 1 shall provide a means to manually open or close valve E11-F003A, under administrative control, from the control room.	Reg Guide 1.97,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-338	Division 1 shall provide valve E11-F003A position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-339	Division 2 shall provide a means to manually open or close valve E11-F003B, under administrative control, from the control room.	Reg Guide 1.97,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-340	Division 2 shall provide valve E11-F003B position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-341	Division 1 shall provide a means to manually open or close valve E11-F047A, under administrative control, from the control room.	Reg Guide 1.97,IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-342	Division 1 shall provide valve E11-F047A position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-343	Division 2 shall provide a means to manually open or close valve E11-F047B, under administrative control, from the control room.	Reg Guide 1.97,IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-344	Division 2 shall provide valve E11-F047B position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-345	Division 1 shall provide a means to manually test valves E11-F041A from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-346	Division 1 shall provide valve E11-F041A position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-347	Division 2 shall provide a means to manually test valve E11-F041B from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-348	Division 2 shall provide valve E11-F041B position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-349	Division 3 shall provide a means to manually test valve E11-F041C from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-350	Division 3 shall provide valve E11-F041C position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-351	Division 4 shall provide a means to manually test valve E11-F041D from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-352	Division 4 shall provide valve E11-F041D position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-353	Division 1 shall provide a means to manually test valve E11-F050A from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-354	Division 1 shall provide valve E11-F050A position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-355	Division 2 shall provide a means to manually test valve E11-F050B from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-356	Division 2 shall provide valve E11-F050B position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-357	Division 2 shall provide a means to manually open or close valve E11-F075, under administrative control, from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	Requirement as written describes Division 3 (B loop) for Unit 1. Unit 2 will be Division 1 (A loop).
RHR-FR-358	Division 2 shall provide valve E11-F075 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-359	Division 2 shall provide a permissive to manually open or close valve E11-F074 from the control room based on the manual operation of valve E11-F075.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-360	Division 2 shall provide a means to manually open or close valve E11-F073, under administrative control, from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-361	Division 2 shall provide valve E11-F073 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-362	Division 2 shall provide a permissive to manually open or close valve E11-F074 from the control room based on the manual operation of valve E11-F075.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-363	Division 1 shall provide valve E11-F077 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-364	Channel A shall condition the RPDF input through a square root converter and provide the resultant flow signal to Division 1.	GDC 34, GDC 35, GDC 38, Reg Guide 1.97, Reg Guide 1.105	
RHR-FR-365	Division 1 shall provide the RPDF flow signal for indicator capability via the HMI and transmit computer data to the non-SR DCS platform.	Reg Guide 1.97	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-366	Channel B shall condition the RPDF input through a square root converter and provide the resultant flow signal to Division 2.	GDC 34, GDC 35, GDC 38, Reg Guide 1.97, Reg Guide 1.105	
RHR-FR-367	Division 2 shall provide the RPDF flow signal for indicator capability via the HMI and transmit computer data to the non-SR DCS platform.	Reg Guide 1.97	
RHR-FR-368	Channel C shall condition the RPDF input through a square root converter and provide the resultant flow signal to Division 3.	GDC 34, GDC 35, GDC 38, Reg Guide 1.97, Reg Guide 1.105	
RHR-FR-369	Division 3 shall provide the RPDF flow signal for indicator capability via the HMI and transmit computer data to the non-SR DCS platform.	Reg Guide 1.97	
RHR-FR-370	Channel D shall condition the RPDF input through a square root converter and provide the resultant flow signal to Division 4.	GDC 34, GDC 35, GDC 38, Reg Guide 1.97, Reg Guide 1.105	
RHR-FR-371	Division 4 shall provide the RPDF flow signal for indicator capability via the HMI and transmit computer data to the non-SR DCS platform.	Reg Guide 1.97	
RHR-FR-372	Division 1 shall provide annunciation for RHR SHUTDOWN HEADER HI PRESS via the HMI when 1oo1 annunciate votes for RSSCP input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-373	Division 1 shall provide annunciation for RHR PUMP DISCHARGE HI/LO PRESS via the HMI when 1oo1 annunciate votes for RPDP high input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-374	Division 1 shall provide annunciation for RHR PUMP DISCHARGE HI/LO PRESS via the HMI when 1oo1 annunciate votes for RPDP low input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-375	Division 2 shall provide annunciation for RHR PUMP DISCHARGE HI/LO PRESS via the HMI when 1oo1 annunciate votes for RPDP high input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-376	Division 2 shall provide annunciation for RHR PUMP DISCHARGE HI/LO PRESS via the HMI when 1oo1 annunciate votes for RPDP low input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-377	Division 3 shall provide annunciation for RHR PUMP DISCHARGE HI/LO PRESS via the HMI when 1oo1 annunciate votes for RPDP high input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-378	Division 3 shall provide annunciation for RHR PUMP DISCHARGE HI/LO PRESS via the HMI when 1oo1 annunciate votes for RPDP low input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-379	Division 4 shall provide annunciation for RHR PUMP DISCHARGE HI/LO PRESS via the HMI when 1oo1 annunciate votes for RPDP high input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-380	Division 4 shall provide annunciation for RHR PUMP DISCHARGE HI/LO PRESS via the HMI when 1oo1 annunciate votes for RPDP low input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-381	Division 1 shall provide annunciation for LPCI LINE INTERNAL BREAK via the HMI when 1oo1 annunciate votes for LLDP high input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-382	Division 1 shall provide annunciation for LPCI LINE INTERNAL BREAK via the HMI when 1oo1 annunciate votes for LLDP low input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-383	Division 2 shall provide annunciation for LPCI LINE INTERNAL BREAK via the HMI when 1oo1 annunciate votes for LLDP high input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-384	Division 2 shall provide annunciation for LPCI LINE INTERNAL BREAK via the HMI when 1oo1 annunciate votes for LLDP low input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-385	Division 1 shall provide annunciation for RHR AUTO START via the HMI when 1oo1 annunciate votes for CI28 input is received **AND** the manual control switch for RHP pump A is in AUTO position.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-386	Division 2 shall provide annunciation for RHR AUTO START via the HMI when 1oo1 annunciate votes for CI28 input is received **AND** the manual control switch for RHP pump B is in AUTO position.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-387	Division 3 shall provide annunciation for RHR AUTO START via the HMI when 1oo1 annunciate votes for CI28 input is received **AND** the manual control switch for RHP pump C is in AUTO position.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-388	Division 4 shall provide annunciation for RHR AUTO START via the HMI when 1oo1 annunciate votes for CI28 input is received **AND** the manual control switch for RHP pump D is in AUTO position.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RHR-FR-389	Division 1 shall provide annunciation for RHR OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI29 input is received.	Reg Guide 1.47 (BISI), IEEE Standard 279	
RHR-FR-390	Division 2 shall provide annunciation for RHR OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI29 input is received.	Reg Guide 1.47 (BISI), IEEE Standard 279	
RHR-FR-391	Division 3 shall provide annunciation for RHR OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI29 input is received.	Reg Guide 1.47 (BISI), IEEE Standard 279	
RHR-FR-392	Division 4 shall provide annunciation for RHR OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI29 input is received.	Reg Guide 1.47 (BISI), IEEE Standard 279	
RHR-FR-393	Division 1 shall provide annunciation for RHR OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI30 input is received.	Reg Guide 1.47 (BISI), IEEE Standard 279	
RHR-FR-394	Division 2 shall provide annunciation for RHR OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI30 input is received.	Reg Guide 1.47 (BISI), IEEE Standard 279	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-395	Division 3 shall provide annunciation for RHR OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI30 input is received.	Reg Guide 1.47 (BISI), IEEE Standard 279	
RHR-FR-396	Division 4 shall provide annunciation for RHR OUT OF SERVICE via the HMI when 1oo1 annunciate votes for CI30 input is received.	Reg Guide 1.47 (BISI), IEEE Standard 279	
RHR-FR-397	Each division shall provide annunciation for RHR OUT OF SERVICE and alarm light capability via the HMI during any test condition.	Reg Guide 1.47 (BISI), IEEE Standard 279	
RHR-FR-398	Each division shall provide annunciation for RHR OUT OF SERVICE and alarm light capability via the HMI due to any respective RHP pump motor condition (breaker open, loss of power, trip, etc.)	Reg Guide 1.47 (BISI), IEEE Standard 279	
RHR-FR-399	Each division shall provide a means to manually provide annunciation for RHR OUT OF SERVICE and alarm capability via the HMI.	Reg Guide 1.47 (BISI), IEEE Standard 279	
RHR-FR-400	Each division shall provide the means to perform functional tests during normal plant operation.	GDC 37, GDC 40, Reg Guide 1.22, Reg Guide 1.118, IEEE Standard 279	
RHR-FR-401	Each division shall be capable of automatically returning to a LPCI mode from a test mode when a condition is initiated.	Original design feature	
RHR-FR-402	Each division shall provide the means via soft controls on the HMI to automate valve sequencing, alignment and throttling and RHR pump operation to support Suppression Pool Cooling - Normal Mode.	Original design feature	
RHR-FR-403	Each division shall provide the means via soft controls on the HMI to automate valve sequencing, alignment and throttling and RHR pump operation to support Suppression Pool Cooling - Emergency Mode.	Original design feature	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-404	Each division shall provide the means via soft controls on the HMI to automate valve sequencing, alignment and throttling and RHR pump operation to support Suppression Pool Cooling -Alternate Mode.	Original design feature	
RHR-FR-405	Each division shall provide the means via soft controls on the HMI to automate valve sequencing, alignment and throttling and RHR pump operation to support Containment Spray Cooling.	Original design feature	
RHR-FR-406	Each division shall provide the means via soft controls on the HMI to automate valve sequencing, alignment and throttling and RHR pump operation to support Shutdown Cooling.	Original design feature	
RHR-FR-407	Each division shall provide the means via soft controls on the HMI to automate valve sequencing, alignment and throttling and RHR pump operation to support Fuel Pool Cooling Assist.	Original design feature	
RHR-FR-408	Each division shall provide the means via soft controls on the HMI to automate valve sequencing, alignment and throttling and RHR pump operation to support Radwaste Discharge.	Original design feature	
RHR-FR-409	Each division shall provide the means via soft controls on the HMI to automate valve sequencing, alignment and throttling and RHR pump operation to support RHR Service Water Cross-Tie.	Original design feature	
RHR-FR-410	Each division shall provide the means via soft controls on the HMI to automate valve sequencing, alignment and throttling and RHR pump operation to support RHR Alternate Decay Heat Removal (ADHR).	Original design feature	

RHR/LPCI FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RHR Requirement**	**PPS/RHR Source / Basis**	**Notes / Clarification**
RHR-FR-411	Each division shall provide the means via soft controls on the HMI to automate valve sequencing, alignment and throttling and RHR pump operation to support RHR Flow Testing.	Original design feature	
RHR-FR-412	Each channel and each division shall provide sufficient features and documented evaluations to support elimination of most Technical Specification Surveillance Tests, and minimize the requirements for manual calibration checks.	Project design approach	
RHR-FR-413	For all PPS inputs that have the potential to require manual test insertion or external measurement of input values (i.e., use of an external digital multi meter by a technician), test jacks are provided in the cabinets.	Project design approach	
RHR-FR-414	For all inputs that have the potential to require manual multi-point calibration checks with external calibration equipment, knife edge disconnects along with test jacks are incorporated in the field termination panels.	Project design approach	

G

G.1 RCIC Design Requirements

RCIC DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RCIC-DR-1	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. 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. 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.	GDC 1 - Quality standards and records
RCIC-DR-2	Structures, systems, and components important to safety shall be designed to withstand the effect of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions.	GDC 2 - Design Bases for Protection Against Natural Phenomena
RCIC-DR-3	Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions.	GDC 3 - Fire protection
RCIC-DR-4	Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents (LOCAs).	GDC 4 - Environmental and dynamic effects design bases
RCIC-DR-5	The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.	GDC 10 - Reactor design

RCIC DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RCIC-DR-6	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.	GDC 13 - Instrumentation and control
RCIC-DR-7	A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. 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 I&C 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.	GDC 19 - Control Room
RCIC-DR-8	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.	GDC 20 - Protection system functions

RCIC DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RCIC-DR-9	The protection system shall be designed for high functional reliability and in-service 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.	GDC 21 - Protection system reliability and testability
RCIC-DR-10	The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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.	GDC 22- Protection system independence
RCIC-DR-11	The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.	GDC 29 - Protection against anticipated operational occurrences
RCIC-DR-12	The protection system shall be designed to permit periodic testing of its initiation functions inclusive of the actuation devices and actuated equipment when the reactor is in operation.	Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions (Safety Guide 22)

RCIC DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RCIC-DR-13	Those structures, systems, and components (SSC) that should be designed to remain functional if the Safe Shutdown Earthquake (SSE) occurs shall be designated as Seismic Category I. (This includes Systems or portions of systems that are required for reactor shutdown; all electric and mechanical devices and circuitry between the process and the input terminals of the actuator systems involved in generating signals that initiate protective action; systems or portions of systems that are required for (1) monitoring of systems important to safety and (2) actuation of systems important to safety.)	Regulatory Guide 1.29 - Seismic Design Classification
RCIC-DR-14	The RCIC shall comply with the requirements of Appendix B to 10 CFR Part 50 for the installation, inspection, and testing of nuclear power plant instrumentation and electric equipment.	Regulatory Guide 1.30 - Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment (Safety Guide 30)
RCIC-DR-15	The RCIC shall meet the requirements for design, operation and testing of safety-related power systems within nuclear power plants as defined within IEEE Std. 308.	Regulatory Guide 1.32 - Criteria for Power Systems for Nuclear Power Plants
RCIC-DR-16	The RCIC shall meet the requirements for indicating the bypass or inoperable status of portions of the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the system it actuates to perform their safety-related functions:	Regulatory Guide 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
RCIC-DR-17	The RCIC shall comply with the IEEE Std. 279 requirement that any single failure within the protection system shall not prevent proper protective action at the system level when required, by utilizing the guidance in IEEE Std. 379-1972 for applying the single-failure criterion to the design and analysis of nuclear power plant protection systems.	Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Safety Systems
RCIC-DR-18	The RCIC shall provide a means for manual initiation of protective actions.	Regulatory Guide 1.62 - Manual Initiation of Protective Actions

RCIC DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RCIC-DR-19	The RCIC shall meet the requirements for physical independence of the circuits and electric equipment comprising or associated with the Class 1E power system, the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety related functions.	Regulatory Guide 1.75 - Physical Independence of Electric Systems
RCIC-DR-20	The RCIC shall comply with design verification requirements to verify adequacy of design under the most adverse design conditions.	Regulatory Guide 1.89 - Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants
RCIC-DR-21	The RCIC shall comply with the requirement to: (1) provide information required to permit the operator to take preplanned manual actions to accomplish safe plant shutdown; (2) determine whether the reactor trip, engineered safety feature systems, and manually initiated safety systems and other systems important to safety are performing their intended functions (i.e., reactivity control, core cooling, maintaining reactor coolant system integrity, and maintaining containment integrity); (3) provide information to the operators that will enable them to determine the potential for causing a gross breach of the" barriers to radioactivity release (i.e., fuel cladding, reactor coolant pressure boundary, and containment) and to determine if a gross breach of a barrier has occurred.	Regulatory Guide 1.97 - Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants
RCIC-DR-22	The RCIC shall comply with design verification requirements to verify the seismic adequacy of electric equipment.	Regulatory Guide 1.100 - Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants

RCIC DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RCIC-DR-23	The RCIC shall design shall implement setpoints that assure sufficient margin between Technical Specification limits and the trip setpoint to account for instrument inaccuracy, calibration uncertainties and instrument drift. Consideration of instrument span and range as well as environmental influences must be included.	Regulatory Guide 1.105 - Instrument Setpoint
RCIC-DR-24	The RCIC shall comply with the requirements for periodic testing of electric power and protection systems.	Regulatory Guide 1.118 - Periodic Testing of Electric Power and Protection Systems
RCIC-DR-25	The RCIC shall, with precision and reliability, initiate the startup of a steam driven turbine pump and alignment of valves to support a flow injection pathway to the reactor vessel.	IEEE Std. 603, Section 5.0 Safety System Criteria and 6.1 Automatic Control
RCIC-DR-26	The RCIC shall initiate a trip when the analog signal exceeds a level corresponding to the following trip setpoint: Reactor Vessel Water Level 2 < -38 inches Reactor Vessel Water Level 8 > 54 inches	IEEE Std. 603, Section 6.1 Automatic Control
RCIC-DR-27	The RCIC I&C digital platform signal input to actuation output propagation time shall be less than 100 milliseconds.	IEEE Std. 603, Section 4.10
RCIC-DR-28	The RCIC shall be capable of initiating RCIC under all modes of reactor operation.	IEEE Std. 603, Section 4.1
RCIC-DR-29	The RCIC shall be capable of being manually initiated.	IEEE Std. 603, Section 6.2 Manual Control
RCIC-DR-30	The RCIC shall ensure that the protective action, once started, continues to completion.	IEEE Std. 603, Section 5.2 Completion of Protective Action
RCIC-DR-31	Any single failure within the RCIC shall not prevent proper protective action at the system level when required.	IEEE Std. 603, Section 5.1 Single Failure Criterion and IEEE Std. 7-4.3.2 Section 5.1 Single Failure Criterion

RCIC DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RCIC-DR-32	Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.	IEEE Std. 603 section 5.3 Quality and IEEE Std. 7-4.3.2 section 5.3 Quality
RCIC-DR-33	Type test data or reasonable engineering extrapolation based on test data shall be available to verify that protection system equipment shall meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements.	IEEE Std. 603 section 5.4 Equipment Qualification and IEEE Std. 7-4.3.2 section 5.4 Equipment Qualification
RCIC-DR-34	All protection system channels shall be designed to maintain necessary functional capability under extremes of conditions (as applicable) relating to environment, energy supply, malfunctions and accidents.	IEEE Std. 603 section 5.5 System Integrity and IEEE Std. 7-4.3.2 and section 5.5 Independence
RCIC-DR-35	Channels that provide signals for the same protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 System Integrity
RCIC-DR-36	Any equipment that is used for both protective and control functions shall be classified as part of the protection system and shall meet all the applicable requirements.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence
RCIC-DR-37	The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system and shall meet all the applicable requirements. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence

RCIC DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RCIC-DR-38	Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
RCIC-DR-39	Provisions shall be included so that the protective action can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
RCIC-DR-40	Where a credible single event can cause a control system action that results in a condition requiring protective action and can concurrently prevent the protective action from those protection system channels designated to provide principal protection against the condition, then alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design bases.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
RCIC-DR-41	To the extent feasible and practical, protection system inputs shall be derived from signals that are direct measures of the desired variables.	IEEE Std. 603 section 6.4 Derivation of System Inputs
RCIC-DR-42	Means shall be provided for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
RCIC-DR-43	Capability shall be provided for testing and calibrating channels and the devices used to derive the final system output signal from the various channel signals.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
RCIC-DR-44	For those parts of the system where the required interval between testing will be less than the normal time interval between generating station shutdowns, there shall be capability for testing during power operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration

RCIC DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RCIC-DR-45	The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective action at the systems level.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
RCIC-DR-46	During such operation, the active parts of the system shall of themselves continue to meet the single failure criterion.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
RCIC-DR-47	Where operating requirements necessitate automatic or manual bypass of a protective function, the design shall be such that the bypass will be removed automatically whenever permissive conditions are not met.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
RCIC-DR-48	Devices used to achieve automatic removal of the bypass of a protective function are part of the protection system and shall be designed in accordance with these criteria.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
RCIC-DR-49	If the protective action of some part of the system has been bypassed or deliberately rendered inoperative for any purpose, this fact shall be continuously indicated in the control room.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RCIC-DR-50	The design shall permit the administrative control of the means for manually bypassing channels or protective functions.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
RCIC-DR-51	Where it is necessary to change to a more restrictive set point to provide adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of assuring that the more restrictive set point is used.	IEEE Std. 603 section 6.8 Setpoints
RCIC-DR-52	The devices used to prevent improper use of less restrictive set points shall be considered a part of the protection system and shall be designed in accordance with the other provisions of these criteria regarding performance and reliability.	IEEE Std. 603 section 6.8 Setpoints
RCIC-DR-53	The protection system shall be so designed that, once initiated, a protective action at the system level shall go to completion.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action

RCIC DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RCIC-DR-54	Return to operation shall require subsequent deliberate operator action.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action
RCIC-DR-55	The protection system shall include means for manual initiation of each protective action at the system level (for example, reactor trip, containment isolation, safety injection, core spray, etc.).	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
RCIC-DR-56	No single failure within the manual, automatic, or common portions of the protection system shall neither prevent initiation of protective action by manual or automatic means nor falsely initate protective actions.	IEEE Std. 603 section 7.2 Manual Control
RCIC-DR-57	Manual initiation should depend upon the operation of a minimum of equipment.	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
RCIC-DR-58	The design shall permit the administrative control of access to all set point adjustments, module calibration adjustments, and test points.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
RCIC-DR-59	Protective actions shall be indicated and identified down to the channel level.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RCIC-DR-60	The protection system shall be designed to provide the operator with accurate, complete, and timely information pertinent to its own status and to generating station safety.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RCIC-DR-61	The design shall minimize the development of conditions which would cause meters, annunciators, recorders, alarms, etc., to give anomalous indications confusing to the operator.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RCIC-DR-62	The system shall be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.	IEEE Std. 603 section 5.10 Repair

RCIC DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RCIC-DR-63	In order to provide assurance that the requirements given in this document can be applied during the design, construction, maintenance, and operation of the plant, the protection system equipment (for example, interconnecting wiring, components, modules, etc.), shall be identified distinctively as being in the protection system.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
RCIC-DR-64	This identification shall distinguish between redundant portions of the protection system. (In the installed equipment, components, or modules mounted in assemblies that are clearly identified as being in the protection system do not themselves require identification.) All software, firmware, and programmable logic shall be identified in accordance with IEEE Std. 7-4.3.2 Clause 5.11.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
RCIC-DR-65	The RCIC shall conform to the design criteria and features for Class 1E electric systems to ensure that functional requirements under the conditions produced by design basis events are met.	IEEE Std. 308 - Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations
RCIC-DR-66	The RCIC shall conform to the methods for demonstrating the qualification of Class 1E equipment including components or equipment of any interface whose failure could adversely affect the performance of Class 1E systems and electronic equipment.	IEEE Std. 323 - Qualifying Class 1E Equipment for Nuclear Power Generating Stations
RCIC-DR-67	RCIC shall conform to the design and operational criteria for the performance of periodic testing of nuclear power generating station safety systems.	IEEE Std. 338 - Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems
RCIC-DR-68	RCIC shall meet its Class 1E performance requirements during and following one SSE (safe shutdown earthquake) preceeded by a number of OBEs (operating basis earthquakes).	IEEE Std. 344 - Guide for Seismic Qualification of Class 1 Electric Equipment for Nuclear Power Generating Stations
RCIC-DR-69	RCIC shall meet the single failure criterion as described and classified in IEEE Std. 379.	IEEE Std. 379 - Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

RCIC DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RCIC-DR-70	RCIC shall meet the criteria and requirements for establishing and maintaining the independence of Class 1E equipment and circuits and auxiliary supporting features by physical separation and electrical isolation.	IEEE Std. 384 - Criteria for Independence of Class 1E Equipment and Circuits

G.2 RCIC Functional Requirements

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-1	RCIC shall be capable of providing signals to start the steam turbine pump and align valves for delivering water to the reactor as well as to initiate other SR equipment either automatically when any of the monitored parameters exceeds a pre-established value, or by manual initiation.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-2	PPS/RCIC shall be comprised of two (2) independent and separate divisions (Division 1 and Division 3) to perform the following: • Initiate a RCIC turbine pump start • Provide RCIC turbine flow Control • Trip the RCIC turbine • Isolate the RCIC turbine	Reg Guide 1.53, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-3	PPS/RCIC shall have four (4) independent channels (Channel A, Channel B, Channel C and Channel D) that each provide votes / signals to each of the divisions.	Reg Guide 1.53, IEEE Std. 603/IEEE Std. 7-4.3.2	The four channels are common to both divisions.
RCIC-FR-4	The trip system shall be capable of being powered by 125VDC power.	Original design feature	
RCIC-FR-5	Each division shall provide outputs that are capable of interfacing with 125VDC loads.	Original design feature	
RCIC-FR-6	Each channel shall receive an input from each of the following monitored parameters that are provided as common inputs to the PPS platform and are shared by each of the PPS functions: • Reactor Vessel Water Level 2 (low) (RWL2) • Reactor Vessel Water Level 8 (high) (RWL8) • Drywell High Pressure (DHP) • Reactor Vessel Pressure (RVP)	IEEE Std. 603/IEEE Std. 7-4.3.2	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-7	Each channel shall receive an input from each of the following monitored parameters (4-20 mA sensor): • Steam Line Pressure (SLP) • Turbine Exhaust Diaphragm High Pressure (TEDHP)	Original design feature	
RCIC-FR-8	Channel A and Channel C shall receive 4-20 mA inputs for each of the following monitored parameters: • Condensate Storage Tank Level (CSTL) • RCIC Turbine Exhaust Pressure (RTEP) • RCIC Steam Flow (RSF) (forward and reverse)	Original design feature	
RCIC-FR-9	Channel A shall receive a 4-20 mA input for each of the following monitored parameters: • RCIC Pump Flow (RPF1) • RCIC Pump Flow (RPF2) • RCIC Pump Discharge Pressure (RPDP) • RCIC Pump Suction Pressure Low (RCICP1) • RCIC Pump Suction Pressure High (RCICP2) • RCIC Turbine Steam Supply Pressure (RTSSP)	Original design feature	
RCIC-FR-10	Each channel shall receive the following contact inputs: • E51-F045 LS2 (CI9)	Original design feature	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-11	Channel A shall receive the following contact inputs: • RCIC Turbine Conditional Supervisory Alarm (CI1) • RCIC Turbine Trip and Throttle Valve LS4 (CI2) • Barometric Condenser Vacuum Tank Level H1/H2 (CI4) • E51-F029 LS2 (CI5) • E51-F031 LS2 (CI6) • E51-F013 LS13 (CI7) • E51-F013 LS16 (CI8) • E51-N010 LS (CI10) • not used (CI11), (CI12), (CI13), (CI14) • E51-F008 LS11 (CI15) • E51-F060 LS11 (CI17) • RCIC Oil Pressure PS1 (CI18) • RCIC Vacuum Tank Pressure PSH (CI19) • RCIC Turbine Bearing Temperature TS2 (CI20) • RCIC Vacuum Tank Level LOW (CI21) • RCIC Oil Filter Diff Pressure DP-1 (CI22) • RCIC Vacuum Tank Level H1/H2 (CI23) • E51-F080 LS11 (CI24) • E51-F002 LS11 (CI25) • Vacuum pump OL/LOP 49X (CI26) • Condensate Pump OL/LOP 49X (CI27) • E51-F076 LS15 (CI28) • E51-F060 LS2 (CI29)	Original design feature	
RCIC-FR-12	Channel C shall receive the following contact inputs • E51-F007 LS11 (CI16) • E51-F084 LS11 (CI31)	Original design feature	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-13	Channel A and Channel C shall receive the following contact inputs (cont'd): • E51-F045 LS6 (CI3) • Associated RCIC valve motor overcurrent (CI30)	Original design feature	
RCIC-FR-14	Channels A and C shall receive the following digital inputs from PPS/N4S: • RCIC area temperatures (isolate) (DI1)	Original design feature	
RCIC-FR-15	Channel A shall provide an annunciate vote to Division 1 when CI1 is satisfied (contact closed) after a 15 second time delay.	Project design approach	
RCIC-FR-16	Channel A shall provide a condition vote to Division 1 when CI1 is satisfied (contact closed).	Project design approach	
RCIC-FR-17	Channel A shall provide a condition vote to Division 1 when CI2 is satisfied (contact closed)	Project design approach	
RCIC-FR-18	Channel A shall provide an annunciate vote to Division 1 when CI2 is satisfied (contact closed)	Project design approach	
RCIC-FR-19	Channel A shall provide a condition vote to Division 1 when CI3 is satisfied (contact open)	Project design approach	
RCIC-FR-20	Channel C shall provide a condition vote to Division 3 when CI3 is satisfied (contact open)	Project design approach	
RCIC-FR-21	Channel A shall provide a condition vote to Division 1 when CI4 is satisfied (contact closed).	Project design approach	
RCIC-FR-22	Channel A shall provide a condition vote to Division 1 when CI5 is satisfied (contact closed)	Project design approach	
RCIC-FR-23	Channel A shall provide a condition vote to Division 1 when CI6 is satisfied (contact closed)	Project design approach	
RCIC-FR-24	Channel A shall provide a condition vote to Division 1 when CI7 is satisfied (contact closed)	Project design approach	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-25	Channel A shall provide a condition vote to Division 1 when CI8 is satisfied (contact closed)	Project design approach	
RCIC-FR-26	Channel A shall provide an open vote to Division 1 when CI10 is satisfied (contact closed)	Project design approach	
RCIC-FR-27	Channel A shall provide an annunciate vote to Division 1 when CI10 is satisfied (contact closed)	Project design approach	
RCIC-FR-28	Channel A shall provide an annunciate vote to Division 1 when CI15 is satisfied (contact closed)	Project design approach	
RCIC-FR-29	Channel C shall provide an annunciate vote to Division 3 when CI16 is satisfied (contact closed)	Project design approach	
RCIC-FR-30	Channel A shall provide an annunciate vote to Division 1 when CI17 is satisfied (contact closed)	Project design approach	
RCIC-FR-31	Channel A shall provide an annunciate vote to Division 1 when CI18 is satisfied (contact closed)	Project design approach	
RCIC-FR-32	Channel A shall provide an annunciate vote to Division 1 when CI19 is satisfied (contact closed)	Project design approach	
RCIC-FR-33	Channel A shall provide an annunciate vote to Division 1 when CI20 is satisfied (contact closed)	Project design approach	
RCIC-FR-34	Channel A shall provide an annunciate vote to Division 1 when CI21 is satisfied (contact closed)	Project design approach	
RCIC-FR-35	Channel A shall provide an annunciate vote to Division 1 when CI22 is satisfied (contact closed)	Project design approach	
RCIC-FR-36	Channel A shall provide an annunciate vote to Division 1 when CI23 is satisfied (contact closed)	Project design approach	
RCIC-FR-37	Channel A shall provide an annunciate vote to Division 1 when CI24 is satisfied (contact closed)	Project design approach	
RCIC-FR-38	Channel A shall provide a condition vote to Division 1 when CI25 is satisfied (contact closed)	Project design approach	
RCIC-FR-39	Channel A shall provide an annunciate vote to Division 1 when CI26 is satisfied (contact closed)	Project design approach	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-40	Channel A shall provide an annunciate vote to Division 1 when CI27 is satisfied (contact closed)	Project design approach	
RCIC-FR-41	Channel A shall provide an annunciate vote to Division 1 when CI28 is satisfied (contact closed)	Project design approach	
RCIC-FR-42	Channel A shall provide a condition vote to Division 1 when CI29 is satisfied (contact closed)	Project design approach	
RCIC-FR-43	Channel A shall provide an annunciate vote to Division 1 when CI30 is satisfied (contact closed)	Project design approach	
RCIC-FR-44	Channel C shall provide an annunciate vote to Division 3 when CI30 is satisfied (contact closed)	Project design approach	
RCIC-FR-45	Channel C shall provide an annunciate vote to Division 3 when CI31 is satisfied (contact closed)	Project design approach	
RCIC-FR-46	Channel A shall provide a vote to start when RPDP exceeds setpoint high.	Project design approach	
RCIC-FR-47	Channel A shall provide the RPDP input to Division 1.	Project design approach	
RCIC-FR-48	Channel A shall condition the RPF1 input through a square root converter and convert dP to a flow signal.	Project design approach	
RCIC-FR-49	Channel A shall provide the resultant RPF1 flow signal to Division 1.	Project design approach	
RCIC-FR-50	Channel A shall provide the RTSSP input to Division 1.	Project design approach	
RCIC-FR-51	Channel A shall provide the RWL2 input to Division 1.	Project design approach	
RCIC-FR-52	Channel A shall provide the RVP input to Division 1.	Project design approach	
RCIC-FR-53	Channel A shall provide a vote to open to Division 1 when RPF2 exceeds setpoint low.	Project design approach	
RCIC-FR-54	Channel A shall provide a vote to annunciate to Division 1 when RPF2 exceeds setpoint low.	Project design approach	
RCIC-FR-55	Channel A shall provide a vote to close to Division 1 when RPF2 exceeds setpoint high.	Project design approach	
RCIC-FR-56	Channel A shall provide a vote to annunciate to Division 1 when RPF2 exceeds setpoint high.	Project design approach	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-57	Channel A shall provide a vote to transfer to each division when CSTL exceeds setpoint low after a 12 second time delay.	Project design approach	
RCIC-FR-58	Channel A shall provide an annunciate vote to each division when CSTL exceeds setpoint low after a 12 second time delay.	Project design approach	
RCIC-FR-59	Channel C shall provide a vote to transfer to each division when CSTL exceeds setpoint low after a 12 second time delay.	Project design approach	
RCIC-FR-60	Channel C shall provide an annunciate vote to each division when CSTL exceeds setpoint low after a 12 second time delay.	Project design approach	
RCIC-FR-61	Channel A shall provide a vote to trip to Division 1 when RCICP1 exceeds setpoint low.	Project design approach	
RCIC-FR-62	Channel A shall provide a vote to annunciate to Division 1 when RCICP1 exceeds setpoint low.	Project design approach	
RCIC-FR-63	Channel A shall provide the RCICP2 input to Division 1.	Project design approach	
RCIC-FR-64	Channel A shall provide a vote to annunciate to Division 1 when RCICP2 exceeds setpoint high.	Project design approach	
RCIC-FR-65	Channel A shall provide a vote to trip to each division when HTEP exceeds setpoint high.	Project design approach	
RCIC-FR-66	Channel A shall provide an annunciate vote to each division when HTEP exceeds setpoint high.	Project design approach	
RCIC-FR-67	Channel A shall provide the RTEP input to Division 1.	Project design approach	
RCIC-FR-68	Channel C shall provide a vote to trip to each division when HTEP exceeds setpoint high.	Project design approach	
RCIC-FR-69	Channel C shall provide an annunciate vote to each division when HTEP exceeds setpoint high.	Project design approach	
RCIC-FR-70	Channel A shall provide a vote to isolate to each division when RSF exceeds setpoint high after a three (3) second time delay.	Project design approach	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-71	Channel A shall provide a vote to annunciate to each division when RSF exceeds setpoint high after a three (3) second time delay.	Project design approach	
RCIC-FR-72	Channel A shall provide a vote to isolate to each division when RSF exceeds setpoint low after a three (3) second time delay.	Project design approach	
RCIC-FR-73	Channel A shall provide a vote to annunciate to each division when RSF exceeds setpoint low after a three (3) second time delay.	Project design approach	
RCIC-FR-74	Channel C shall provide a vote to isolate to each division when RSF exceeds setpoint high after a three (3) second time delay.	Project design approach	
RCIC-FR-75	Channel C shall provide a vote to annunciate to each division when RSF exceeds setpoint high after a three (3) second time delay.	Project design approach	
RCIC-FR-76	Channel C shall provide a vote to isolate to each division when RSF exceeds setpoint low after a three (3) second time delay.	Project design approach	
RCIC-FR-77	Channel C shall provide a vote to annunciate to each division when RSF exceeds setpoint low after a three (3) second time delay.	Project design approach	
RCIC-FR-78	Channel A shall provide an isolate vote to each division when DI1 is satisfied.	Project design approach	
RCIC-FR-79	Channel C shall provide an isolate vote to each division when DI1 is satisfied.	Project design approach	
RCIC-FR-80	Each channel shall provide a vote to isolate to each division when SLP exceeds setpoint low.	Project design approach	
RCIC-FR-81	Each channel shall provide a vote to annunciate to each division when SLP exceeds setpoint low.	Project design approach	
RCIC-FR-82	Each channel shall provide a vote to isolate to each division when TEDHP exceeds setpoint high.	Project design approach	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-83	Each channel shall provide a vote to annunciate to each division when TEDHP exceeds setpoint high.	Project design approach	
RCIC-FR-84	Each input to a channel (ma, contact input, or digital signal) shall be voted on by the channel based on the condition (condition met or not met).	Project design approach	The term "shall be voted on" indicates that the channel performs a bi-stable comparison against a pre-determined configurable setpoint to determine whether the input is at or above/below the setpoint value.
RCIC-FR-85	Each channel shall provide the status of the vote (e.g. vote to not function if condition not met; vote to function if condition met; vote to annunciate) to each of the divisions.	Project design approach	The terms “not function”, “function”, “annunciate” describe different types of votes that may be provided by a channel (Note -others may be specified within the requirements). A particular vendor solution may combine one or more of the vote types into a single channel vote based on the capabilities of the platform.
RCIC-FR-86	Each division shall determine whether the votes to function for each type of input satisfy the voting criteria (e.g. 2oo4).	Project design approach	
RCIC-FR-87	Each division shall execute a function when the voting criteria is satisfied.	Project design approach	
RCIC-FR-88	Each input to a channel shall have an associated voter (e.g. 2oo4) within each division to ensure that trip inputs are voted separately.	Project design approach	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-89	Each division shall generate an output for an isolation, trip or initiation, when the required voting has been satisfied.	Project design approach	As an example, the RWL2 input to Channels A, B, C and D shall be sent to a 2oo4 voter in each of the divisions (Division 1 and Division 3). When at least two of the four RWL2 inputs to the 2oo4 voter achieves a trip state, the associated division generates an output. The generated output may be dependent on additional voting to be satisfied. Some outputs require different voting schemes which are described within the requirement.
RCIC-FR-90	Channel A shall include a manual initiation feature located in the control room that requires two distinct actions (e.g. arming prior to functioning) to be completed.	GDC 13, GDC 22, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	
RCIC-FR-91	Channel A shall provide a vote to annunciate to Division 1 upon the first distinct action for the associated manual initiation feature being satisfied.	Project design approach	
RCIC-FR-92	Division 1 shall provide annunciation for MANUAL INITIATION SWITCH ARMED via the HMI when 1oo1 annunciate votes are received for the first distinct action for the manual initiation feature.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-93	Channel A shall provide a vote for manual initiation to Division 1 on the second distinct action being satisfied.	Project design approach	
RCIC-FR-94	Each channel shall provide a vote for RCIC pump start to each division when RWL2 input reaches setpoint.	Project design approach	
RCIC-FR-95	Each channel shall provide a vote to shutdown to each division when RWL8 exceeds setpoint high **AND** CI9 is satisfied (contact closed).	Project design approach	
RCIC-FR-96	Each channel shall provide a vote to annunciate to each division when RWL8 exceeds setpoint high **AND** CI9 is satisfied (contact closed).	Project design approach	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-97	Each channel shall seal in the RWL8 input when CI9 is satisfied (contact closed)	Original design feature	
RCIC-FR-98	Each channel shall provide a vote to close when SLP exceeds setpoint low **AND** DHP exceeds setpoint high.	Project design approach	
RCIC-FR-99	Division 1 shall initiate a RCIC turbine pump start when 2oo4 start votes for RWL2 input are received.	GDC 34	
RCIC-FR-100	Division 1 shall initiate a RCIC turbine pump start when 1oo1 manual initiation votes are received.	GDC 34	
RCIC-FR-101	On a RCIC start, Division 1 shall provide an output to an indicating light on the HMI.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-102	Division 1 shall provide the capability to manually reset the indicating light (HMI) unless the RCIC turbine pump start condition is present.	Original design feature	
RCIC-FR-103	Division 1 shall provide a permissive to the RCIC manual isolation logic when the RCIC start logic is satisfied.	Original design feature	
RCIC-FR-104	Division 1 shall inhibit the RCIC manual isolation logic when the RCIC start logic is not satisfied.	Original design feature	
RCIC-FR-105	On a RCIC start, Division 1 shall provide an output to start the barometric condenser vacuum pump (BCVP).	Original design feature	
RCIC-FR-106	Division 1 shall provide a means to manually introduce a momentary signal to start or stop the BCVP by providing a signal to the pump control circuit.	Original design feature	
RCIC-FR-107	Division 1 shall provide BCVP operating status indication via the HMI based on contact inputs from the associated pump control circuit.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-108	On a RCIC start, Division 1 shall provide a signal to close valve E51-F022.	GDC 13, GDC 29, GDC 34	
RCIC-FR-109	Division 1 shall provide an output to close valve E51-F022 when 1oo1 condition votes for CI5 input are received.	GDC 13, Reg Guide 1.22	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-110	Division 1 shall provide an output to close valve E51-F022 when 1oo1 condition votes for CI6 input are received.	GDC 13, Reg Guide 1.22	
RCIC-FR-111	Division 1 shall provide an output to close valve E51-F022 when 1oo1 condition votes for CI8 input are received.	GDC 13, Reg Guide 1.22	
RCIC-FR-112	Division 1 shall provide an interlock that prevents the opening of valve E51-F022 when 0oo1 condition votes for CI7 input is received.	Original design feature	
RCIC-FR-113	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E51-F022 or terminate valve motion midstream from the control room.	GDC 19	
RCIC-FR-114	Division 1 shall provide valve E51-F022 position indication via the HMI based on contact inputs from the associated valve limit switches.	GDC 19, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-115	On a RCIC start, Division 1 shall provide an output to open valve E51-F010 when 0oo1 condition votes for CI5 input is received.	GDC 13, GDC 29, GDC 34, Reg Guide 1.22	
RCIC-FR-116	On a RCIC start, Division 1 shall provide an output to open valve E51-F010 when 0oo1 condition votes for CI6 input is received.	GDC 13, GDC 29, GDC 34, Reg Guide 1.22	
RCIC-FR-117	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E51-F010 or terminate valve motion midstream from the control room.	GDC 19	
RCIC-FR-118	Division 1 shall provide valve E51-F010 position indication via the HMI based on contact inputs from the associated valve limit switches.	GDC 19, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-119	On a RCIC start, Division 1 shall provide an output to open valve E51-F013 when 1oo1 condition votes for CI2 input **AND** 1oo1 condition votes for CI3 input are received.	GDC 13, GDC 29, GDC 34	
RCIC-FR-120	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E51-F013 or terminate valve motion midstream from the control room.	GDC 19	
RCIC-FR-121	Division 1 shall provide valve E51-F013 position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	GDC 19, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-122	Division 1 shall provide a means to manually override the RCIC start initiated open signal to valve E51-F013 to support testing.	Original design feature	
RCIC-FR-123	On a RCIC start, Division 1 shall provide an output to open valve E51-F012.	GDC 13, GDC 29, GDC 34	
RCIC-FR-124	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E51-F012 or terminate valve motion midstream from the control room.	GDC 19	
RCIC-FR-125	Division 1 shall provide valve E51-F012 position indication via the HMI based on contact inputs from the associated valve limit switches.	GDC 19, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-126	Division 1 shall provide a means to manually override the RCIC start initiated open signal to valve E51-F012 to support testing.	Original design feature	
RCIC-FR-127	On a RCIC start, the trip system shall provide an output to open valve E51-F045 when 1oo1 condition votes for CI29 input is received.	GDC 13, GDC 29, GDC 34	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-128	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E51-F045 or terminate valve motion midstream from the control room.	GDC 19	
RCIC-FR-129	Division 1 shall provide valve E51-F045 position indication via the HMI based on contact inputs from the associated valve limit switches.	GDC 19, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-130	On a RCIC start, Division 1 shall provide an output to open valve E51-F046.	GDC 13	
RCIC-FR-131	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E51-F046 or terminate valve motion midstream from the control room.	GDC 19	
RCIC-FR-132	Division 1 shall provide valve E51-F046 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-133	Division 1 shall provide a means to manually open or close valve E51-F002, under administrative control, from the control room.	GDC 19	
RCIC-FR-134	Division 1 shall provide valve E51-F002 position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	GDC 19, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-135	Division 1 shall provide annunciation for RCIC VACUUM PUMP DISCHARGE VALVE NOT FULLY OPEN via the HMI when valve E51-F002 is manually closed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-136	Division 1 shall provide annunciation for RCIC VACUUM PUMP DISCHARGE VALVE NOT FULLY OPEN via the HMI when 1oo1 condition votes for CI25 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-137	Division 1 shall provide an output to start the RCIC Room Unit Coolers when 1oo1 start votes for RPDP input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-138	Division 1 shall provide the RPDP signal input for indicator capability via the HMI and transmit computer data to the non-SR DCS platform.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-139	Division 1 shall provide an output to open valve E51-F019 when 1oo1 open votes for RPF2 input is received **AND** 1oo1 start votes for RPDP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-140	Division 1 shall provide annunciation for RCIC PUMP LO FLOW via the HMI when 1oo1 annunciate votes for RPF2 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-141	Division 1 shall provide annunciation for RCIC PUMP LO FLOW via the HMI when 1oo1 annunciate votes for CI1 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-142	Division 1 shall provide an output to close valve E51-F019 when 1oo1 close votes for RPF2 input is received.	GDC 13, Reg Guide 1.105, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-143	Division 1 shall provide an output to close valve E51-F019 when 1oo1 condition votes for CI1 input is received.	GDC 13, Reg Guide 1.105, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-144	Division 1 shall provide an output to close valve E51-F019 when 0oo1 condition votes for CI2 input is received.	GDC 13, Reg Guide 1.105, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-145	Division 1 shall provide indicating light capability via the HMI when 1oo1 annunciate votes for RPF2 high input is received.	Original design feature	
RCIC-FR-146	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E51-F019 or terminate valve motion midstream from the control room.	GDC 19, Reg Guide 1.22	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-147	Division 1 shall provide valve E51-F019 position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-148	Division 1 shall provide an output to close valve E51-F025 when 1oo1 condition votes for CI3 input is received.	Original design feature	
RCIC-FR-149	Division 1 shall provide a means to manually open valve E51-F025 when 0oo1 condition votes for CI3 input is received.	GDC 19	
RCIC-FR-150	Division 1 shall provide a means to manually close valve E51-F025.	GDC 19	
RCIC-FR-151	Division 1 shall provide valve E51-F025 position indication via the HMI based on contact inputs from the associated valve limit switches.	GDC 19, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-152	Division 3 shall provide an output to close valve E51-F026 when 1oo1 condition votes for CI3 input is received.	Original design feature	
RCIC-FR-153	Division 3 shall provide a means to manually open valve E51-F026 when 0oo1 condition votes for CI3 input is received.	GDC 19	
RCIC-FR-154	Division 3 shall provide a means to manually close valve E51-F026.	GDC 19	
RCIC-FR-155	Division 3 shall provide valve E51-F026 position indication via the HMI based on contact inputs from the associated valve limit switches.	GDC 19, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-156	Division 3 shall provide an output to close valve E51-F005 when 1oo1 condition votes for CI3 input is received.	Original design feature	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-157	Division 3 shall provide a means to manually open valve E51-F005 when 0oo1 condition votes for CI3 input is received.	GDC 19	
RCIC-FR-158	Division 3 shall provide a means to manually close valve E51-F005.	GDC 19	
RCIC-FR-159	Division 3 shall provide valve E51-F005 position indication via the HMI based on contact inputs from the associated valve limit switches.	GDC 19, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-160	Division 1 shall provide an output to open valve E51-F004 when 0oo1 condition votes for CI3 input **AND** 1oo1 condition votes for CI4 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-161	Division 1 shall provide a signal to start the RCIC Vacuum Tank Condensate Pump when a 1oo1 condition votes for CI4 input is received.	Original design feature	
RCIC-FR-162	Division 1 shall provide a means to manually introduce a momentary signal to start or stop the RCIC Vacuum Tank Condensate Pump by providing a signal to the pump control circuit.	Original design feature	
RCIC-FR-163	Division 1 shall provide RCIC Vacuum Tank Condensate Pump operating status indication via the HMI based on contact inputs from the associated pump control circuit.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-164	Division 1 shall provide a means to manually open valve E51-F004 when 0oo1 condition votes for CI3 input is received.	GDC 19	
RCIC-FR-165	Division 1 shall provide a means to manually close valve E51-F004.	GDC 19	
RCIC-FR-166	Division 1 shall provide valve E51-F004 position indication via the HMI based on contact inputs from the associated valve limit switches.	GDC 19, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-167	Channel A shall condition the RPF1 signal through a square root converter and convert dP to a flow signal.	GDC 34, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-168	Channel A shall provide the resultant flow signal to Division 1.	GDC 34, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-169	Division 1 shall provide the RCIC pump flow signal to a flow controller.	GDC 34, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-170	Division 1 shall provide the RCIC pump flow signal for indicator capability via the HMI and transmit computer data to the non-SR DCS platform.	GDC 34, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-171	Division 1 flow controller shall compare the flow signal to a flow setpoint and provide a speed demand signal to the turbine control ramp/signal generator and transmit computer data to the non-SR DCS platform.	GDC 34, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-172	Division 1 flow controller shall be capable of providing PID flow control.	Stakeholder design item	
RCIC-FR-173	Division 1 flow controller shall provide a means to manually adjust the flow setpoint of the flow controller.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-174	Division 1 shall provide the means to manually transfer from flow control mode to a level control mode.	Stakeholder design item	
RCIC-FR-175	Division 1 shall provide the RWL2 input signal to a level controller.	Stakeholder design item	
RCIC-FR-176	Division 1 shall provide the RWL2 signal for indicator capability via the HMI and transmit computer data to the non-SR DCS platform.	Stakeholder design item	
RCIC-FR-177	Division 1 level controller shall compare the RWL2 level signal to a level setpoint and provide a speed demand signal to the turbine control ramp/signal generator and transmit computer data to the non-SR DCS platform.	Stakeholder design item	
RCIC-FR-178	Division 1 level controller shall be capable of providing PID level control.	Stakeholder design item	
RCIC-FR-179	Division 1 shall provide a means to manually adjust the level setpoint of the level controller.	Stakeholder design item	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-180	Division 1 shall provide the means to manually transfer from flow control mode to a pressure control mode.	Stakeholder design item	
RCIC-FR-181	Division 1 shall provide the RVP input signal to a pressure controller.	Stakeholder design item	
RCIC-FR-182	Division 1 shall provide the RVP signal for indicator capability via the HMI and transmit computer data to the non-SR DCS platform.	Stakeholder design item	
RCIC-FR-183	Division 1 level controller shall compare the RVP pressure signal to a pressure setpoint and provide a speed demand signal to the turbine control ramp/signal generator and transmit computer data to the non-SR DCS platform.	Stakeholder design item	
RCIC-FR-184	Division 1 pressure controller shall be capable of providing PID pressure control.	Stakeholder design item	
RCIC-FR-185	Division 1 shall provide a means to manually adjust the pressure setpoint of the pressure controller.	Stakeholder design item	
RCIC-FR-186	Division 1 shall be capable of receiving a 0-1 mA turbine speed signal from the turbine EGM control box and providing it for engineering units indication on the HMI and transmission as computer data to the non-SR DCS platform.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-187	Division 1 shall provide the RTSSP signal for indicator capability via the HMI and transmit computer data to the non-SR DCS platform.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-188	Division 1 shall initiate a transfer of the RCIC pump suction source from the CST to the suppression chamber when 1oo2 transfer votes for CSTL input are received.	GDC 13, NUREG-0737	
RCIC-FR-189	On a suction transfer, Division 1 shall provide an output to open valves E51-F029 and E51-F031 to transfer the suction source.	Original design feature	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-190	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E51-F029 from the control room and provide indicating light capability via the HMI when closing the valve.	Original design feature	
RCIC-FR-191	Division 1 shall provide valve E51-F029 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-192	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E51-F031 from the control room and provide indicating light capability via the HMI when closing the valve.	Original design feature	
RCIC-FR-193	Division 1 shall provide valve E51-F031 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-194	Division 1 shall provide annunciation for CONDENSATE STORAGE TANK LEVEL LOW SUCTION TRANSFER via the HMI when 1oo2 annunciate votes for CSTL input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-195	Division 1 shall provide the capability to shutdown the RCIC turbine when 2oo4 shutdown votes for RWL8/CI9 input are received.	Original design feature	
RCIC-FR-196	On a RCIC turbine shutdown, Division 1 shall provide an output to close valves E51-F045 and E51-F046.	Original design feature	
RCIC-FR-197	Division 1 shall be capable of automatically restarting the RCIC turbine when 0oo4 shutdown votes for RWL8 input are received the RCIC start logic is satisfied.	GDC 34, NUREG-0737	
RCIC-FR-198	Division 1 shall provide annunciation for VESSEL LEVEL 8 RCIC TURBINE SHUTDOWN and indicating light capability via the HMI when 2oo4 annunciate votes for RWL8 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-199	Division 1 shall provide a means to manually introduce a momentary signal to trip the RCIC turbine.	GDC 19, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-200	Division 1 shall trip the RCIC turbine when 1oo1 trip votes for RCICP1 input is received.	Original design feature	
RCIC-FR-201	Division 1 shall provide annunciation for RCIC PUMP SUCTION LO PRESS via the HMI when 1oo1 annunciate votes for RCICP1 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-202	Division 1 shall provide the RCICP2 pressure signal for indicator capability via the HMI.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-203	Division 1 shall provide annunciation for RCIC PUMP SUCTION HI PRESS via the HMI when 1oo1 annunciate votes for RCICP2 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-204	Division 1 shall trip the RCIC turbine when 1oo2 trip votes for RTEP input is received.	Original design feature	
RCIC-FR-205	Division 1 shall provide annunciation for RCIC TURBINE EXHAUST HI PRESS via the HMI when 1oo2 annunciate votes for RTEP input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-206	Division 1 shall provide the RTEP pressure signal for indicator capability via the HMI and transmit computer data to the non-SR DCS platform.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-207	Division 1 shall trip the RCIC turbine by providing an output to energize the turbine trip solenoid.	Original design feature	
RCIC-FR-208	Division 1 shall provide annunciation for RCIC OIL LO PRESS via the HMI when 1oo1 annunciate votes for CI18 input **AND** 1oo1 annunciate votes for CI1 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-209	Division 1 shall provide annunciation for RCIC VACUUM TANK LO VACUUM via the HMI when 1oo1 annunciate votes for CI19 input **AND** 1oo1 annunciate votes for CI1 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-210	Division 1 shall provide annunciation for RCIC TURBINE BEARING HI TEMP via the HMI when 1oo1 annunciate votes for CI20 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-211	Division 1 shall provide annunciation for RCIC VACUUM TANK LO LEVEL via the HMI when 1oo1 annunciate votes for CI21 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-212	Division 1 shall provide annunciation for RCIC OIL FILTER ΔP via the HMI when 1oo1 annunciate votes for CI22 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-213	Division 1 shall provide annunciation for RCIC VACUUM TANK HI LEVEL when 1oo1 annunciate votes for CI23 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-214	The RCIC isolation signal (whether automatic or manually initiated) shall remain sealed in until manually reset.	Original design feature	
RCIC-FR-215	Division 1 shall provide a means to manually initiate an isolation signal.	GDC 19, Reg Guide 1.47, Reg Guide 1.62	
RCIC-FR-216	Division 1 shall include an interlock which prohibits manual isolation unless a system initiation signal (automatic or manual) is present.	Original design feature	
RCIC-FR-217	Each division shall provide annunciation for RCIC OUT OF SERVICE via the HMI when a RCIC isolation signal is initiated.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-218	Each division shall provide RCIC Isolation Initiated alarm light capability via the HMI when a RCIC isolation signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-219	Each division shall provide indicating light capability via the HMI when a RCIC isolation signal is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-220	Division 1 shall initiate a RCIC isolation signal when 2oo4 isolate votes for RSF input are received.	Original design feature	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-221	Division 1 shall provide annunciation for RCIC STEAM LINE HI FLOW when 2oo4 annunciate votes for RSF input are received.	Original design feature	
RCIC-FR-222	Division 3 shall initiate a RCIC isolation signal when 2oo4 isolate votes for RSF input are received.	Original design feature	
RCIC-FR-223	Division 3 shall provide annunciation for RCIC STEAM LINE HI FLOW when 2oo4 annunciate votes for RSF input are received.	GDC 13, GDC 54, GDC 55, GDC 56, Reg Guide 1.141, NUREG-0737	
RCIC-FR-224	Division 1 shall initiate a RCIC solation signal when 1oo2 isolate votes for DI1 input are received.	GDC 13, GDC 54, GDC 55, GDC 56, Reg Guide 1.141	
RCIC-FR-225	Division 3 shall initiate a RCIC solation signal when 1oo2 isolate votes for DI1 input are received.	GDC 13, GDC 54, GDC 55, GDC 56, Reg Guide 1.141	
RCIC-FR-226	Division 1 shall initiate a RCIC solation signal when 2oo4 isolate votes for SLP input are received.	GDC 13, GDC 54, GDC 55, GDC 56, Reg Guide 1.141	
RCIC-FR-227	Division 3 shall initiate a RCIC solation signal when 2oo4 isolate votes for SLP input are received.	GDC 13, GDC 54, GDC 55, GDC 56, Reg Guide 1.141	
RCIC-FR-228	Each division shall provide annunciation for RCIC STEAM LINE LO PRESS via the HMI when 2oo4 annunciate votes for SLP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-229	Division 1 shall initiate a RCIC solation signal when 2oo4 isolate votes for TEDHP input are received.	GDC 13, GDC 54, GDC 55, GDC 56, Reg Guide 1.141	
RCIC-FR-230	Division 3 shall initiate a RCIC solation signal when 2oo4 isolate votes for TEDHP input are received.	GDC 13, GDC 54, GDC 55, GDC 56, Reg Guide 1.141	
RCIC-FR-231	Each division shall provide annunciation for RCIC TURBINE EXHAUST DIAPHRAGM RUPTURED when 2oo4 annunciate votes for TEDHP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-232	On a RCIC isolation, Division 1 shall provide an output to close the following outboard valves: • E51-F008 • E51-F076	IEEE Std. 603/IEEE Std. 7-4.3.2	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-233	On a RCIC isolation, Division 1 shall provide an output to trip the RCIC turbine.	Original design feature	
RCIC-FR-234	On a RCIC isolation, Division 1 shall provide indicating light capability via the HMI and transmit computer data to the non-SR DCS platform.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-235	Division 1 shall provide a means to manually open or close valve E51-F008, under administrative control, from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-236	Division 1 shall provide valve E51-F008 position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-237	Division 1 shall provide annunciation for RCIC OUT OF SERVICE via the HMI when valve E51-F008 is manually closed.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-238	Division 1 shall provide Valve E51-F008 Not Fully Open alarm light capability via the HMI when valve E51-F008 is manually closed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-239	Division 1 shall provide Valve E51-F008 Not Fully Open alarm light capability via the HMI when 1oo1 annunciate votes for CI15 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-240	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E51-F076 or terminate valve motion midstream from the control room.	Original design feature	
RCIC-FR-241	Division 1 shall provide valve E51-F076 position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-242	Division 1 shall provide annunciation for RCIC ISOLATION VALVE WARM-UP LINE E51-076 NOT FULLY CLOSED via the HMI when 1oo1 annunciate votes for CI28 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-243	On a RCIC isolation, Division 3 shall provide an output to close the following outboard valves: • E51-F007	original design feature	
RCIC-FR-244	On a RCIC isolation, Division 3 shall provide an output to trip the RCIC turbine.	Original design feature	
RCIC-FR-245	On a RCIC isolation, Division 3 shall provide indicating light capability via the HMI.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-246	Division 3 shall provide a means to manually open or close valve E51-F007, under administrative control, from the control room.	Original design feature	
RCIC-FR-247	Division 3 shall provide valve E51-F007 position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-248	Division 3 shall provide annunciation for RCIC OUT OF SERVICE via the HMI when valve E51-F007 is manually closed.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-249	Division 3 shall provide Valve E51-F007 Not Fully Open alarm light capability via the HMI when valve E51-F007 is manually closed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-250	Division 3 shall provide Valve E51-F007 Not Fully Open alarm light capability via the HMI when 1oo1 annunciate votes for CI16 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-251	Division 1 shall provide an output to close valve E51-F080 when 2oo4 close votes for SLP/DHP input are received.	GDC 54, GDC 56, Reg Guide 1.141	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-252	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E51-F080 or terminate valve motion midstream from the control room.	GDC 19, Reg Guide 1.97	
RCIC-FR-253	Division 1 shall provide an interlock to prevent valve E51-F080 from being manually opened when 2oo4 close votes for SLP/DHP input are received.	Original design feature	
RCIC-FR-254	Division 1 shall provide valve E51-F080 position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	GDC 19, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-255	Division 1 shall provide annunciation for RCIC VACUUM BREAKER ISOLATION VALVE E51-F080 NOT FULLY OPEN via the HMI when 1oo1 annunciate votes for CI24 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-256	Division 3 shall provide an output to close valve E51-F084 when 2oo4 close votes for SLP/DHP input are received.	GDC 54, GDC 56, Reg Guide 1.141	
RCIC-FR-257	Division 3 provide a means to manually introduce a momentary signal to open or close valve E51-F084 or terminate valve motion midstream from the control room.	GDC 19, Reg Guide 1.97	
RCIC-FR-258	Division 3 shall provide valve E51-F084 position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	GDC 19, Reg Guide 1.97, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-259	Division 3 shall provide an interlock to prevent valve E51-F084 from being manually opened when 2oo4 close votes for SLP/DHP input are received.	Original design feature	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-260	Division 3 shall provide annunciation for RCIC VACUUM BREAKER ISOLATION VALVE E51-F084 NOT FULLY OPEN via the HMI when 1oo1 annunciate votes for CI31 is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-261	Division 1 shall provide an output to open valve E51-F054 when 1oo1 open votes for CI10 input is received.	Original design feature	
RCIC-FR-262	Division 1 shall provide annunciation for RCIC TURBINE INLET DRAIN POT HI LEVEL via the HMI when 1oo1 annunciate votes for CI10 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-263	Division 1 shall provide a means to manually open or close valve E51-F054 from the control room.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-264	Division 1 shall provide valve E51-F054 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-265	Division 1 shall provide a means to manually open or close valve E51-F060, under administrative control, from the control room.	Original design feature	
RCIC-FR-266	Division 1 shall provide annunciation for RCIC OUT OF SERVICE via the HMI when valve E51-F060 is manually closed.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-267	Division 1 shall provide valve E51-F060 position indication via the HMI and transmit computer data to the non-SR DCS platform based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-268	Division 1 shall provide RCIC Turbine Exhaust Vlv Not Fully Open alarm light capability via the HMI when valve E51-F060 is manually closed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-269	Division 1 shall provide RCIC Turbine Exhaust Vlv Not Fully Open alarm light capability via the HMI when 1oo1 annunciate votes for CI17 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-270	Division 1 shall provide a means to manually introduce a momentary signal to open or close valve E51-112 or terminate valve motion midstream from the control room.	GDC 19, Reg Guide 1.97	
RCIC-FR-271	Division 1 shall provide valve E51-112 position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-272	Division 1 shall provide annunciation for RCIC OUT OF SERVICE via the HMI when 1oo1 annunciate for CI2 input is received.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-273	Division 1 shall provide annunciation for RCIC OUT OF SERVICE via the HMI when 1oo1 annunciate for CI15 input is received.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-274	Division 1 shall provide annunciation for RCIC OUT OF SERVICE via the HMI when 1oo1 annunciate for CI17 input is received.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-275	Division 1 shall provide annunciation for RCIC OUT OF SERVICE via the HMI when 1oo1 annunciate for CI30 input is received.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-276	Each division shall provide annunciation for RCIC OUT OF SERVICE via the HMI when any loss of logic power condition exists.	Original design feature	
RCIC-FR-277	Each division shall provide a means to manually provide annunciation for RCIC OUT OF SERVICE annunciator as well as annunciation and alarm light capability via the HMI.	Reg Guide 1.47 (BISI), IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-278	Each division shall provide MOV Overload / Power Loss alarm light capability via the HMI when 1oo1 annunciate votes for CI30 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-279	Division 1 shall provide RCIC Turbine Trip alarm light capability via the HMI when 1oo1 annunciate votes for CI2 input is received.	Original design feature	
RCIC-FR-280	Division 1 shall provide Trip and Throttle Valve Open Position Supervisory Light capability via the HMI when 1oo1 annunciate votes for CI2 input is received.	Original design feature	
RCIC-FR-281	Division 1 shall provide ANY PUMP MOTOR OVERLOAD OR POWER LOSS via the HMI when 1oo1 annunciate votes for CI26 input is received.	Original design feature	
RCIC-FR-282	Division 1 shall provide ANY PUMP MOTOR OVERLOAD OR POWER LOSS via the HMI when 1oo1 annunciate votes for CI27 input is received.	Original design feature	
RCIC-FR-283	Division 1 shall provide turbine governor valve position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-284	Division 1 shall provide turbine stop valve position indication via the HMI based on contact inputs from the associated valve limit switches.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-285	Each division shall provide the means to perform functional tests during normal plant operation without inadvertently initiating a protective action.	Reg Guide 1.22, Reg Guide 1.118, IEEE Std. 603/IEEE Std. 7-4.3.2	
RCIC-FR-286	Each division shall be capable of automatically returning to a coolant injection mode from a test mode when an automatic initiation condition occurs.	GDC 13, GDC 34	
RCIC-FR-287	Each channel and each division shall provide sufficient features and documented evaluations to support elimination of most Technical Specification Surveillance Tests, and minimize the requirements for manual calibration checks.	Project design approach	

RCIC FUNCTIONAL REQUIREMENTS			
ID #	**PPS/RCIC Requirement**	**PPS/RCIC Source / Basis**	**Notes / Clarification**
RCIC-FR-288	For all PPS inputs that have the potential to require manual test insertion or external measurement of input values (i.e., use of an external digital multi meter by a technician), test jacks are provided in the cabinets.	Project design approach	
RCIC-FR-289	For all inputs that have the potential to require manual multi-point calibration checks with external calibration equipment, knife edge disconnects along with test jacks are incorporated in the field termination panels.	Project design approach	
RCIC-FR-290	For the analog output, knife edge disconnects along with test jacks are incorporated in the field termination panels.	Project design approach	

H

H.1 SR Platform Requirements

Requirement #	Requirement	Source / Basis
	FUNCTIONAL REQUIREMENTS	
	Safety Classification	
PPS1	The platform and supporting components shall be safety related (Class 1E).	FSAR Section 7.2.1.1.2 (RPS), Section 7.3.1.1.1 (ECCS); FSAR Section 7.1.2.1.2.1 (N4S)
	Platform Architecture	
PPS2	The safety related (Class 1E) components of the PPS shall include the control and protection logic, the I/O interfaces, and the HMI displays providing control and indication.	Project requirement
PPS3	The PPS shall be capable of simultaneously performing the operational functionality (control and protection logic) of multiple safety related systems.	Project requirement
PPS4	The PPS shall include or be capable of being expanded to include the capability for automated control functionality to replace existing on-off control.	Project requirement
PPS5	The control and protection logic functionality of the following safety related systems shall be separate functions within the PPS: • Reactor Protection System (RPS) • Nuclear Steam Supply Shutoff System (N4S) - Steam Leak Detection (SLD) Emergency Core Cooling Systems (ECCS) • Core Spray (CS) - Undervoltage relay (27) protection logic for Emergency Diesel Generator (EDG) System interface • High Pressure Coolant Injection (HPCI) • Reactor Core Isolation Cooling (RCIC) • Residual Heat Removal (RHR) • Automatic Depressurization System (ADS)	Project requirement The functional control and protection logic functionality for each safety related system provided in separate spreadsheets.

Requirement #	Requirement	Source / Basis
PPS6	The PPS shall be capable of interfacing (discrete inputs and outputs) with other NSR systems (e.g. digital feedwater) through qualified isolation.	Project requirement. The interfacing functionality for each NSR system with a safety related system is provided in separate respective spreadsheets.
PPS7	The PPS shall have decentralized logic solving to support each of the resident safety related functions or demonstrate adequate segmentation strategy to achieve the same.	Project requirement.
PPS8	The PPS design shall have inherent redundancy to assure reliability and availability of the control and protection functionality.	IEEE Std. 603/IEEE Std. 7-4.3.2
PPS9	The PPS shall include redundant divisional power supplies.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
PPS10	The PPS shall be capable of performing various types of voting schemes within a function (e.g. 4oo4, 2oo4, 1oo3, 1oo1, etc.)	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
PPS11	The PPS shall be capable of adjusting the voting scheme as a result of a bypass / inoperable condition for a channel (e.g. 2oo4 to 2oo3, 2oo3 to 1oo2, automatic initiation).	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
PPS12	If placing a channel in bypass would compromise the minimum acceptable voting scheme, the PPS shall reject the bypass request and convey this to the operator via the HMI. One failed channel can be bypassed. Additional failed channels are marked as voting to scram or actuate.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
PPS13	The PPS shall conservatively initiate the protective function if the minimum acceptable voting scheme cannot be achieved with the available channels.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
PPS14	The PPS shall include priority logic to assure protection functions override any active control functions.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
PPS15	None of the PPS logic shall be encoded as negative logic (i.e. active low). The digital representation of input and output data shall be in positive logic to the maximum extent practical.	Eliminate design and V&V mistakes common to negative logic.
PPS16	The PPS shall be readily testable and maintainable online or offline.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2

Requirement #	Requirement	Source / Basis
PPS17	The PPS shall support, to the maximum extent practical, hot swap of any field replaceable module without impeding the system's ability to initiate, continue, complete, or terminate a protective function or inadvertently causing the initiation or termination of a required protective function.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
PPS18	The PPS shall be designed such that it does not suffer any degradation in performance, processing speed, memory allocation, etc. under abnormal operating conditions or high loading.	Improved fault tolerance and good engineering practice.
PPS19	Performance diagnostics, such as processor loading, power supply status, network loading, etc. shall be viewable from a dedicated Engineering Workstation (EWS).	Project requirement
PPS20	All software shall be designed with sufficient modularity to minimize the time and complexity involved in making a change to any program.	NUREG/CR-6463
PPS21	Communication among programs for data or program control shall be symbolic rather than absolute (i.e., no use of global variables) so a given program is essentially an independent unit.	NUREG/CR-6463
PPS22	Changes required in one program necessitated by changes in another shall be minimal and through established and controlled interfaces.	NUREG/CR-6463
PPS23	Processor and device state software shall identify the operating condition of each function processor and peripheral device within the PPS.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
PPS24	In the presence of software common cause failure in the PPS, the architecture shall support priority logic that allows the DAS function of the DCS to safely trip the plant and actuate required safety features.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
PPS25	Floating point math computations shall be supported in hardware.	NUREG/CR-6463
PPS26	The design shall ensure that divide-by-zero and similar out-of-bounds errors are not possible.	NUREG/CR-6463
PPS27	If floating point calculations are performed, error handling shall include detection and appropriate handling of floating point not a number (NAN).	NUREG/CR-6463

Requirement #	Requirement	Source / Basis
PPS28	Software modules shall have inherent features to validate data received for use from other modules within the system, from any external data links, and from Operators and technicians.	NUREG/CR-6463
PPS29	Detected faults and failures shall be reported as PPS health error messages to be communicated to a separate Non Safety DCS. (The DCS will save PPS health in an error log.)	Project requirement
PPS30	The PPS health error message from the PPS shall include sufficient information to identify the module reporting the error, data item found in error, and PPS processor which the reporting software module was running at the time of detection. (The DCS shall time stamp the message upon receipt.)	Project requirement
PPS31	Vendor shall provide an obsolescence plan for future maintainability of the system, which shall not require wholesale replacement as the means of coping with obsolescence.	Project requirement
PPS32	The PPS shall be capable of providing control function capability.	Project requirement
PPS33	The PPS shall be capable of performing various operations on input signals (e.g. conditioning, summing, averaging, square root conversion).	Project requirement
PPS34	No setpoint, derived setpoint, or tolerance shall be hardcoded within the PPS.	Project requirement
PPS35	All bi-stable functions shall include hysteresis on reset.	Project requirement
PPS36	Hysteresis for each bi-stable shall be user-settable controlled constants.	Project requirement
PPS37	All constants used for the PID controllers shall be user modifiable and not require re-programming the application logic.	Project requirement
PPS38	Each constant value to which an engineering unit input is compared shall be a user-settable controlled constant.	Project requirement
PPS39	The application software shall prevent the hysteresis value from being set in the domain where the bi-stable function has exceeded the action point.	Project requirement

Requirement #	Requirement	Source / Basis
PPS40	All PPS outputs that initiate scrams, actuations, or isolations shall be single failure tolerant and diagnosable.	Project requirement
PPS41	No single failure of a discrete output to the shorted or open state shall prevent a required change of output state.	Project requirement
PPS42	No single failure of a discrete output to the shorted or open state shall falsely cause an unintended change of output state.	Project requirement
PPS43	Failures in the single failure tolerant output circuits shall be detectable and detected by the PPS.	Project requirement
	System I/O	
	Note - Specific I/O for each of the PPS functions can be derived from the individual functional requirements provided separately. Entries included below provide additional PPS capabilities that warrant identification for each function.	
PPS44	The PPS shall utilize fault tolerant I/O interfaces (modules / cards) (e.g. shorts, grounds, open circuit, etc)	Project requirement
PPS45	The PPS input interfaces shall be compatible with standard analog signals inputs as well as analog signals from smart transmitters (e.g. HART) with communication active on the analog signal link.	Project requirement
PPS46	The PPS shall support qualified safety to non-safety related analog signal isolators for 4-20mA inputs that will be utilized by a non-SR DCS platform.	Project requirement
PPS47	The PPS shall be capable of providing SOE outputs suitable for sampling by DCS SOE input modules or for direct drive of the existing annunciator.	Project requirement
PPS48	The PPS SOE outputs shall have minimal propagation delay.	Project requirement
PPS49	The PPS shall support a pair of discrete inputs from the Remote Shutdown Panel that inhibit operation of PPS.	Project requirement

Requirement #	Requirement	Source / Basis
PPS50	The PPS shall monitor the state of the Reactor Mode switch and use the Reactor Mode Switch input as a trip input, as is done in the existing system.	Project requirement
PPS51	The PPS shall monitor the state of the manual scram switches.	Project requirement
PPS52	The PPS shall support maintenance bypass inputs (vendor shall describe extent of bypass capability within the design and demonstrate single failure tolerance)	Project requirement
	RPS I/O	
PPS53	The PPS shall monitor the powered state of each scram solenoid group output driver.	Project requirement
PPS54	The PPS shall monitor the powered state of the backup scram solenoids and shutdown volume isolation output drivers.	Project requirement
PPS55	The PPS shall monitor contact inputs from scram discharge volume vent and drain valve limit switches (1 FO and 1 FC from each valve).	Project requirement
	N4S I/O	
PPS56	The PPS shall support cold junction compensation capability for thermocouple inputs.	Project requirement
	HPCI I/O	
PPS57	The PPS shall provide a 1-5 VDC control signal output to provide HPCI turbine control. If HPCI is included in the DAS function in the DCS, then the ability shall be provided to arbitrate whether the PPS or the DAS function outputs the control signal.	Project requirement
	RCIC I/O	
PPS58	The PPS shall provide a 1-5 VDC control signal output to provide RCIC turbine control. If RCIC is included in the DAS function in the DCS, then the ability shall be provided to arbitrate whether the PPS or the DAS function outputs the control signal.	Project requirement

Requirement #	Requirement	Source / Basis
	Independence, Separation and Segmentation	
PPS59	PPS operation shall be accomplished independent of any other digital system interfaces. The PPS VDUs are considered part of the PPS.	Ensures that the PPSs operate independent of any other system (e.g. the non-safety DCS).
PPS60	Use of digital communications in the PPS shall in no way compromise PPS channel/division independence or control segment independence. The PPS shall supply communications buffers in accordance with IEEE Std. 7-4.3.2 requirements.	Any failure or improper configuration in the PPS digital communications/VDUs that adversely effects channel/division independence or control segment independence could place the plant in an undesired state.
PPS61	Redundancy (separate channels/divisions of equipment) shall be provided for PPS protective functions.	IEEE Std. 603 single failure criteria
PPS62	PPS channels shall be independent.	Including communication independence as described in ISG-04. Single failure criteria.
PPS63	PPS divisions shall be independent.	Including communication independence as described in ISG-04. Single failure criteria.
PPS64	The modernized system design shall reduce the total number of required sensor inputs through consolidation.	Project requirement
PPS65	Where possible, redundant sensors that feed different functions within the same channel/division of the PPS shall be consolidated.	Sharing sensors for multiple control and protection functions within the same channel/division reduces the numbers of sensors that must be calibrated, tested, and maintained, and the corresponding input modules and cabling without compromising independence.
PPS66	Functions of Individual relay logic strings, bistables, single loop controllers, and voting functions within a channel division shall be consolidated into the software, requiring a much smaller number of digital devices.	Reduce acquisition and lifecycle support costs without compromising channel/division concept.
PPS67	PPS control function physical and/or logical segmentation capability shall be provided for inputs/outputs and their related control processor(s).	Segmentation of control functions is either expressly described or implied in the UFSAR. This segmentation addresses functionality not already segmented in individual channels/divisions.

Requirement #	Requirement	Source / Basis
PPS68	Where possible, individual functions within a segment of the PPS shall be consolidated.	Supports the requirement to minimize the number of unique FRUs. Reduces acquisition and lifecycle support costs without compromising the segmentation concept.
PPS69	Consolidation shall not create new malfunctions or malfunction with a different result for the function.	Supports the requirement to minimize the number of unique FRUs. Reduces acquisition and lifecycle support costs without compromising the segmentation concept.
PPS70	All PPS protection processes shall be executed continuously on a cyclical, non-varying basis.	Ensures bounded, deterministic performance over varying plant conditions, unaffected by the likely maximum and minimum propagation delays through the channels and divisions.
PPS71	The PPS shall be capable of initiating the protective function within the required response time of receiving a valid protective signal. This shall account for scan times, processing times and communication times for the logic as part of the control throughput so that maximum protection system response is not affected.	Response time as determined by design and licensing basis. Refer to DR spreadsheets.
PPS72	The PPS time response for the RPS, N4S, and ECCS functions shall be validated by test, with the time response histogram, including maximum recorded response time and minimum recorded response time, recorded and provided as part of the test record.	Project requirement
PPS73	PPS control segments shall be digitally connected to enable features such as system wide data aggregation, capture, and use of Visual Display Units (VDUs) for monitoring and control.	Data aggregation and capture directly reduces operator workload. It also allows for analysis to improve plant operational performance and to detect maintenance issues.
PPS74	No failure in one PPS control segment shall propagate to another control segment.	Ensures that no new failure is introduced into the PPS design that has not been evaluated in the safety analysis.
PPS75	The PPS shall be expandable by the addition of future segments without impacting the performance of other segments or the performance of other channels/divisions.	Allows for the future expansion of the PPS to support consolidation of plant PPS I&C functions to the PPS Platform.
PPS76	The number of unique field replaceable units (FRU) shall be minimized	Reduce acquisition cost, reduce lifecycle support costs.

Requirement #	Requirement	Source / Basis
PPS77	No single failure of a FRU shall cause spurious actuation or prevent a necessary commanded actuation from occurring unless allowed by the clarification below.	IEEE Std. 603 single failure criteria.
PPS78	Clarification - If it can be shown that through a combination of PPS attributes that address the (1) the possibility of spurious actuation or (2) prevention of a necessary commanded actuation AND/OR (3) segmentation that establishes the single failure is sufficiently unlikely or can be tolerated within the bounds of the safety analysis, then implementation of Requirement PPS77 shall not be required.	This is consistent with the design bases for single function/loop control in legacy implementations. Allowing this exception promotes reducing control system complexity/unnecessary redundancy. This translates into reduced acquisition costs and reduced lifecycle support costs.
PPS79	Where individual PPS FRUs require testing, calibration, or other configuration changes with the control system online, the PPS shall retain its capability to perform its functions while these activities are being performed on the subject FRU.	IEEE Std. 603 clause 5.7 – support for testing and calibration.
PPS80	PPS testing shall be restricted to one component or channel at a time.	Project requirement
	Health Monitoring	
PPS81	The PPS shall be capable of self-monitoring, self-diagnostics, fault detection, and alarming any abnormalities within itself.	Improved fault tolerance and good engineering practice.
PPS82	Active equipment health monitoring shall be performed down to the FRU level.	Active health monitoring continuously demonstrates FRU operability and minimizes/eliminates the need for surveillance testing.
PPS83	Detected equipment faults shall be self-announcing and identify the affected FRU.	Eliminate need for performing surveillance tests, eliminate need for troubleshooting, and reduce workload.
PPS84	The PPS shall be capable of performing self-tests and online diagnostics to identify and isolate failures of I/O cards, busses, power supplies, controllers, communications paths, etc.	These features shall identify the presence of all faults, and determine the location of failure(s) to replaceable module level(s).
PPS85	The PPS shall provide indication when the PPS self-test functions are operating (e.g. counter, heartbeat, etc).	Project requirement

Requirement #	Requirement	Source / Basis
PPS86	The PPS shall employ a watchdog timer(s) to detect faults and failures within the system.	Project requirement
PPS87	Watchdog timers shall be independent of the processing CPU.	Project requirement
PPS88	The PPS shall include diagnostics to detect a logic related failure within an individual segment.	Project requirement
PPS89	The diagnostic features provided shall include all the necessary indications and alarms to allow an Operator to take corrective or alternative actions.	Project requirement
PPS90	Online and offline diagnostics shall be provided to check and verify the operation of the hardware, firmware, software, and programmable logic.	Project requirement
PPS91	Online system health monitoring shall be provided for verifying the health status of system components to support software and hardware maintenance activities.	Project requirement
PPS92	The on-line diagnostics shall be sufficient to allow reduction of related Technical Specification Surveillance Tests. (e.g. logic system functional tests)	Project requirement
	Surveillance Testing	
PPS93	When surveillance testing is required to demonstrate a safety function is operable, the PPS design shall automate the surveillance to the maximum extent practicable.	Reduce operator workload.
PPS94	For redundant PPS functions where multiple instances of the safety function are required to actuate plant response (e.g. a plant trip or a turbine trip), surveillance testing shall be able to fully test a single instance of that safety function without initiating an actuation. This includes actuation of individual physical components configured in a coincidence configuration. (e.g. testing a single actuator located in single train in a 2oo2 train configuration where each train is 1oo2, or actuating a suction isolation valve to a pump without actuating the pump or the output isolation valve for that pump)	Enable maximum surveillance testing while not impacting plant operation. This is also consistent with design attribute of minimizing single point vulnerabilities. Reduction in cost/workload to perform surveillance testing.

Requirement #	Requirement	Source / Basis
PPS95	Analog and discrete input and output field wiring connections shall be provided with a terminal block with integral test points. The field terminal block shall provide integral knife switch disconnects if signal injection or external signal monitoring is required for calibration or test.	Project requirement
PPS96	The PPS design shall minimize the surveillance test requirements.	Project requirement
PPS97	The PPS design shall support the automation of surveillance testing by allowing the capability for inter-channel checks that produce necessary data outputs for validation.	These channel checks are performed in the non-safety related equipment to which the PPS provides the required analog engineering units data, and are NOT performed in the PPS software.
PPS98	The PPS shall provide the capability to automate the performance of valve strokes and timing.	Project requirement
	Communication	
PPS99	No communication shall be provided between channels.	IEEE Std. 7-4.3.2
PPS100	No communication shall be provided between divisions.	IEEE Std. 7-4.3.2
PPS101	All four channels shall provide one-way communication to both divisions.	Project requirement
PPS102	All serial data communication shall implement the guidance of DI&C-ISG-04 for Interdivisional Communication.	ISG-04
PPS103	Bi-directional channel and divisional communication shall exist between the PPS platform and the VDU to allow for control, operator trending (as required), grouping, and alarming in the MCR or other operational areas.	This supports real-time operation of the plant and immediate/short term operator action.

Requirement #	Requirement	Source / Basis
PPS104	One way data communication shall exist from the PPS to the non-safety platform (DCS) and shall include data associated with: Sequence of Events (SOE) All raw analog data All Engineering unit data All discrete status All votes to trip or actuate Channel Checks Historian / Analytics Platform diagnostics	Project requirement
PPS105	The PPS shall utilize a suitable one-way protocol for communicating data from the PPS to the non-safety platform (DCS). No handshaking from the DCS back to the PPS is allowed.	Project requirement
PPS106	All data messages shall be designed with a fixed format and shall comply with formatting requirements.	Project requirement
PPS107	The signal response from soft control selection on the HMI, through the PPS and back for indication (data latency) shall not exceed 0.25 second.	Project requirement
PPS108	Communication shall use fixed format messages for safety data processing, always broadcasting the same data in every message. This supports a consistent communication loading.	Project requirement
	Human-Machine Interfaces (HMI)	
PPS109	The primary HMIs for the platform shall consist of multiple VDUs that provide access to channel, division, and segment data and offer the capability for soft controls, using touch screen, trackball, or other pointing device [TBD].	Promotes the design objective for a VDU driven end-state control room. This provides for a more compact control room design, reduces equipment and corresponding maintenance costs.
PPS110	The HMI functionality shall be capable of replacing existing hand switch / indicating light configurations via soft controls.	Project requirement

Requirement #	Requirement	Source / Basis
PPS111	Manual controls (switches, pushbuttons) shall be retained only when required by regulation or regulatory guidance. Retained manual controls shall be monitored by the PPS.	Project requirement
PPS112	Two VDUs (set) shall be employed on a divisionalized basis (1 set per division).	Project requirement
PPS113	A primary set of VDUs shall be provided to support the required number of safety divisions plus one VDU for continuous data display.	Project requirement
PPS114	A redundant (backup) set of VDUs shall be provided to support the required number of safety divisions plus one for continuous data display.	Project requirement
PPS115	The PPS HMIs shall be capable of making all PPS data available for display.	Project requirement
PPS116	A separate Engineering Work Station (EWS) shall be provided for configuration management.	Project requirement
PPS117	The EWS shall not be connected to more than one channel or one division at any time.	Project requirement
PPS118	The EWS shall be at least password protected and shall offer multiple levels of password protected functionality (e.g., view configuration and show data within the program versus change setpoint values versus change the program).	Project requirement
PPS119	The EWS shall not be capable of initiating, terminating, or bypassing safety functions.	Project requirement
PPS120	The EWS shall only be capable of displaying data in a single channel/division pair that is in maintenance bypass.	Project requirement
PPS121	The EWS shall include fully integrated local storage devices to support PPS backup and restore of settable setpoint values and other similar field-modifiable constants.	Project requirement
PPS122	Backup shall be on bulk storage devices and copies of these backups must be able to be removed from the system.	Project requirement

Requirement #	Requirement	Source / Basis
PPS123	EWS and PPS real time diagnostic/maintenance utilities shall include the following: System Performance Analysis, Status of PPS communication links, System Health Displays, Workstation Activity Monitor, and Program Execution Timing and Scheduling	Project requirement
PPS124	The EWS shall not be capable of being connected to more than one channel or one division at any time.	Project requirement
PPS125	The VDU shall be powered from the same divisional power as the PPS which is supplied from multiple sources so the loss of a single power source does not result in the loss of multiple VDUs.	Project requirement
PPS126	If a VDU fails, the redundant VDU shall be capable of the same functionality and operation shall be maintained without any functional or operational deterioration.	Project requirement
PPS127	VDU shall support keyboard and mouse inputs in addition to more advanced methods such as touch screen inputs.	Project requirement
PPS128	All control actions initiated from a Human Machine Interface shall propagate through the system such that control system signals sent to final plant control elements appear at the control system output interface connected to the associated plant control elements at an established, bounded rate that does not inhibit operator performance or timely operator control actions.	Ensures bounded, repeatable performance over varying plant conditions. This also enables the use of single point plant interfaces to the digital PPS vs using hardwired controls.
PPS129	No single point of failure within the VDU component and communication design shall disable other / all PPS VDUs in the Main Control Room.	IEEE Std. 603 single failure criteria
PPS130	PPS VDUs shall be switchable so that they can also provide HMI functionality to other connected systems (e.g. a non-safety DCS).	Promotes the design objective for a VDU driven end-state control room. This provides for a more compact control room design, reduces equipment and corresponding maintenance costs.

Requirement #	Requirement	Source / Basis
PPS131	PPS VDUs shall be switchable so that they can also provide HMI functionality for other PPS channels and divisions. This switchable feature shall in no way compromise the independent function of the PPS.	IEEE Std. 603 / 7-4.3.2 single failure criteria
PPS132	Only one system (PPS or non PPS) shall be accessed by the VDU at a time. This switchable feature shall in no way compromise the independent function of the PPS.	IEEE Std. 603 / 7-4.3.2 single failure criteria
PPS133	No plant control logic of any kind shall be resident within that portion of the PPS architecture that supports VDU functionality and VDU functional switching.	The portion of PPS architecture is only intended to provide Keyboard/Video/Mouse capability for PPS and this same capability for other connected systems (e.g. a non-safety DCS). This is to support to support the VDU driven end-state control room concept. The plant control functions of VDU connected systems are fully contained within those connected system. VDU functionality only provides an HMI interface for the selected system.
PPS134	The PPS HMI design shall be expandable without impacting the performance of other HMI or the performance of the safety related channels/divisions functionality. (Vendor to provide a maximum count of VDUs that can be supported.)	Project requirement
PPS135	The VDU switching system shall be maintainable on-line, with internal redundancy and hot swap on all modules. Sufficient redundancy shall be provided in the switching system to support shutting down one switching network for maintenance without disabling all control room VDUs.	Project requirement
PPS136	Identification of HMI design and communication compliance with ISG-04 shall be provided.	Project requirement
PPS137	Non-VDU operating interface devices (e.g. switches/pushbuttons) that provide digital inputs to the PPS shall only be provided to meet specific regulatory or operational commitments to provide such a feature.	This provides for a more compact control room design, reduces equipment and corresponding maintenance costs. This also provides increased redundancy in that functions not tied to switches can be manipulated from displays presented on multiple VDUs.

Requirement #	Requirement	Source / Basis
PPS138	Non-VDU Operator interface devices (e.g. switches/pushbuttons) that are connected electrically to plant actuated devices (either directly or through a control relay) shall only be employed when required to meet a specific regulatory requirement or commitment to provide such a feature.	Excessive, direct, point-to-point wiring of switches and pushbutton actuators is expensive and inefficient from a human factors perspective. Use of these devices is limited to only the most critical actuation functions. See IEEE Std. 603-2018 Clauses 4e, 5.1, 5.2, 5.8.1, 5.8.3, 5.8.4, 6.2, 7.2, 7.3, 7.4, and 7.5.
PPS139	Non-VDU parameter displays are not in vendor scope and shall not be driven by the PPS.	Project requirement
PPS140	The PPS HMI shall be capable of logging commands and communicating this to the DCS for purposes of data collection.	Project requirement
PPS141	The PPS HMI shall provide the capability to automate valve lineups to support initiation and restoration operational scenarios.	Project requirement
	Visual Display Units (VDUs) Displays	
PPS142	The PPS VDU's shall be supported by a color, full graphics package that supports: (A) Full color (256 colors at a minimum) (B) Mimic displays of plant systems (e.g. one-line diagrams of plant fluid systems) (C) Logic displays of implemented control logic (D) The ability to depict dynamic graphical objects (e.g., tanks, valves, pumps, logic devices, etc.) that show information as to state (e.g., tank level, valve position, pump running status, logic states, etc.) (E) The ability to control plant processes and equipment either through •graphical control objects, and/or •physical switches/buttons located on or near the VDU	Provides improved, graphical HMI interface to improve operator performance. Promotes the design objective for a VDU driven end-state control room. This provides for a more compact control room design, reduces equipment and corresponding maintenance costs.
PPS143	The HMI displays shall have a 16:9 aspect ratio regardless of size.	Project requirement
PPS144	The HMI displays shall utilize a pixel geometry resolution of at least 1600 x 900.	The 1600 x 900 pixel resolution also is compatible with most current desktop and wide screen laptops.

Requirement #	Requirement	Source / Basis
PPS145	Use of the VDU switching network shall not result in perceptible display jitter or other video degradation.	Project requirement
PPS146	The VDU shall be capable of displaying any data that is provided from the PPS platform.	Project requirement
PPS147	The VDU shall be capable of providing an on-screen “logic diagram” which shows state of logic and process values.	Project requirement
PPS148	A minimum of 30 pre-configured graphics / division shall be provided (mix of low/medium/high complexity).	Project requirement
PPS149	VDU shall support at least 20 additional custom graphics.	Project requirement
PPS150	The Purchaser shall be provided with the tools and instructions necessary to modify or augment the graphics.	Project requirement
PPS151	The VDU display convention shall comply with a display style guide (to be developed and provided by Purchaser).	NUREG-0711
PPS152	The Operator interactions via the VDU display screen shall be confirmed as "received" by the VDU within the refresh rate.	NUREG-0700, Section 7.3.9-1 (Display screen sensitivity and response)
PPS153	The time to call up any VDU display shall not exceed two (2) seconds under peak loading conditions, which does not require double touch.	NUREG-0700, Section 2.4.3-1 for Response Time Appropriate to Transaction, typical response time for a next page request should be within 0.5 to 1.0 seconds.

Requirement #	Requirement	Source / Basis
PPS154	All HMI displays shall be updated (refreshed) with system data at a rate not greater than once per second so as not to inhibit operator performance.	Ensures bounded, repeatable performance of the HMI over varying plant conditions. NUREG-0700, Section 1.4-1 contains a guideline stating the maximum update rate should be determined by the time required for the user to identify and process the changed features of the display. NUREG-0700, Section 1.4-3 states changing alphanumeric values the user must reliably read should not be updated more than once per second. NUREG-0700, Section 2.4.3-1 states the speed of computer response to user entries should be appropriate to the transaction involved.
PPS155	Touch screen interface shall require double touch action (e.g. separate select and execute touches in disparate screen areas) to initiate a control function.	NUREG-0700, Section 7.3.3-2 Second "touch" provides confirmation that the requested action is indeed intended.
PPS156	The HMI VDU shall be capable of providing soft controls that replicate the functionality provided by existing switches consisting of, but not limited to: 2 position maintained contact Keylock switch – 2 position (administrative control) Keylock switch – 3 position (administrative control) 3 - position spring return to center 3 - position, pull out, spring return to center 3 – position, spring return from stop position	Project requirement
PPS157	The VDU displays shall be configured to comply with Human Factors requirements (e.g. Support peer checking without obscuring the item being peer checked.)	NUREG-0711
PPS158	All HMI shall be designed, implemented, verified, and validated under a Human Factors Engineering program.	NUREG-0711

Requirement #	Requirement	Source / Basis
PPS159	A timeout/reset feature shall be provided for non-executed data entry/commands.	Project requirement
PPS160	A system “Heart Beat” shall be on the HMI display to indicate the display is active and not in a frozen or locked state (which shall not be by display of the local time).	Project requirement
PPS161	The heartbeat shall be based on an artifact in the logic solver, which shall demonstrate that the VDU is communicating with the logic solver.	Project requirement
PPS162	To reduce the possibility of data entry errors, the HMI shall provide the capability to use an on-screen numeric keypad permitting the Operators to keep their view on the display.	Project requirement
PPS163	The HMI shall provide the capability to insert or remove an operational or maintenance bypass, start or terminate a protective action, as well as trip an individual sensor, a logic channel, or the trip system.	Project requirement
	Data Historian, Sequence of Events, Data Transmission	
PPS164	All SOE data shall be presented to a non-safety related system for archiving in the data historian and addition analysis.	SOE data is used in post-event analysis to identify event initiators and to ensure intended sequenced actions occurred at the proper time intervals. Data analysis is a non-safety function.
PPS165	All data required to support Requirement PPS 105 shall be provided to and stored by the data historian.	Project requirement
	Cyber Security	
PPS166	The PPS shall comply with the Secure Development and Operational Environment (SDOE), as evaluated in the NRC platform’s Safety Evaluation Report.	Reg Guide 1.152, Rev 3, Regulatory Position C2.
PPS167	The PPS shall support Purchaser compliance with Reg Guide 5.7 or the Exelon Cyber Security "Constitution."	Project requirement

Requirement #	Requirement	Source / Basis
	Simulator	
PPS168	HMI and logic software shall support direct port translation to the Simulator to facilitate Simulator maintenance and integration.	Project requirement
PPS169	System control logic and HMI software shall support direct use in the plant control room simulators without translation.	Re-engineering the provided control logic and HMI software to provide a satisfactory mimic of the actual Safety Systems installed in the plant is a costly endeavor and creates significant configuration control issues.
PPS170	For the Simulator, the system application/control logic and HMI software shall be able to run on commercially available IT equipment (e.g., physical computers, servers). Any necessary software tools to enable this function (e.g. operating systems, virtualization tools, etc.) shall also be provided.	Minimize costs associated with Safety System integration to the Simulator.
PPS171	System logic and HMI software running in the Simulator shall be capable of being linked dynamically and bidirectionally to software provided by third parties that mimic control processes and physical plant performance outside of bounds of the Safety System.	Provides for the basic function of the Simulator to mimic plant operation within a Main Control Room environment.
PPS172	Safety System logic and HMI software running in the Simulator shall be capable of executing in such a manner that it provides an operating facsimile of the Safety System in the plant to operators in the simulator. This includes, but is not limited to: (A) No appreciable time delay when compared to the operation of the actual Safety System in the plant. (B) Repeatable performance for given scenarios with defined inputs.	Provides for the basic function of the Simulator to mimic plant operation within a Main Control Room environment. (ANSI/ANS 3.5-2009)

Requirement #	Requirement	Source / Basis
PPS173	Safety System logic and HMI software running in the Simulator shall be capable supporting features required for Simulator training as commanded by the Simulator instructor, including: (A) Reset: Setting the Simulator to a selected pre-defined set of initial conditions out many sets of initial conditions (B) Freeze: Halt the Simulator function at any time as commanded by the simulator instructor (C) Backtrack: To return the Simulator to a previous point in time to permit re-initiation of training using the simulator from that point in time. (D) Run: Initiate Simulator operation for the purposes of training, either from a “Reset,” “Freeze,” or a “Backtrack” condition.	Provides Simulator features to promote training
	ENVIRONMENTAL CHARACTERISTICS	
	Electromagnetic Compatibility	
PPS174	The PPS and HMI shall meet Electromagnetic Compatibility (EMC) requirements of Reg Guide 1.180, Rev 2 or be mitigated through analysis or design control.	Reg Guide 1.180, Rev 2
PPS175	PPS I/O hardware shall be capable of filtering out noise on plant signal cables.	Plant cables pass by high voltage / current applications and the new I/O hardware shall be capable of filtering out this noise from the actual process signal.
	Cabinet Requirements	
PPS176	All equipment shall be capable of being installed into existing enclosed cabinets	Project requirement
PPS177	All field interfaces shall be compatible with the existing PGCC "Cannon" plugs	Project requirement

Requirement #	Requirement	Source / Basis
	Environmental Parameters	
PPS178	The PPS HMI shall be capable of operating within the following Control Room parameters: Temperature: 65°F (Min) / 78°F (Max) Pressure: +0.25 (in WG) Relative Humidity: 30% (Min) / 50% (Avg) / 90% Max) Integrated Dose: 2.64E+02 RADS (Normal) / 2.71E+02 RADS (Total)	Spec M-171
PPS179	The PPS HMI shall be capable of operating within the following Auxiliary Equipment Room parameters: Temperature: 60°F (Min) / 82°F (Max) Pressure: Atmos Relative Humidity: 30% (Min) / 50% (Avg) / 90% Max) Integrated Dose: 2.64E+02 RADS (Normal) / 2.77E+02 RADS (Total)	Spec M-171
PPS180	Vibration spectra (AER and MCR)	TBD by LGS
	Component Requirements	
	*Hardware	To be populated following vendor selection
	*KVM switches	To be populated following vendor selection
	*Printers	To be populated following vendor selection
	*Work stations	To be populated following vendor selection
	*Operating System	To be populated following vendor selection
	*Servers / Chassis	To be populated following vendor selection
	*Virtual servers	To be populated following vendor selection
	*Thin clients	To be populated following vendor selection
	*Redundancy Requirement	To be populated following vendor selection

Requirement #	Requirement	Source / Basis
	*Server / workstation performance	To be populated following vendor selection
	*Anti-virus software	To be populated following vendor selection

Appendix B

Vendor-Independent Boiling Water Reactor Non-Safety Platform and Redundant Reactivity Control Requirements Baseline

1129-0172-SPEC-002
Revision 0

Vendor Independent Boiling Water Reactor Non-Safety Platform and Redundant Reactivity Control Requirements Baseline

Prepared for: Battelle Energy Alliance, LLC

Preparer:	Paul Heaney	E-signed by: Paul Heaney on 2020-05-07 11:13:21
Reviewer:	Matthew Minkoff	E-signed by: Matthew Minkoff on 2020-05-07 11:33:53
Reviewer:	John DiBartolomeo	E-signed by: John DiBartolomeo on 2020-05-07 11:23:33
Reviewer:	David Herrell	E-signed by: David Herrell on 2020-05-07 14:00:34
Approver:	R. Jason Gwaltney	E-signed by: R. Jason Gwaltney on 2020-05-07 14:04:23

QA Statement of Compliance

This document has been prepared, reviewed, and approved in accordance with the Quality Assurance requirements of the MPR Standard Quality Program.

Created: 2020-05-07 11:13:21
Project-Task No. 1129G046-0172

MPR Associates, Inc.
320 King St. • Alexandria, VA 22314
(703) 519-0200 • www.mpr.com

Vendor Independent Boiling Water Reactor Non-Safety Platform and Redundant Reactivity Control Requirements Baseline

RECORD OF REVISIONS		
Revision Number	**Pages /Sections Revised**	**Revision Description**
0	All	Original Issue

Table of Contents

Figures

1.0 Introduction

1.1. Purpose

This document identifies vendor-independent Distributed Control System (DCS) non safety related (NSR) digital platform functional requirements and associated functional requirements for the Diverse Actuation System (DAS) functions that are implemented as augmented quality applications within the DCS. These baseline Boiling Water Reactor (BWR) instrumentation and control (I&C) functional requirements have been developed as a tool for the nuclear industry to engage vendors in a collaborative effort to conform them with the needs of a particular unit and with the capabilities of the selected vendor's product line.

To provide a firm foundation for this requirements baseline, a particular nuclear plant was selected as a reference for this effort. With the cooperation and support of Exelon Generation, the Limerick Generating Station Unit1 and 2 (LGS) was chosen as the reference plant for this effort. Because of this, the information contained herein is tailored to the LGS plant design and reflects design decisions made by the Exelon design team to achieve objectives associated with their digital transformation plans. Exelon is using these baseline requirements as part of a pilot effort to perform first echelon I&C upgrades at LGS.

When used by other utilities, the baseline requirements provided herein need to be adapted to conform to that utility's particular unit design, the equipment capabilities of that utility's selected vendor's equipment, and to that utility's particular I&C digitalization strategy.

The functional requirements are provided in a narrative form to describe the process control and operational philosophy of the system. These functional requirements also describe system interlocks and process limits for assuring the equipment protective functions needed for safe and proper operation of the system. Requirements are also identified for the NSR digital platform upon which the NSR system functions will reside.

1.2. Background

The design of many existing BWR safety related (SR) and NSR systems is based either on analog or solid state control logic technology both of which are obsolete and becoming difficult to maintain. In order to address this concern, a solution that supports an overall digital transformation strategy is being pursued. The objective within this document is to provide the framework for an initial migration of selected NSR system(s) that will reside on a common and easily expandable digital platform. In turn, this establishes a prescriptive and cost-effective approach that can support the future migration of other obsolete plant control systems to the common platform.

The LGS BWR system selected for migration to the NSR DCS is the Redundant Reactivity Control System (RRCS). The RRCS is currently classified as a SR system. RRCS provides a diverse means of shutting down the reactor, essentially serving as a diverse actuation system for the Reactor Protection System (RPS). The RRCS satisfies the Nuclear Regulatory Commission (NRC) requirements for the Anticipated Transient Without a Scram (ATWS) rule defined in 10 CFR 50.62. The rule does not require the ATWS equipment to be safety related but that the

equipment is designed to be independent from the primary SR equipment and perform its function in a reliable manner. Generic Letter 85-06 was issued to provide quality assurance guidance for the ATWS NSR equipment, which is required to be augmented quality.

The design requirements (DRs) and source / basis identified within this document reflect the existing RRCS SR pedigree that is based on an Appendix B Quality Assurance (QA) program, General Design Criteria, adopted regulatory guides, and industry standards. This document does not require the vendor's proposed design to meet these design requirements verbatim, but rather that the regulations, regulatory guidance, and industry standards are used by the vendor to frame a level of rigor and augmented quality for the proposed solution that demonstrates that the NSR ATWS function will perform its function in a reliable manner. The utility will establish their expectations for augmented quality and work with the vendor to identify either how a design requirement is satisfied or how the spirit of the design requirement is met.

1.3. Description of Scope

1.3.1. The scope of this specification encompasses the following system at each unit:

- Redundant Reactivity Control System

1.3.2. The scope of this specification will be extended to be applicable to the other Nuclear Steam Supply Shutoff System (N4S) and Emergency Core Cooling System (ECCS) functions that the Defense-in-Depth and Diversity (D3) Analysis determines are required to support the Plant Protection System (PPS). Requirements for the other elements of the DAS to be implemented in the DCS to support the D3 determination will be added to this specification in a later revision.

1.3.3. This document provides the design, functional and performance requirements for the instrumentation and control functionality that represents, to the extent practical, the licensing and design basis of the original system.

1.3.4. Existing field sensors (that provide inputs to the system) and actuated devices (that receive outputs from the system) will remain unchanged for purposes of this document. Therefore, the requirements identified are focused on that portion of the original system that support the protection and control logic functionality. It should be noted that the elimination of any Single Component Vulnerability (SCV) is dependent on the specific cost benefit analysis for eliminating such a SCV. While the elimination of SCVs is always desirable, eliminating SCVs in field sensors and actuated devices is beyond the scope of these functional requirements. Accordingly, SCVs in field sensors and actuated devices would be uniquely addressed as part of the design change process associated with each system migration to the common platform.

1.3.5. This document also identifies requirements that define the unique features and capabilities for the digital architecture that is to be employed as the common platform with consideration of being further expanded to support future non-safety related applications.

1.3.6. The control logic and functionality associated with the system listed in Section 1.3.1 resides as an application on a single common digital platform defined as the DCS. To that end, the original "system" shall be termed a NSR function within this DCS.

1.3.7. The functionality of the existing functions migrated to the DCS replicates to the extent possible the original analog and solid state control systems at LGS, but with additional enhancements that can be leveraged using the existing capabilities and features of the digital architecture (e.g., fault tolerant control processors).

1.3.8. The requirements for the DCS have been developed with a goal of reducing instrumentation, eliminating physical switches, indicators, and recorders (to the extent possible), and reducing/eliminating tech spec surveillances, calibration checks, loop calibrations, etc.

1.4. Approach / Concept

1.4.1. By using a single digital platform to support all of the DCS functions, it is possible to reduce the number of monitored plant process parameters, many of which are functional duplicates of each other, that are currently used for an existing system. The objective is to establish a minimum population of monitored plant process parameters that can be shared by current and future functions on the DCS. As part of the overall digital transformation strategy for LGS, this migration of functions to a common digital platform is being performed in concert with a similar effort being pursued to migrate SR functions to a SR digital platform. The effort to reduce the population of monitored plant variables is being achieved by sharing the same SR plant process parameter signals with the functions on the DCS via a qualified SR-NSR signal isolator. This isolation could take the form of a traditional electrical analog isolator, a data diode between digital communications ports of the SR to the NSR platforms, or a one-way fiber optic transmission network from the SR to the NSR platforms. The DAS concept will leverage a two division / four channel arrangement that utilizes a 2 out of 4 (2oo4) voting scheme for each of the NSR DAS functions implemented in the DCS, to the extent practical. Figure 1-1 provides a representation of this logic arrangement.

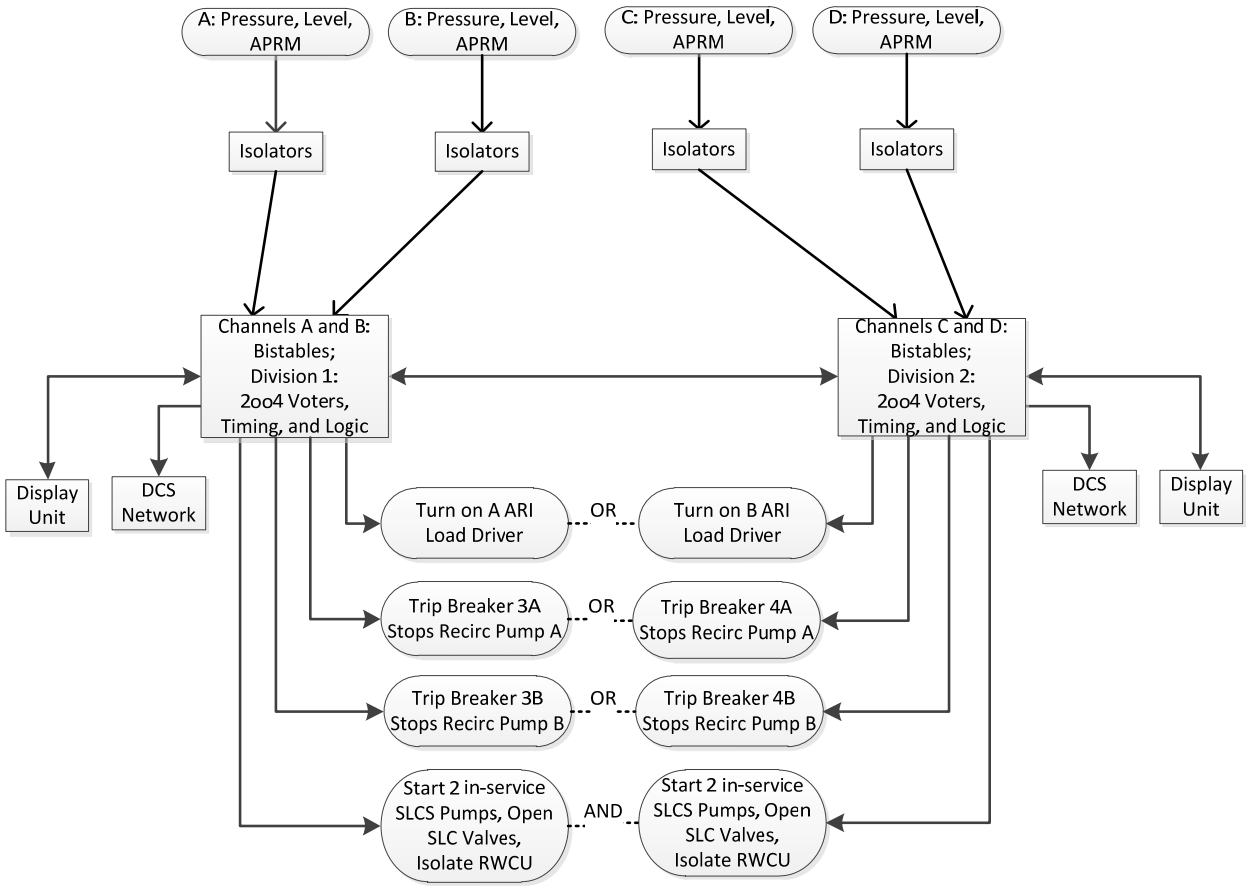

Figure 1-1. Logic Arrangement

1.5. Definitions

1.5.1. Plant Protection System (PPS): The single common SR digital platform on which the SR protection functions and subfunctions shall exist as applications.

1.5.2. Distributed Control System (DCS): The single common NSR digital platform on which the NSR protection functions shall exist as applications.

1.5.3. NSR Protection and Control Function: Functions which replicate those provided by the LGS original systems (e.g., RRCS).

1.6. Acronyms and Abbreviations

Term	Definition for this document
0oo4	Zero-out-of-four (voting) (to allow reset of RRCS)
1oo1	One-out-of-one (voting)
1oo2	One-out-of-two (voting)
2oo2	Two-out-of-two (voting)
2oo3	Two-out-of-three (voting)
2oo4	Two-out-of-four (voting)
AER	Auxiliary Equipment Room
ARI	Alternate Rod Insertion
ATWS	Anticipated Transient Without Scram
BWR	Boiling Water Reactor
CFR	Code of Federal Regulations
CRD	Control Rod Drive
D3	Defense-in-Depth and Diversity
DAS	Diverse Actuation System
DCS	Distributed Control System
DKT	Display, Keyboard, and Trackball (or Touchscreen)
DR	Design Requirement
DST	Daylight Savings Time
ECCS	Emergency Core Cooling System
EIM	Equipment Interface Modules
EWS	Engineering Work Station
FR	Functional Requirement
FRU	Field Replaceable Units
FTP	File Transfer Protocol
GDC	General Design Criteria
HMI	Human-Machine Interface
I&C	Instrumentation & Control
LGS	Limerick Generating Station Units 1 and 2

Term	Definition for this document
LOCA	Loss of Coolant Accident
MWe	Megawatts Electric
MWt	Megawatts Thermal
N4S	Nuclear Steam Supply Shutoff System
NAN	Not a Number
NRC	Nuclear Regulatory Commission
NSR	Non-Safety Related
PPS	Plant Protection System
RPS	Reactor Protection System
QA	Quality Assurance
RO	Reactor Operator
RRCS	Redundant Reactivity Control System
RWCU	Reactor Water Cleanup
SCV	Single Component Vulnerability
SDOE	Secure Development and Operational Environment
SOE	Sequence of Events
SR	Safety Related
SRO	Senior Reactor Operator
SSC	Systems, Structures and Components
SLCS	Standby Liquid Control System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
V&V	Verification and Validation
UFSAR	Updated Final Safety Analysis Report
UTC	Coordinated Universal Time

2.0 System Description and Criteria

2.1. General Description

2.1.1. LGS is comprised of two units located on the east bank of the Schuylkill River in Limerick Township of Montgomery County, Pennsylvania. LGS is approximately 4 river miles downriver from Pottstown, 35 river miles upriver from Philadelphia, and 49 river miles above the confluence of the Schuylkill with the Delaware River. Each of the LGS units employs a GE Boiling Water Reactor (BWR) originally designed and licensed to operate at a rated core thermal power of 3293 megawatts thermal (MWt) at 100% steam flow with a corresponding gross electrical output of 1092 megawatts electric (MWe). The Units were rerated to a power output of 3458 MWt and a subsequent power uprate through measurement uncertainty recapture (MUR) to 3515 MWt.

2.2. General Design Criteria

2.2.1. The LGS design conforms to the requirements given in 10 CFR 50, Appendix A, "General Design Criteria for Nuclear Power Plants."

2.2.2. The plant is designed in such a way that the release of radioactive materials to the environment does not exceed the limits and guideline values of applicable government regulations pertaining to the release of radioactive materials for normal operations, and for abnormal transients and accidents. Various systems are designed to permit safe plant operation and to accommodate postulated accidents without endangering the health and safety of the public.

2.3. Non-Safety Related Systems Description

2.3.1. General

Certain systems provide actions necessary to support safe shutdown, to protect the integrity of radioactive material barriers, and/or to prevent the release of radioactive material in excess of allowable dose limits. These systems can be components, groups of components, systems, or groups of systems.

2.3.2. Distributed Control System

The DCS is a NSR digital platform that will execute the protective and control functions for the diverse reactor scram system identified in Section 2.3.3. The control and logic functionality of this system will exist on the DCS as an individual application.

2.3.3. Redundant Reactivity Control System

The RRCS provides a redundant and diverse method of initiating an automatic reactor shutdown through insertion of the control rods (scram) if monitored system variables exceed pre-established limits. This action is taken in time to prevent fuel damage and limit system pressure, thus restricting the release of radioactive material. The RRCS is designed to mitigate the potential consequences of an ATWS event.

2.4. Systems Criteria

2.4.1. General

2.4.1.1 Certain systems act in response to abnormal operational transients so that fuel cladding retains its integrity as a radioactive material barrier to keep any failures within acceptable limits.

2.4.1.2 Certain systems act to ensure that no damage to the nuclear system process barrier results from internal pressures caused by abnormal operational transients or accidents.

2.4.1.3 Certain systems act to prevent radioactive material released from the containment volumes from exceeding the guideline values of applicable regulations.

2.4.1.3 Certain systems act to act to prevent radioactive material released from the containment volumes from exceeding the guideline values of applicable regulations.

2.4.1.4 Where positive, precise actions are immediately required in response to accidents, these actions are automatic and require no decision or manipulation of controls by operations personnel.

2.4.1.5 Essential actions are carried out by equipment of sufficient redundancy and independence so that no single failure of active components prevents the required actions.

3.0 System Requirements

The identification of the applicable design and functional requirements for the RRCS system to be migrated to the digital platforms begins with a review of relevant documents. The types of documents reviewed included, but were not limited to, the Updated Final Safety Analysis Report (UFSAR), plant drawings, plant procedures, Design Basis Documents (DBDs), specifications, calculations, and system descriptions. The lists of LGS documentation used in the development of the respective design and functional requirements for the systems are identified in Section 5 and separately identified throughout the requirements listed in the accompanying appendices.

The requirements for the I&C portions of the system that describe the system functionality are listed as functional requirements in the appendices. The functional requirements incorporate elements that reflect design constraints, physical constraints, licensing commitments, system interfaces, system boundaries, control philosophy, controlling parameters, etc.

3.1. Redundant Reactivity Control System

The primary function of the RRCS is to mitigate the potential consequences of an ATWS event. The RRCS provides signals to mitigate an ATWS event by:

- Initiating an Alternate Rod Insertion (ARI) which is redundant and diverse from the normal RPS
- Tripping the reactor recirculation pump (RPT)
- Initiating the Standby Liquid Control System (SLCS) and isolating the Reactor Water Cleanup System (RWCU) automatically

NOTE: One of the existing functions of the RRCS is to provide feedwater runback. As part of this digital modernization effort, this function will be removed as part of a project team decision and is not included as a requirement within this document.

The RRCS provides the ATWS function by monitoring certain plant parameters and, if one or more parameters exceeds a specified limit, power is applied to scram pilot valve solenoids in the Control Rod Drive (CRD) System which, when energized, exhaust air from the scram valves causing the control rods to scram.

3.1.1. Interface Requirements

These reflect the logical and physical interfaces between the RRCS and other systems, platforms, etc. These interfaces are accounted for within the developed functional requirements within the appendices.

The RRCS function will have protection and control logic interfaces with the following PPS functions or external systems:

PPS Functions

Shared monitored parameter signals, isolated by qualified isolators in the PPS

External Systems

120VAC System

Class 1E 125VDC System

Neutron Monitoring System

Reactor Recirculation System

Control Rod Drive System

Standby Liquid Control System

Reactor Water Cleanup System

3.1.2. Design Requirements

These reflect the requirements that establish the licensing and design basis for the existing system that have been incorporated into various codes, criteria, and regulatory requirements. For the I&C portions of the systems, the regulatory guides, 10 CFR 50 Appendix A "General Design Criteria" (GDC), and industry codes and standards that are applicable are listed in the respective design requirements section of the appendices. As discussed earlier, this document does not require the vendor's proposed design to meet these design requirements verbatim but rather that they are used by the vendor to frame a level of rigor and augmented quality for the proposed solution that demonstrates that the NSR ATWS function will perform its function in a reliable manner. The utility will establish their expectations for augmented quality and work with the vendor to identify either how a design requirement is satisfied or how the spirit of the design requirement is met.

Design requirements for the RRCS include regulatory, industry, and project defined requirements. These are identified in Appendix A-1. The design requirements are identified by a RRCS-DR-XX designation.

3.1.3. Performance Requirements

These reflect the requirements associated with the I&C portion of the system that are required to be fulfilled when the particular application is migrated to the DCS. These are listed in the respective design requirements section of the appendices.

3.1.3.1 ARI Response Time

The RRCS signal input to ARI actuation output propagation time is less than TBD milliseconds.

Basis: TBD by LGS

3.1.3.2 Recirculation Pump Trip Time

The maximum time delay between occurrence of an RRCS initiation signal on high Reactor pressure to the completion of the RPT breaker function is 230 milliseconds. There is no minimum Recirculation Pump trip time.

Basis: NEDE-24222

3.1.3.3 Recirculation Pump Trip Time Delay

The recirculation pump trip time delay between occurrence of an RRCS initiation signal on low Reactor water level (Level 2) and the time that the RRCS sends the signal to trip the Recirculation pump drive motor breakers is a minimum of 8 seconds and a maximum of 10.2 seconds.

Basis: GENE-637-011-0493, NEDE-20566-P

3.1.3.4 SLCS Startup Time Delay

The RRCS signal input to SLCS actuation output occurs after 118 seconds, unless inhibited by the operator.

Basis: NUREG 0991, NEDE-24222

3.1.4. Functional Requirements

The functional requirements (FRs) reflect the I&C portions of the system that incorporate elements that reflect design constraints, physical constraints, licensing commitments, system interfaces, system boundaries, control philosophy, controlling parameters, etc.

The functional requirements define the control philosophy required to fulfill the function of the RRCS. These are identified in Appendix A-2. The functional requirements are identified by a RRCS-FR-XX designation.

4.0 NSR Platform Requirements

In order to support the digital transformation strategy, a common digital platform is to be leveraged. The identification of the applicable functional requirements for the NSR platform was based on the familiarity with features and capabilities that are available with and unique to digital platform designs. Many of these functional requirements reflect typical architecture, human-machine interface (HMI), communication, and other related requirements prevalent in the industry.

Requirements for the DCS are identified in Appendix B-1 and are identified by a DCS-XX designation.

4.1. Functional Requirements

There are a number of functional requirements identified that that are unique to the needs of the LGS project. Platform requirements have been identified and are categorized into several categories identified below.

- Safety Classification
- Platform Architecture
- System I/O
- Independence, Separation and Segmentation
- Health Monitoring
- Surveillance Testing
- Communication
- Human-Machine Interface
- Display, Keyboard, and Trackball (DKT) HMIs
- Data Historian, Sequence of Events, Data Transmission
- Cyber Security
- Simulator

4.2. Environmental Characteristics

Electromagnetic Compatibility

Cabinet Requirements

Environmental Parameters

5.0 References

5.1. Code of Federal Regulations (CFR)

Appendix A to 10 CFR Part 50, General Design Criteria for Nuclear Power Plants

5.1.1. GDC 1 – Quality Standards and Records

5.1.2. GDC 2 – Design Bases for Protection Against Natural Phenomena

5.1.3. GDC 3 – Fire Protection

5.1.4. GDC 4 – Environmental and Dynamic Effects Design Bases

5.1.5. GDC 20 – Protection System Functions

5.1.6. GDC 21 – Protection System Reliability and Testability

5.1.7. GDC 22 – Protection System Independence

5.1.8. GDC 29 – Protection Against Anticipated Operational Occurrences

5.1.9. 10 CFR 50.62, Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants

5.2. Nuclear Regulatory Commission

5.2.1. Generic Letter 85-06, “Quality Assurance Guidance for ATWS Equipment That is Not Safety-Related”

5.2.2. Regulatory Guide 1.6 (March 1971) – Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems (Safety Guide 6)

5.2.3. Regulatory Guide 1.22 (February 1972) – Periodic Testing of Protection System Actuation Functions (Safety Guide 22)

5.2.4. Regulatory Guide 1.29 (September 1978) – Seismic Design Classification

5.2.5. Regulatory Guide 1.30 (August 1972) – Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment (Safety Guide 30)

5.2.6. Regulatory Guide 1.32 (February 1977) – Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants

5.2.7. Regulatory Guide 1.47 (May 1973) – Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

5.2.8. Regulatory Guide 1.53 (June 1973) – Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems

5.2.9. Regulatory Guide 1.62 (October 1973) – Manual Initiation of Protective Actions

5.2.10. Regulatory Guide 1.75 (September 1978) – Physical Independence of Electric Systems

5.2.11. Regulatory Guide 1.89 (November 1974) – Qualification of Class 1E Equipment for Nuclear Power Plants

5.2.12. Regulatory Guide 1.100 (August 1977) – Seismic Qualification of Electric Equipment for Nuclear Power Plants

5.2.13. Regulatory Guide 1.105 (November 1976) – Instrument Setpoints

5.2.14. Regulatory Guide 1.118 (June 1978) – Periodic Testing of Electric Power and Protection Systems

5.2.15. Regulatory Guide 1.152 (July 2011) - Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

5.2.16. Regulatory Guide 1.168 (July 2013) - Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

5.2.17. Regulatory Guide 1.169 (July 2013) - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

5.2.18. Regulatory Guide 1.170 (July 2013) - Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

5.2.19. Regulatory Guide 1.171 (July 2013) - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

5.2.20. Regulatory Guide 1.172 (July 2013) - Software Requirement Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants

5.2.21. Regulatory Guide 1.173 (July 2013) - Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

5.2.22. DI&C-ISG-04, Interim Staff Guidance, Revision 1, Highly-Integrated Control Rooms – Communications Issues (HICRc)

5.2.23. NUREG/CR-6463, 1996, Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems

5.2.24. NUREG-0700, Rev 2, Human-System Interface Design Review Guidelines

5.2.25. NUREG-0711, Rev 3, Human Factors Engineering Program Review Model

5.3. Industry Standards

5.3.1. IEEE Std. 279-1971 – IEEE Standard Criteria for Protection Systems for Nuclear Power Generating Stations

5.3.2. IEEE Std. 308 (1971 and 1974) – Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations

5.3.3. IEEE Std. 323 (1971 and 2003) – General Guide for Qualifying Class 1 Electric Equipment for Nuclear Power Generating Stations

5.3.4. International Electrotechnical Commission (IEC)/IEEE 60780/323 2016, Nuclear facilities – Electrical equipment important to safety – Qualification

5.3.5. IEEE Std. 336 (1971 and 2010) - IEEE Standard Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment during the Construction of Nuclear Power Generating Stations

5.3.6. IEEE Std. 338 (1971, 1975, 1977, 1987 and 2012) – Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems

5.3.7. IEEE Std. 344 (1971 and 1975) – Guide for Seismic Qualification of Class 1 Electric Equipment for Nuclear Power Generating Stations

5.3.8. IEEE Std. 379 (1972, 1977, 2003 and 2014) – Guide for the Application of the Single Failure Criterion to Nuclear Power Generating Station Protection Systems

5.3.9. IEEE Std. 384 (1977 and 2018) – Criteria for Independence of Class 1E Equipment and Circuits

5.3.10. IEEE Std. 603 (1991 and 2018) – Standard Criteria for Safety Systems for Nuclear Power Generating Stations

5.3.11. IEEE Std. 7-4.3.2 (2003 and 2016) – Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

5.3.12. ANS 3.5-2009, Nuclear Power Plant Simulators for Use in Operator Training and Examination

5.4. Limerick Drawings

5.4.1. M-1-C22-1050-E-100 through M-1-C22-1050-E-142, “Redundant Reactivity Control Sys”

5.5. Limerick Specific Documents

5.5.1. LGS Unit 1 Technical Specification (Through Amendment 235)

5.5.2. LGS Updated Final Safety Analysis Report (USFAR), Rev 16

5.5.3. M-171, Rev 17, Specification for Environmental Service Conditions Limerick Generating Stations Units 1&2

5.5.4. NEDE-20566-P, November 1975, General Electric Company Analytical Model for Loss-of-Coolant Analysis in Accordance with 10CFR50, Appendix K

5.5.5. NEDE-24222, December 1979, General Electric Licensing Topical Report for Assessment of BWR Mitigation of ATWS

5.5.6. GENE-637-011-0493, April 1993, General Electric Licensing Topical Report for Evaluation of Limerick ATWS Performance for Power Rerate Condition

5.5.7. L-S-55, Rev 2, Redundant Reactivity Control System

A

A.1 RRCS Design Requirements

NOTE

The design requirements identified within this Appendix reflect the existing RRCS SR pedigree that is based on an Appendix B QA program, General Design Criteria, adopted regulatory guides and industry standards. It is not the intent of this document to require the vendor's proposed design to meet these design requirements verbatim, but rather that they are used by the vendor to frame a level of rigor and augmented quality for the proposed solution that demonstrates that the NSR ATWS function will perform its function in a reliable manner. The utility will establish their expectations for augmented quality and work with the vendor to identify either how a design requirement is satisfied or how the spirit of the design requirement is met.

RRCS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RRCS-DR-1	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. 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. 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.	GDC 1 - Quality standards and records.
RRCS-DR-2	Structures, systems, and components important to safety shall be designed to withstand the effect of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions.	GDC 2 - Design Bases for Protection Against Natural Phenomena
RRCS-DR-3	Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions.	GDC 3 - Fire protection
RRCS-DR-4	Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents (LOCAs).	GDC 4 - Environmental and dynamic effects design bases

RRCS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RRCS-DR-5	A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident. 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.	GDC 19 - Control Room
RRCS-DR-6	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.	GDC 20 - Protection system functions
RRCS-DR-7	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.	GDC 21 - Protection system reliability and testability

RRCS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RRCS-DR-8	The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. 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.	GDC 22- Protection system independence
RRCS-DR-9	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.	GDC 24 - Separation of protection and control systems
RRCS-DR-10	The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.	GDC 29 - Protection against anticipated operational occurrences
RRCS-DR-11	The protection and reactivity control systems shall be designed to assure that onsite electrical power systems have sufficient independence to perform their safety functions assuming a single failure.	Regulatory Guide 1.6 - Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems (Safety Guide 6)
RRCS-DR-12	The protection system shall be designed to permit periodic testing of its initiation functions inclusive of the actuation devices and actuated equipment when the reactor is in operation.	Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions (Safety Guide 22)

RRCS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RRCS-DR-13	Those structures, systems, and components (SSC) that should be designed to remain functional if the Safe Shutdown Earthquake (SSE) occurs shall be designated as Seismic Category I. (This includes Systems or portions of systems that are required for reactor shutdown; all electric and mechanical devices and circuitry between the process and the input terminals of the actuator systems involved in generating signals that initiate protective action; systems or portions of systems that are required for (1) monitoring of systems important to safety and (2) actuation of systems important to safety.)	Regulatory Guide 1.29 - Seismic Design Classification
RRCS-DR-14	The RRCS shall comply with the requirements of Appendix B to 10 CFR Part 50 for the installation, inspection, and testing of nuclear power plant instrumentation and electric equipment.	Regulatory Guide 1.30 - Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment (Safety Guide 30)
RRCS-DR-15	The RRCS shall meet the requirements for design, operation, and testing of safety-related power systems within nuclear power plants as defined within IEEE Std. 308.	Regulatory Guide 1.32 - Criteria for Power Systems for Nuclear Power Plants
RRCS-DR-16	The RRCS shall meet the requirements for indicating the bypass or inoperable status of portions of the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the system it actuates to perform their safety-related functions:	Regulatory Guide 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
RRCS-DR-17	The RRCS shall comply with the IEEE Std. 279 requirement that any single failure within the protection system shall not prevent proper protective action at the system level when required, by utilizing the guidance in IEEE Std. 379-1972 for applying the single-failure criterion to the design and analysis of nuclear power plant protection systems.	Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Safety Systems
RRCS-DR-18	The RRCS shall provide a means for manual initiation of protective actions.	Regulatory Guide 1.62 - Manual Initiation of Protective Actions

RRCS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RRCS-DR-19	The RRCS shall meet the requirements for physical independence of the circuits and electric equipment comprising or associated with the Class 1E power system, the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the systems it actuates to perform their safety related functions.	Regulatory Guide 1.75 - Physical Independence of Electric Systems
RRCS-DR-20	The RRCS shall comply with design verification requirements to verify adequacy of design under the most adverse design conditions.	Regulatory Guide 1.89 - Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants
RRCS-DR-21	The RRCS shall comply with design verification requirements to verify the seismic adequacy of electric equipment.	Regulatory Guide 1.100 - Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants
RRCS-DR-22	The RRCS shall design shall implement setpoints that assure sufficient margin between Technical Specification limits and the trip setpoint to account for instrument inaccuracy, calibration uncertainties, and instrument drift. Consideration of instrument span and range as well as environmental influences must be included.	Regulatory Guide 1.105 - Instrument Setpoint
RRCS-DR-23	The RRCS shall comply with the requirements for periodic testing of electric power and protection systems.	Regulatory Guide 1.118 - Periodic Testing of Electric Power and Protection Systems
RRCS-DR-24	The RRCS shall, with precision and reliability, initiate a reactor scram to prevent or limit fuel damage following abnormal operational transients; prevent damage to the RCPB as a result of excessive internal pressure; and limit the uncontrolled release of radioactive materials from the fuel assembly or RCPB.	IEEE Std. 603, Section 5.0 Safety System Criteria and 6.1 Automatic Control

RRCS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RRCS-DR-25	The RRCS shall initiate a trip when the analog signal exceeds a level corresponding to the following trip setpoint: Reactor Vessel Water Level ≤ -38 inches Reactor Vessel Pressure ≥ 1149 psig	IEEE Std. 603, Section 6.1 Automatic Control
RRCS-DR-26	The signal input to actuation output propagation time of the RRCS ARI logic shall be less than TBD milliseconds.	IEEE Std. 603, Section 4.10
RRCS-DR-27	The RRCS shall be capable of initiating a reactor scram under all modes of reactor operation.	IEEE Std. 603, Section 4.1
RRCS-DR-28	The RRCS shall be capable of initiating a reactor scram via discrete signals (contact input) from dual, concurrent manually initiated switches.	IEEE Std. 603, Section 6.2 Manual Control
RRCS-DR-29	The RRCS shall ensure that the protective action, once started, continues to completion.	IEEE Std. 603, Section 5.2 Completion of Protective Action
RRCS-DR-30	Any single failure within the RRCS shall not prevent proper protective action at the system level when required.	IEEE Std. 603, Section 5.1 Single Failure Criterion and IEEE Std. 7-4.3.2 Section 5.1 Single Failure Criterion
RRCS-DR-31	Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.	IEEE Std. 603 section 5.3 Quality and IEEE Std. 7-4.3.2 section 5.3 Quality
RRCS-DR-32	Type test data or reasonable engineering extrapolation based on test data shall be available to verify that protection system equipment shall meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements.	IEEE Std. 603 section 5.4 Equipment Qualification and IEEE Std. 7-4.3.2 section 5.4 Equipment Qualification

RRCS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RRCS-DR-33	The RRCS system channels shall be designed to maintain necessary functional capability under extremes of conditions (as applicable) relating to environment, energy supply, malfunctions and accidents.	IEEE Std. 603 section 5.5 System Integrity and IEEE Std. 7-4.3.2 and section 5.5 Independence
RRCS-DR-34	The PPS and RRCS shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction. As allowed by 10 CFR 50.62, the PPS and RRCS can share the same transmitters as signal sources.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 System Integrity
RRCS-DR-35	Any equipment that is used for both protective and control functions shall be classified as part of the protection system and shall meet all the applicable requirements. The DAS functions in the DCS shall be segmented from the DCS plant control functions in a manner that precludes any adverse effects on the DAS functions by the control functions.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence
RRCS-DR-36	The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system and shall meet all the applicable requirements. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified.	IEEE Std. 603 section 5.6 Independence and IEEE Std. 7-4.3.2 and section 5.6 Independence
RRCS-DR-37	Provisions shall be included so that the protective action can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel.	IEEE Std. 603 section 6.3 Interaction Between the Sense and Command Features and Other Systems
RRCS-DR-38	To the extent feasible and practical protection system inputs shall be derived from signals that are direct measures of the desired variables.	IEEE Std. 603 section 6.4 Derivation of System Inputs

RRCS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RRCS-DR-39	Means shall be provided for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
RRCS-DR-40	Capability shall be provided for testing and calibrating channels and the devices used to derive the final system output signal from the various channel signals.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
RRCS-DR-41	For those parts of the system where the required interval between testing will be less than the normal time interval between generating station shutdowns, there shall be capability for testing during power operation.	IEEE Std. 603 section 6.5 Capability for Testing and Calibration
RRCS-DR-42	The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective action at the systems level.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
RRCS-DR-43	During such operation, the active parts of the system shall of themselves continue to meet the single failure criterion.	IEEE Std. 603 sections 6.7 Maintenance Bypass and 7.5 Maintenance Bypass
RRCS-DR-44	Where operating requirements necessitate automatic or manual bypass of a protective function, the design shall be such that the bypass will be removed automatically whenever permissive conditions are not met.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
RRCS-DR-45	Devices used to achieve automatic removal of the bypass of a protective function are part of the protection system and shall be designed in accordance with these criteria.	IEEE Std. 603 sections 6.6 Operating Bypasses and 7.4 Operating Bypasses
RRCS-DR-46	If the protective action of some part of the system has been bypassed or deliberately rendered inoperative for any purpose, this fact shall be continuously indicated in the control room.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RRCS-DR-47	The design shall permit the administrative control of the means for manually bypassing channels or protective functions.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access

RRCS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RRCS-DR-48	The devices used to prevent improper use of less restrictive set points shall be considered a part of the protection system and shall be designed in accordance with the other provisions of these criteria regarding performance and reliability.	IEEE Std. 603 section 6.8 Setpoints
RRCS-DR-49	The protection system shall be so designed that, once initiated, a protective action at the system level shall go to completion.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action
RRCS-DR-50	Return to operation shall require subsequent deliberate operator action.	IEEE Std. 603 sections 5.2 Completion of Protective Action and 7.3 Completion of Protective Action
RRCS-DR-51	The protection system shall include means for manual initiation of each protective action at the system level (for example, reactor trip, containment isolation, safety injection, core spray, etc.). The ATWS functions shall provide a grouped sequential application of means to shut down the nuclear reaction.	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
RRCS-DR-52	No single failure within the manual, automatic, or common portions of the protection system shall prevent initiation of protective action by manual or automatic means.	IEEE Std. 603 section 7.2 Manual Control
RRCS-DR-53	Manual initiation should depend upon the operation of a minimum of equipment.	IEEE Std. 603 sections 6.2 Manual Control and 7.2 Manual Control
RRCS-DR-54	The design shall permit the administrative control of access to all set point adjustments, module calibration adjustments, and test points.	IEEE Std. 603 section 5.9 Control of Access and IEEE Std. 7-4.3.2 section 5.9 Control of Access
RRCS-DR-55	Protective actions shall be indicated and identified down to the channel level.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RRCS-DR-56	The protection system shall be designed to provide the operator with accurate, complete, and timely information pertinent to its own status and to generating station safety.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays
RRCS-DR-57	The design shall minimize the development of conditions which would cause meters, annunciators, recorders, alarms, etc., to give anomalous indications confusing to the operator.	IEEE Std. 603 section 5.8 Information Displays and IEEE Std. 7-4.3.2 section 5.8 Information Displays

RRCS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RRCS-DR-58	The system shall be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.	IEEE Std. 603 section 5.10 Repair
RRCS-DR-59	In order to provide assurance that the requirements given in this document can be applied during the design, construction, maintenance, and operation of the plant, the protection system equipment (for example, interconnecting wiring, components, modules, etc.), shall be identified distinctively as being in the protection system.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
RRCS-DR-60	This identification shall distinguish between redundant portions of the protection system. (In the installed equipment, components, or modules mounted in assemblies that are clearly identified as being in the protection system do not themselves require identification.) All software, firmware, and programmable logic shall be identified in accordance with IEEE Std. 7-4.3.2 Clause 5.11.	IEEE Std. 603 section 5.11 Identification and IEEE Std. 7-4.3.2 section 5.11 Identification
RRCS-DR-61	The RRCS shall conform to the design criteria and features for Class 1E electric systems to ensure that functional requirements under the conditions produced by design basis events are met.	IEEE Std. 308 - Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations
RRCS-DR-62	The RRCS shall conform to the methods for demonstrating the qualification of Class 1E equipment including components or equipment of any interface whose failure could adversely affect the performance of Class 1E systems and electronic equipment.	IEEE Std. 323 - Qualifying Class 1E Equipment for Nuclear Power Generating Stations
RRCS-DR-63	RRCS shall conform to the design and operational criteria for the performance of periodic testing of nuclear power generating station safety systems.	IEEE Std. 338 - Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems
RRCS-DR-64	RRCS shall meet its Class 1E performance requirements during and following one SSE (safe shutdown earthquake) after a number of OBEs (operating basis earthquakes).	IEEE Std. 344 - Guide for Seismic Qualification of Class 1 Electric Equipment for Nuclear Power Generating Stations

RRCS DESIGN REQUIREMENTS		
ID #	**Requirement**	**New Source / Basis**
RRCS-DR-65	RRCS shall meet the single failure criterion as described and classified in IEEE 379.	IEEE Std. 379 - Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems
RRCS-DR-66	RRCS shall meet the criteria and requirements for establishing and maintaining the independence of Class 1E equipment and circuits and auxiliary supporting features by physical separation and electrical isolation.	IEEE Std. 384 - Criteria for Independence of Class 1E Equipment and Circuits
RRCS-DR-67	The DAS functions, including the RRCS, may not make use of any PPS or other data provided through the serial data links to the DCS.	Design requirement to minimize the potential for PPS software common cause failure affecting the DAS function.

A.2 RRCS Functional Requirements

NOTE

The source / basis identified within this Appendix reflect the existing RRCS SR pedigree that is based on an Appendix B QA program, General Design Criteria, adopted regulatory guides and industry standards. It is not the intent of this document to require the vendor's proposed design to meet these source / basis requirements verbatim, but rather that they are used by the vendor to frame a level of rigor and augmented quality for the proposed solution that demonstrates that the NSR ATWS function will perform its function in a reliable manner. The utility will establish their expectations for augmented quality and work with the vendor to identify either how a design requirement is satisfied or how the spirit of the design requirement is met.

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-1	The DCS/RRCS shall be capable of initiating an ARI signal either automatically when any of the monitored parameters exceeds a pre-established value, or by manual initiation. RRCS shall also provide outputs for imitating other system/equipment functions.	10CFR50.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-2	DCS/RRCS shall be comprised of two (2) independent and separate divisions (Division 1 and Division 2) to initiate the following: • Alternate Rod Insertion • Recirculation Pump Trip • Standby Liquid Control System Initiation	Reg Guide 1.6, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 384	
RRCS-FR-3	DCS/RRCS shall have four (4) independent channels (Channel A, Channel B, Channel C and Channel D) that each provide votes / signals to each of the divisions.	Reg Guide 1.6, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 384	
RRCS-FR-4	The DCS/RRCS shall be capable of being powered by 125VDC power.	Original design feature	
RRCS-FR-5	The DCS/RRCS shall be a normally de-energized system and energize to trip.	Original design feature	
RRCS-FR-6	Each channel shall receive an isolated (SR to NSR) input from each of the following monitored parameters that are provided as common inputs to the PPS platform, where the isolators are part of the PPS: • Reactor Vessel Pressure (RVP) • Reactor Vessel Water Level 2 (RWL2)	10CFR50.62, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379 Project requirement	
RRCS-FR-7	Each channel shall receive an isolated input (SR transmitter to RRCS NSR input) input from the following monitored parameter (4-20 mA sensor): • SLCS Tank Level (STL)	Original design feature Project requirement	
RRCS-FR-8	Each channel shall provide an annunciate vote to each division when RVP exceeds setpoint high.	Project design approach	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-9	Each channel shall provide a condition vote to each division when RVP exceeds setpoint high.	Project design approach	
RRCS-FR-10	Each channel shall initiate a 20 msec timer when RVP exceeds setpoint high.	Original design feature	The 20ms delay is provided to avoid noise spikes and random transient false operation.
RRCS-FR-11	If RVP still exceeds setpoint when the timer expires, each channel shall seal in the RVP condition.	Original design feature	
RRCS-FR-12	Each channel shall provide an RPT/SLCS vote to each division when the RVP condition is sealed in.	Project design approach	
RRCS-FR-13	Each channel shall initiate a 118 second timer when the RVP condition is sealed in.	Original design feature	
RRCS-FR-14	Each channel shall provide an annunciate vote when the RVP condition is sealed in.	Project design approach	
RRCS-FR-15	When the 118 second timer for the RVP sealed in condition expires, each channel shall provide an SLCS vote for RVP input to each division.	Project design approach	
RRCS-FR-16	When the 118 second timer for the RVP sealed in condition expires, each channel shall provide a reset vote for RVP input to each division.	Project design approach	
RRCS-FR-17	Each channel shall provide an annunciate vote to each division when RWL2 exceeds setpoint low.	Project design approach	
RRCS-FR-18	Each channel shall provide a condition vote to each division when RWL2 exceeds setpoint low.	Project design approach	
RRCS-FR-19	Each channel shall initiate a 20 msec timer when RWL2 exceeds setpoint low.	Original design feature	The 20ms delay is provided to avoid noise spikes and random transient false operation.

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-20	If RWL2 still exceeds setpoint when the timer expires, each channel shall seal in the RWL2 condition.	Original design feature	
RRCS-FR-21	Each channel shall initiate a 9 second timer when the RWL2 condition is sealed in.	Original design feature	
RRCS-FR-22	When the 9 second timer expires, each channel shall provide an RPT vote for RWL2 input to each division.	Project design approach	
RRCS-FR-23	Each channel shall initiate a 118 second timer when the RWL2 condition is sealed in.	Original design feature	
RRCS-FR-24	Each channel shall provide an annunciate vote when the RWL2 condition is sealed in.	Project design approach	
RRCS-FR-25	When the 118 second timer for the RWL2 sealed in condition expires, each channel shall provide an SLCS vote for RWL2 input to each division.	Project design approach	
RRCS-FR-26	When the 118 second timer for the RWL2 sealed in condition expires, each channel shall provide a reset vote for RWL2 input to each division.	Project design approach	
RRCS-FR-27	Each channel shall provide an annunciate vote to each division when STL exceeds setpoint low.	Project design approach	
RRCS-FR-28	Each channel shall provide a condition vote to each division when STL exceeds setpoint low.	Project design approach	
RRCS-FR-29	Each channel shall receive a contact input from each of the following monitored parameters: • APRM Neutron Flux (CI1) • APRM Neutron Flux (CI2)	Original design feature	
RRCS-FR-30	Each channel shall provide a condition vote to each division when CI1 is satisfied (contact closed).	Project design approach	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-31	Each channel shall provide a condition vote to each division when CI2 is satisfied (contact closed).	Project design approach	
RRCS-FR-32	Each input to a channel (ma, contact input, or digital signal) shall be voted on by the channel based on the condition (condition met or not met).	Project design approach	The term "shall be voted on" indicates that the channel performs a bi-stable comparison against a pre-determined configurable setpoint to determine whether the input is at or above/below the setpoint value.
RRCS-FR-33	Each channel shall provide the status of the vote (e.g., vote to not function if condition not met; vote to function if condition met; vote to annunciate) to each of the divisions.	Project design approach	The terms “not function,” “function,” and “annunciate” describe different types of votes that may be provided by a channel. A particular vendor solution may combine one or more of the vote types into a single channel vote based on the capabilities of the platform.
RRCS-FR-34	Each division shall determine whether the votes to function for each type of input satisfy the voting criteria (e.g., 2oo4).	Project design approach	
RRCS-FR-35	Each division shall execute a function when the voting criteria are satisfied.	Project design approach	
RRCS-FR-36	Each division shall not execute a function based on any combination of non-coincident input conditions received from the channels.	Project design approach	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-37	Each division shall generate an output for an isolation, trip, or initiation when the required voting has been satisfied.	Project design approach	As an example, the RWL2 input to Channels A, B, C, and D shall be sent to a 2oo4 voter in each of the divisions (Division 1 and Division 2). When at least two of the four RWL2 inputs to the 2oo4 voter achieve a trip state, the associated division generates an output. The generated output may be dependent on additional voting to be satisfied. Some outputs require different voting schemes which are described within the requirement.
RRCS-FR-38	Each division shall include a manual initiation feature located in the control room that requires two distinct actions (e.g., arming prior to functioning) to be completed.	Original design feature	
RRCS-FR-39	Each division shall provide annunciation for MANUAL INITIATION SWITCH ARMED via the HMI when the first distinct action for the manual initiation has been executed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-40	Only one of the two divisions shall be required to initiate automatic protective actions.	Reg Guide 1.53, IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-41	Each trip system shall be capable of providing outputs to automatically initiate the following protective actions: • Alternate Rod Insertion • Recirculation Pump Trip • Standby Liquid Control System Initiation • Reactor Water Cleanup Isolation	Original design feature	
RRCS-FR-42	Each division shall initiate ARI when 2oo4 condition votes for RVP input are received.	10CFR50.62, IEEE Std. 603/IEEE Std. 7-4.3.2	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-43	Each division shall initiate ARI when 2oo4 condition votes for RWL2 input are received.	10CFR50.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-44	Each division shall initiate ARI when the second distinct action for manual initiation has been executed.	10CFR50.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-45	Each division shall seal in the manual initiation input when the second distinct action for manual initiation has been executed.	Original design feature	
RRCS-FR-46	Each division shall initiate a 118 second timer when the manual initiation input is sealed in.	Original design feature	
RRCS-FR-47	Each division shall initiate a 30 second timer when ARI is initiated.	Original design feature	
RRCS-FR-48	Each division shall provide outputs to energize four (4) division specific 125VDC solenoid valves when ARI is initiated.	NEDE-24222	
RRCS-FR-49	Division 1 shall provide annunciation for RRCS CHANNEL ACTIVATED DIVISION 1 via the HMI when ARI is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-50	Division 2 shall provide annunciation for RRCS CHANNEL ACTIVATED DIVISION 2 via the HMI when ARI is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-51	Each division shall generate an output for RRCS TROUBLE status light capability via the HMI when 1oo4 annunciate votes for RVP input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-52	Each division shall generate an output for RRCS TROUBLE status light capability via the HMI when 1oo4 annunciate votes for RWL2 input is received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-53	Each division shall generate an output for RRCS ARI INITIATED status light capability via the HMI when 2oo4 annunciate votes for RVP inputs are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-54	Each division shall generate an output for RRCS ARI INITIATED status light capability via the HMI when 2oo4 annunciate votes for RWL2 inputs are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-55	Each division shall generate event data to be retained on the non-SR DCS platform when ARI is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-56	Each division shall provide annunciation for RRCS CHANNEL ACTIVATED via the HMI when 2oo4 annunciate votes for RVP input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-57	Each division shall provide annunciation for RRCS CHANNEL ACTIVATED via the HMI when 2oo4 annunciate votes for RWL2 input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-58	Each division shall provide RRCS TROUBLE status light capability via the HMI when 2oo4 annunciate votes for RVP inputs are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-59	Each division shall provide RRCS TROUBLE status light capability via the HMI when 2oo4 annunciate votes for RWL2 inputs are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-60	Each division shall provide HIGH DOME PRESSURE status light capability via the HMI when 2oo4 annunciate votes for RVP inputs are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-61	Each division shall provide LOW WATER LEVEL 2 TRIP status light capability via the HMI when 2oo4 annunciate votes for RWL2 inputs are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-62	Each division shall initiate an RPT trip when 2oo4 RPT/SLCS votes for RVP sealed in condition are received.	10CFR50.62, IEEE Std. 603/IEEE Std. 7-4.3.2, NEDE-24222	
RRCS-FR-63	Each division shall initiate an RPT trip when 2oo4 RPT votes for RWL2 sealed in condition are received.	10CFR50.62, IEEE Std. 603/IEEE Std. 7-4.3.2, NEDE-24222	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-64	Each division shall provide annunciation for RRCS RECIRC PUMPS TRIP INITIATED status light capability via the HMI when RTP trip is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-65	Each division shall provide outputs to trip two (2) division specific Recirculation Pump breakers (125VDC trip coils) when an RPT trip is initiated.	Reg Guide 1.53, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 379	
RRCS-FR-66	Division 1 shall provide annunciation for RRCS CHANNEL ACTIVATED DIVISION 1 via the HMI when an RPT trip is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-67	Division 2 shall provide annunciation for RRCS CHANNEL ACTIVATED DIVISION 2 via the HMI when an RPT trip is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-68	Each division shall provide RRCS TROUBLE status light capability via the HMI when an RPT trip is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-69	Each division shall generate event data to be retained on the non-SR DCS platform when an RPT trip is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-70	Each division shall initiate SLCS when 2oo4 RPT/SLCS votes for RVP input are received **AND** 2oo4 SLCS votes for RVP input are received **AND** 2oo4 condition votes for CI1 are received **AND** 2oo4 condition votes for CI2 are received.	IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338, IEEE Std. 379 Project design decision	
RRCS-FR-71	Each division shall initiate SLCS when 2oo4 RPT/SLCS votes for RVP input are received **AND** 2oo4 SLCS votes for RWL2 input are received **AND** 2oo4 condition votes for CI1 are received **AND** 2oo4 condition votes for CI2 are received.	IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338, IEEE Std. 379 Project design decision	
RRCS-FR-72	Each division shall initiate SLCS when 2oo4 RPT/SLCS votes for RVP input are received **AND** 2oo4 condition votes for CI1 are received **AND** 2oo4 condition votes for CI2 are received **AND** the 118 sec timer for RRCS manual initiation has expired.	IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338, IEEE Std. 379 Project design decision	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-73	Each division shall initiate SLCS when 2oo4 condition votes for RWL2 input are received **AND** 2oo4 RPT/SLCS votes for RVP input are received **AND** 2oo4 condition votes for CI1 are received **AND** 2oo4 condition votes for CI2 are received.	IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338, IEEE Std. 379 Project design decision	
RRCS-FR-74	Each division shall initiate SLCS when 2oo4 condition votes for RWL2 input are received **AND** 2oo4 SLCS votes for RWL2 input are received **AND** 2oo4 condition votes for CI1 are received **AND** 2oo4 condition votes for CI2 are received.	IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338, IEEE Std. 379 Project design decision	
RRCS-FR-75	Each division shall initiate SLCS when 2oo4 condition votes for RWL2 input are received **AND** 2oo4 condition votes for CI1 are received **AND** 2oo4 condition votes for CI2 are received **AND** the 118 sec timer for RRCS manual initiation has expired.	IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338, IEEE Std. 379 Project design decision	
RRCS-FR-76	Each division shall initiate SLCS when the manual initiation input is sealed in **AND** 2oo4 RPT/SLCS votes for RVP input are received **AND** 2oo4 condition votes for CI1 are received **AND** 2oo4 condition votes for CI2 are received.	IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338, IEEE Std. 379 Project design decision	
RRCS-FR-77	Each division shall initiate SLCS when the manual initiation input is sealed in **AND** 2oo4 SLCS votes for RWL2 input are received **AND** 2oo4 condition votes for CI1 are received **AND** 2oo4 condition votes for CI2 are received.	IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338, IEEE Std. 379 Project design decision	
RRCS-FR-78	Each division shall initiate SLCS when the manual initiation input is sealed in **AND** 2oo4 condition votes for CI1 are received **AND** 2oo4 condition votes for CI2 are received **AND** the 118 sec timer for RRCS manual initiation has expired.	IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338, IEEE Std. 379 Project design decision	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-79	Each division shall provide the capability to manually inhibit SLCS initiation.	Project design decision	The requirement incorporates a project decision that In the undesired event of SLCS being unintentionally initiated, the inhibit switch would provide the Operator with a means to manually inhibit the automatic initiation within the 118 second countdown. This inhibit is provided to minimize maintenance risk while working on the ATWS function.
RRCS-FR-80	If either division is inhibiting SLC initiation, the condition shall be annunciated in the control room.	Project design decision	If the SLCS injection is inhibited, the control room operator must be notified and that notification must remain in view.
RRCS-FR-81	The manual inhibit of the SLCS initiation shall not interrupt the 118 second timer.	Project design decision	
RRCS-FR-82	Division 1 shall provide annunciation for RRCS POTENTIAL ATWS DIVISION 1 via the HMI when 2oo4 annunciate votes for RVP condition sealed in are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-83	Division 1 shall provide annunciation for RRCS POTENTIAL ATWS DIVISION 1 via the HMI when 2oo4 annunciate votes for RWL2 condition sealed in are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-84	Division 1 shall provide annunciation for RRCS POTENTIAL ATWS DIVISION 1 via the HMI when the manual initiation input is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-85	Division 2 shall provide annunciation for RRCS POTENTIAL ATWS DIVISION 2 via the HMI when 2oo4 annunciate votes for RVP condition sealed in are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-86	Division 2 shall provide annunciation for RRCS POTENTIAL ATWS DIVISION 2 via the HMI when 2oo4 annunciate votes for RWL2 condition sealed in are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-87	Division 2 shall provide annunciation for RRCS POTENTIAL ATWS DIVISION 2 via the HMI when the manual initiation input is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-88	Each division shall provide RRCS POTENTIAL ATWS status light capability via the HMI when 2oo4 annunciate votes for RVP condition sealed in are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-89	Each division shall provide RRCS POTENTIAL ATWS status light capability via the HMI when 2oo4 annunciate votes for RWL2 condition sealed in are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-90	Each division shall provide RRCS POTENTIAL ATWS status light capability via the HMI when the manual initiation input is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-91	Each division shall generate event data to be retained on the non-SR DCS platform when 2oo4 annunciate votes for RVP condition sealed in are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-92	Each division shall provide all input data, bypass status, timer values, and voter status to the DCS on a periodic basis, with the period to be established in detailed design.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-93	Each division shall generate event data to be retained on the non-SR DCS platform when the 118 second timer is started when 2oo4 annunciate votes for RVP condition sealed in are received		
RRCS-FR-94	Each division shall provide a displayed 118 second timer countdown via the HMI when 2oo4 annunciate votes for RVP condition sealed in are received.	New project design feature	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-95	Each division shall generate event data to be retained on the non-SR DCS platform when 2oo4 annunciate votes for RWL2 condition sealed in are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-96	Each division shall generate event data to be retained on the non-SR DCS platform to indicate that the 118 second timer is started when 2oo4 annunciate votes for RWL2 condition sealed in are received	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-97	Each division shall provide a displayed 118 second timer countdown via the HMI when 2oo4 annunciate votes for RWL2 condition sealed in are received.	New project design feature	
RRCS-FR-98	Each division shall generate event data to be retained on the non-SR DCS platform when the manual initiation input is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-99	Each division shall generate event data to be retained on the non-SR DCS platform to indicate that the 118 second timer is started when the manual initiation input is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-100	Each division shall provide a displayed 118 second timer countdown via the HMI when the manual initiation input is sealed in.	New project design feature	
RRCS-FR-101	Each division shall initiate a 10 minute timer when the 118 second timer for the RRCS manual initiation expires.	Original design feature	
RRCS-FR-102	Each division shall initiate a 10 minute timer when 2oo4 reset votes for RVP input are received.	Original design feature, Project design approach	
RRCS-FR-103	Each division shall initiate a 10 minute timer when 2oo4 reset votes for RWL2 input are received.	Original design feature, Project design approach	
RRCS-FR-104	Each division shall provide the capability to reset RRCS when the 10 minute timer expires.	Original design feature	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-105	Each division shall provide three (3) output drivers to energize 120VAC control circuits and 120VAC firing circuits for each SLCS pump / squib valve pair when SLCS is manually initiated.	10CFR50.62, IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-106	Division 1 shall provide a 120VAC output driver to close RWCU inboard valve G31-F001 when SLCS is manually initiated.	10CFR50.62, IEEE Std. 603/IEEE Std. 7-4.3.2, NEDE-24222	
RRCS-FR-107	Division 2 shall provide a 120VAC output driver to close RWCU outboard valve G31-F004 when SLCS is manually initiated.	10CFR50.62, IEEE Std. 603/IEEE Std. 7-4.3.2, NEDE-24222	
RRCS-FR-108	Each division shall provide annunciation for RRCS CHANNEL ACTIVATED via the HMI when SLCS is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-109	Each division shall provide RRCS TROUBLE status light capability via the HMI when SLCS is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-110	Each division shall provide annunciation for RRCS CONFIRMED ATWS via the HMI when SLCS is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-111	Each division shall provide RRCS CONFIRMED ATWS status light capability via the HMI when SLCS is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-112	Each division shall generate event data to be retained on the non-SR DCS platform when SLCS is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-113	Each division shall provide annunciation for RRCS RWCU ISOLATION INITIATED status light capability via the HMI when SLCS is initiated.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-114	Each division shall provide annunciation for SLCS STORAGE TANK LO-LO-LEVEL PUMP TRIP INITIATED via the HMI when 2oo4 annunciate votes for STL input are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-115	Each division shall provide SLCS STORAGE TANK LO-LO LEVEL status light capability via the HMI when 2oo4 annunciate votes for STL inputs are received.	IEEE Std. 603/IEEE Std. 7-4.3.2	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-116	Each division shall provide an output to trip the 120VAC pump control logic when 2oo4 condition votes for STL input are received.	Original design feature	
RRCS-FR-117	Each division shall provide annunciation for RRCS CHANNEL ACTIVATED via the HMI when the first distinct action for the RRCS manual initiation has been executed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-118	Each division shall provide RRCS TROUBLE status light capability via the HMI when the first distinct action for the RRCS manual initiation has been executed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-119	Each division shall provide RRCS MANUAL INITIATION ARMED status light capability via the HMI when the first distinct action for the RRCS manual initiation has been executed.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-120	Each division shall provide annunciation for RRCS MANUAL INITIATION via the HMI when the RRCS manual initiation input is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-121	Each division shall provide annunciation for RRCS CHANNEL ACTIVATED via the HMI when the RRCS manual initiation input is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-122	Each division shall generate event data to be retained on the non-SR DCS platform when the RRCS manual initiation input is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-123	Each division shall provide RRCS TROUBLE status light capability via the HMI when the RRCS manual initiation input is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-124	Each division shall provide RRCS MANUAL INITIATION status light capability via the HMI when the RRCS manual initiation input is sealed in.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-125	Each division shall provide the capability for ARI manual reset.	IEEE Std. 603/IEEE Std. 7-4.3.2	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-126	The ARI manual reset shall reset the ARI initiating logic provided that RVP and RWL2 no longer exceed setpoint **AND** the 30 second timer has expired.	Original design feature	
RRCS-FR-127	Each division shall provide annunciation for RRCS ARI READY FOR RESET status light capability via the HMI when 0oo4 condition votes for RVP input **AND** 0oo4 condition votes for RWL2 input are received **AND** the 30 second timer has expired.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-128	Each division shall provide annunciation for RRCS READY FOR RESET status light capability via the HMI when 0oo4 condition votes for RVP input are received **AND** 0oo4 condition inputs for RWL2 input are received **AND** the 10 minute timer has expired.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-129	Each division shall provide the capability for RRCS manual reset.	Original design feature	
RRCS-FR-130	The RRCS Manual Reset shall reset the RRCS initiating logic, including the seal in, provided that 0oo4 condition votes for RVP input are received **AND** 0oo4 condition votes for RWL2 input are received **AND** the 10 minute timer has expired.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-131	The RRCS Manual Reset shall also reset the latching logic for: • RPT Beaker Trip • SLCS pump and valve initiation • RWCU isolation	IEEE Std. 603/IEEE Std. 7-4.3.2	This reset only resets the initiation logic and does not terminate SLCS pump operation or open the RWCU isolation valves.
RRCS-FR-132	Each division shall provide annunciation for RRCS OUT OF SERVICE via the HMI when any loss of power or self-test issue is identified.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-133	Each division shall provide RRCS TEST FAULT status light capability via the HMI when a self-test issue is identified.	IEEE Std. 603/IEEE Std. 7-4.3.2	
RRCS-FR-134	Each division shall provide RRCS LOSS OF DC POWER status light capability via the HMI when a loss of power condition is identified.	IEEE Std. 603/IEEE Std. 7-4.3.2	

DCS/RRCS FUNCTIONAL REQUIREMENTS			
ID #	**DCS/RRCS Requirement**	**DCS/RRCS Source / Basis**	**Notes / Clarification**
RRCS-FR-135	The DCS/RRCS shall be capable of supporting tests (manual and self) to verify proper operation of each channel during plant operation without affecting the ability of DCS/RRCS to perform its protective function.	Reg Guide 1.22, Reg Guide 1.118, IEEE Std. 603/IEEE Std. 7-4.3.2, IEEE Std. 338	

B

B.1 NSR Platform Requirements

Requirement #	DCS Requirement	Source / Basis
	FUNCTIONAL REQUIREMENTS	
	Safety Classification	
DCS1	The platform and supporting components shall be non-safety related augmented quality.	10CFR50.62
DCS2	The application software for the DAS portions of the platform shall comply with 10 CFR 50.62	10CFR50.62
	Platform Architecture	
DCS3	The non-safety related components of the DCS shall include the control and protection logic, the I/O interfaces, and the HMI displays providing control and indication.	Project requirement
DCS4	The DCS shall be capable of simultaneously performing the operational functionality (control and protection logic) of multiple non-safety related systems.	Project requirement
DCS5	The DAS shall be implemented in segmented portions of the DCS. The DAS shall be implemented as augmented software quality, in portions of the DCS that are segmented from the rest of the DCS.	Project requirement
DCS6	The DAS shall interface with safety signals and the safety systems through Equipment Interface Modules (EIMs) which provide the required priority logic as required in DI&C-ISG-04 as well as the non-safety to safety related isolation functions.	Project requirement, DI&C-ISG-04
DCS7	The control and protection logic functionality to implement the Anticipated Transient Without Scram (formerly implemented in the deleted Redundant Reactor Shutdown System, RRCS) shall be included in the DAS that is implemented in the DCS.	Project requirement
DCS8	The ECCS and N4S control and protection logic functionality required by the Defense-in-Depth and Diversity Analysis shall be included in the DAS portions of the DCS.	Project requirement

Requirement #	DCS Requirement	Source / Basis
DCS9	The DCS design shall have inherent redundancy to assure reliability and availability of the control and monitoring functionality (e.g., controllers, power supplies, communication modules, networks)	Project requirement
DCS10	The DAS portions of the DCS shall be capable of performing the same voting logic used within the safety functions, including two-out-of-four (2oo4), one-out-of-three (1oo3), one-out-of-two (1oo2), and one-out-of-one (1oo1).	Project requirement
DCS11	The DAS portions of the DCS shall be capable of implementing the same voting logic adjustments to deal with bypass / inoperable conditions within a channel. This requires a 2oo4 to gracefully degrade to two-out-of-three (2oo3) and then 2oo3 to gracefully degrade to 1oo2.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
DCS12	If the placement of a channel in bypass would compromise the minimum acceptable voting scheme, the DAS shall reject the bypass request and convey this to the operator via the HMI.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2 One failed channel can be bypassed. Additional failed channels are marked as voting to actuate.
DCS13	If the minimum acceptable voting scheme cannot be achieved with the available channels, the DAS shall notify the operator so that a manual action can be implemented.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
DCS14	The DAS shall interface with the safety related EIM through non-safety related ports. The EIM is part of the safety system. The EIM includes priority logic to assure protection functions override any active control functions.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
DCS15	None of the DAS logic shall be encoded as negative logic (i.e., active low). The digital representation of input and output data shall be in positive logic to the maximum extent practical.	Eliminate design and verification and validation (V&V) mistakes common to negative logic.
DCS16	Functions within the DCS shall be segmented such that faults and failures will in no way compromise DAS functional channel/division independence or DCS control segment independence.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
DCS17	The DCS shall be readily testable and maintainable online or offline.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2

Requirement #	DCS Requirement	Source / Basis
DCS18	The ability shall exist within the DCS to replace any single failed component online (i.e., hot swap) without impeding the ability of the system to initiate a protective function or inadvertently causing the initiation of the protective function.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
DCS19	The DCS shall be designed such that it does not suffer any degradation in performance, processing speed, memory allocation, etc. under abnormal operating conditions or high loading.	Improved fault tolerance and good engineering practice.
DCS20	Performance diagnostics, such as processor loading, power supply status, network loading, etc. shall be viewable from a dedicated Engineering Workstation (EWS).	Project requirement
DCS21	All software shall be designed and documented with sufficient modularity to minimize the time and complexity involved in making a change to any program.	NUREG/CR-6463
DCS22	Communication among programs for data or program control shall be symbolic rather than absolute so a given program is essentially an independent unit.	NUREG/CR-6463
DCS23	Changes required in one program necessitated by changes in another shall be minimal and through established and controlled interfaces.	NUREG/CR-6463
DCS24	Processor and device state software shall identify the operating condition of each function processor and peripheral device within the DCS.	Project requirement, IEEE Std. 603/IEEE Std. 7-4.3.2
DCS25	Floating point math computations shall be supported in hardware.	NUREG/CR-6463
DCS26	The design shall ensure that divide-by-zero and similar out-of-bounds errors are not possible.	NUREG/CR-6463
DCS27	If floating point calculations are performed, error handling shall include detection and appropriate handling of floating point not a number (NAN).	NUREG/CR-6463

Requirement #	DCS Requirement	Source / Basis
DCS28	Software modules shall have inherent features to validate data received for use from other modules within the system, from any external data links, and from Operators and technicians.	NUREG/CR-6463
DCS29	Detected faults and failures shall be reported as health error messages and saved to a health error log.	Project requirement
DCS30	The DCS shall be capable of receiving health error messages from the PPS (SR platform) and saving these to an error log.	Project requirement
DCS31	The DCS shall time stamp health messages from the PPS upon receipt.	Project requirement
DCS32	Vendor shall provide an obsolescence plan for future maintainability of the system, which shall not require wholesale replacement as the means of coping with obsolescence.	Project requirement
DCS33	The DCS shall be capable of providing control function capability.	Project requirement
DCS34	The DCS shall be capable of performing various operations on input signals (e.g., conditioning, summing, averaging, square root conversion).	Project requirement
DCS35	No setpoint, derived setpoint, or tolerance shall be hardcoded within the DCS.	Project requirement
DCS36	All bi-stable functions shall include hysteresis on reset.	Project requirement
DCS37	Hysteresis for each bi-stable shall use a user-settable, user-controlled constant.	Project requirement
DCS38	Each constant value to which an engineering unit input is compared shall be a user-settable controlled constant.	Project requirement
DCS39	The application software shall prevent the hysteresis value from being set in the domain where the bi-stable function outside has exceeded the action point.	Project requirement

Requirement #	DCS Requirement	Source / Basis
	System I/O	
	Note - Specific I/O for each of the DCS functions can be derived from the individual functional requirements provided separately. Entries included below provide additional DCS capabilities that warrant identification for each function.	
DCS40	The DCS shall utilize fault tolerant I/O interfaces (modules / cards)	Project requirement
DCS41	The DAS input interfaces shall be compatible with standard analog signals inputs as well as those from smart transmitters (e.g., HART).	Project requirement
DCS42	The DAS shall input analog data from the qualified isolators in the SR inputs that provide data to the ATWS function	Project requirement
DCS43	The DAS shall support maintenance bypass inputs (vendor shall describe extent of bypass capability within the design and demonstrate single failure tolerance)	Project requirement
DCS44	All DAS discrete outputs shall be diagnosed and single failure tolerant.	Project requirement
DCS45	If the DAS functions include HPCI or RCIC, then SR means shall be provided to arbitrate between the HPCI and the RCIC analog speed demand outputs from the PPS and the DAS functions.	Project requirement
	Independence, Separation and Segmentation	
DCS46	DCS operation shall be accomplished independent of any other digital system interfaces with the exception of DKT functionality.	Ensures that the DCS operates independent of any other system (e.g., the SR PPS).
DCS47	Use of digital communications in the DCS shall in no way compromise DAS functional channel/division independence or DCS control segment independence.	Any failure or improper configuration in the DCS digital communications/DKTs that adversely effects channel/division independence or control segment independence could place the plant in a state (a Common Cause Failure) not addressed in the UFSAR Chapter 15 Safety Analysis.
DCS48	Redundancy (separate channels/divisions of equipment) shall be provided for DCS protective functions.	IEEE Std. 603/IEEE Std. 7-4.3.2

Requirement #	DCS Requirement	Source / Basis
DCS49	DAS channels shall be functionally independent.	Communication independence as described in DI&C-ISG-04.
DCS50	DAS divisions shall be functionally independent.	Communication independence as described in DI&C-ISG-04.
DCS51	The DAS shall be fed with isolated copies of the same sensors in the PPS. The isolators are provided with and considered part of the safety related PPS.	Sharing sensors for multiple control and protection functions within the same channel/division reduces the numbers of sensors that must be installed and maintained, and the corresponding input modules and cabling without compromising independence.
DCS52	The isolated DAS values shall be compared to each other as well as to the data provided by the PPS, to perform the equivalent channel checks on the DAS data as on the PPS data and validate that the PPS and DAS functions are estimating sufficiently similar plant status.	The isolated DAS inputs shall be diagnosed for correct operation just like the PPS field inputs. Differences are annunciated for troubleshooting a repair.
DCS53	The non-safety related isolated output of the isolators shall be hardwired to the DAS inputs.	Project requirement
DCS54	The DAS bi-stable, timing, and logic functions shall be implemented in software.	Project requirement
DCS55	The DAS functions within the DCS shall be segmented from other DCS functions and shall be appropriately segmented from each other.	Project requirement
DCS56	DCS control function physical and/or logical segmentation capability shall be provided for inputs/outputs and their related control processor(s).	Segmentation of control functions is either expressly described or implied in the UFSAR. The functional segmentation described in the nuclear plant's UFSAR is to be maintained to minimize licensing cost/risk unless there is an overriding functional/financial benefit to alter the segmentation schema. This segmentation addresses functionality not already segmented in individual channels/divisions.
DCS57	Where possible, field inputs and outputs within a segment of the DCS shall be consolidated.	Supports the requirement to minimize the number of unique field replaceable units (FRUs). Reduces acquisition and lifecycle support costs without compromising the segmentation concept.

Requirement #	DCS Requirement	Source / Basis
DCS58	Consolidation shall not create new malfunctions or malfunction with a different result for the function.	Supports the requirement to minimize the number of unique FRUs. Reduces acquisition and lifecycle support costs without compromising the segmentation concept.
DCS59	All DAS protection processes shall be executed continuously on a cyclical, non-varying basis.	Ensures bounded, deterministic performance over varying plant conditions, unaffected by the likely maximum and minimum propagation delays through the channels and divisions.
DCS60	All DCS processes shall be executed continuously on a cyclical, non-varying basis.	Ensures bounded, deterministic performance over varying plant conditions, unaffected by the likely maximum and minimum propagation delays through the control functions.
DCS61	The DAS shall be capable of initiating the protective function within the required response time of receiving a valid protective signal. This shall account for scan times, processing times and communication times for the logic as part of the control throughput so that maximum protection system response is not affected.	Response time as determined by design and licensing basis.
DCS62	DCS control segments shall be digitally connected to enable features such as system wide data aggregation, capture, and use of DKTs for monitoring and control.	Data aggregation and capture directly reduces operator workload. It also allows for analysis to improve plant operational performance and to detect maintenance issues.
DCS63	No failure in one DCS control segment shall propagate to another control segment.	Ensures that no new failure is introduced into the DCS design that has not been evaluated in the safety analysis.
DCS64	The DCS shall be expandable by the addition of future segments without impacting the performance of other segments or the performance of other channels/divisions.	Allows for the future expansion to support consolidation of plant I&C functions to the DCS Platform.
DCS65	The number of unique DCS and network FRUs shall be minimized	Reduce acquisition cost, reduce lifecycle support costs.
DCS66	No single failure of a FRU shall cause spurious actuation or prevent a necessary commanded actuation from occurring unless allowed by the clarification below.	IEEE Std. 603/IEEE Std. 7-4.3.2

Requirement #	DCS Requirement	Source / Basis
DCS67	Clarification - If it can be shown that through a combination of DCS attributes that address the (1) the possibility of spurious actuation or (2) prevention of a necessary commanded actuation AND/OR (3) segmentation that establishes the single failure is sufficiently unlikely or can be tolerated within the bounds of the safety analysis, then implementation of the requirement above shall not be required.	This is consistent with the design bases for single function/loop control in legacy implementations. Allowing this exception promotes reducing control system complexity/unnecessary redundancy. This translates into reduced acquisition costs and reduced lifecycle support costs.
DCS68	Individual FRUs shall be removable/replaceable ("hot-swap") with the DCS online without causing spurious actuation or preventing a necessary commanded actuation from occurring.	Facilitate repair/replacement without affecting operation.
DCS69	Where individual DCS FRUs require testing, calibration, or other configuration changes with the control system online, the DCS shall retain its capability to perform its functions while these activities are being performed on the subject FRU.	IEEE Std. 603/IEEE Std. 7-4.3.2 clause 5.7 – support for testing and calibration.
DCS70	DCS testing shall be restricted to one component or channel at a time.	Project requirement
	Health Monitoring	
DCS71	The DCS shall be capable of self-monitoring, self-diagnostics, fault detection, and alarming any abnormalities within itself.	Improved fault tolerance and good engineering practice.
DCS72	Active equipment health monitoring shall be performed down to the FRU level.	Active health monitoring continuously demonstrates FRU operability and minimizes/eliminates the need for surveillance testing.
DCS73	Detected equipment faults shall be self-announcing and identify the affected FRU.	Eliminate need for performing surveillance tests, eliminate need for troubleshooting, and reduce workload.
DCS74	The DCS shall be capable of performing self-tests and online diagnostics to identify and isolate failures of I/O cards, busses, power supplies, controllers, communications paths, etc.	These features shall identify the presence of all faults, and determine the location of failure(s) to replaceable module level(s).
DCS75	The DCS shall provide indication when the DCS self-test functions are operating (e.g., counter, heartbeat).	Project requirement

Requirement #	DCS Requirement	Source / Basis
DCS76	The DCS shall employ watchdog timers to detect faults and failures within the system.	Project requirement
DCS77	Watchdog timers shall be independent of the processing CPU.	Project requirement
DCS78	The DCS shall continuously validate and compare the values of sensors measuring the same process variable and alarm if the deviation between signals exceeds a preset limit or if signals are trending toward a trip setpoint.	Project requirement
DCS79	The DCS shall include diagnostics to detect a logic related failure within an individual segment.	Project requirement
DCS80	The diagnostic features provided shall include all the necessary indications and alarms to allow an Operator to take corrective or alternative actions.	Project requirement
DCS81	Online and offline diagnostics shall be provided to check and verify the operation of the hardware, firmware, software, and programmable logic.	Project requirement
DCS82	Online system health monitoring shall be provided for verifying the health status of system components to support software and hardware maintenance activities.	Project requirement
DCS83	The on-line diagnostics shall be sufficient to allow reduction of related Technical Specification Surveillance Tests, such as logic system functional tests.	Project requirement
	Surveillance Testing	
DCS84	When surveillance testing is required to demonstrate a DAS function is operable, the DCS design shall automate the surveillance to the maximum extent practicable.	Reduce operator workload.

Requirement #	DCS Requirement	Source / Basis
DCS85	For redundant DAS functions where multiple instances of the function are required to actuate plant response (e.g., a plant trip or a turbine trip), surveillance testing shall be able to fully test a single instance of that function without initiating an actuation. This includes actuation of individual physical components configured in a coincidence configuration, such as testing a single actuator located in single train in a two-out-of-two (2oo2) train configuration where each train is 1oo2, or actuating a suction isolation valve to a pump without actuating the pump or the output isolation valve for that pump.	Enable maximum surveillance testing while not impacting plant operation. This is also consistent with design attribute of minimizing single point vulnerabilities. Reduction in cost/workload to perform surveillance testing.
DCS86	The DAS shall include knife disconnects for any terminations associated with analog and discrete inputs and with analog outputs to support testing including calibration.	Project requirement
DCS87	The DAS design shall minimize the surveillance test requirements.	Project requirement
DCS88	The DAS design shall support the automation of surveillance testing by allowing the capability for inter-channel checks that produce necessary data outputs for validation.	Project requirement
DCS89	The DCS shall provide the capability to automate the performance of valve strokes (for non-squib valves) and timing.	Project requirement
	Communication	
DCS90	The DAS shall be logically implemented differently than the PPS. Channels are functions, divisions are functions, and the channels provide data to divisions through the normal DCS use of global variables and the DCS network.	There is no known requirement to duplicate the PPS architecture in the DAS. Using the same logical structure decreases the design costs for the DAS, keeping the same functional channels and functional divisions using the same voting schemes as the PPS.
DCS91	All serial data communication shall implement the guidance of DI&C-ISG-04 for Interdivisional Communication.	DI&C-ISG-04

Requirement #	DCS Requirement	Source / Basis
DCS92	Bi-directional divisional communication shall exist between the DCS platform and the DKT to allow for control, operator trending (as required), grouping, and alarming in the control room or other operational areas.	This supports real-time operation of the plant and immediate/short term operator action.
DCS93	One way data communication shall exist from the PPS to the DCS and shall include PPS data associated with: Sequence of Events (SOE) All Engineering unit data All discrete status All votes to trip or actuate Channel Checks Historian / Analytics Display Platform diagnostics	Project requirement
DCS94	The DAS function shall not make use of any of the data provided to fulfill Requirement DCS91.	Diversity requirement
DCS95	The DCS shall utilize a suitable protocol that does not require handshaking. Thus, internet protocols such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and File Transport Protocol (FTP) are unacceptable for transport of data from the PPS to the DCS.	Project requirement
DCS96	The signal response from soft control selection on the HMI, through the DCS and back for indication (data latency) shall not exceed 0.25 second.	Project requirement
DCS97	All data messages shall be designed with a fixed format and shall comply with formatting requirements.	Project requirement

Requirement #	DCS Requirement	Source / Basis
	Human-Machine Interfaces	
DCS98	The primary HMIs for the platform shall consist of multiple DKTs that provide access to channel, division, and segment data and offer the capability for touch screen (soft) controls.	Promotes the design objective for a DKT driven end-state control room. This provides for a more compact control room design, reduces equipment and corresponding maintenance costs.
DCS99	The HMI functionality shall be capable of replacing existing hand switch / indicating light configurations via soft controls.	Project requirement
DCS100	A sufficient number of DKTs shall be provided to support the DAS plus two for continuous data display of Bypassed Information and Status Information (BISI).	Project requirement
DCS101	Any DCS DKT shall be configured for any potential use.	Project requirement
DCS102	The configuration of the DCS DKTs at the Senior Reactor Operator's workstation shall only allow the Reactor Operator (RO) to perform commanded actions. Locations that are not in the normal RO work area are not allowed to issue soft commands. Specifically, this restriction includes the Senior Reactor Operator (SRO) workstations which cannot issue soft commands that control safety functions.	The SRO is not allowed to be "at the controls" thus the DKTs assigned to the SRO shall not support soft controls, other than navigation.
DCS103	The DCS HMIs shall be capable of making the following DCS and PPS data available for display and NSR control: Sequence of Events All Engineering unit data All discrete status All votes to trip or actuate Channel Checks Historian / Analytics Platform diagnostics	Project requirement

Requirement #	DCS Requirement	Source / Basis
DCS104	An EWS shall be provided to facilitate system health monitoring and surveillance testing.	This facilitates system support by plant operators and qualified I&C technicians outside of the control room, reducing control room workload. This, in conjunction with other health monitoring/surveillance testing requirements, reduces I&C maintenance technician workload.
DCS105	An EWS shall be provided for configuration management. The EWS should be common to the entire DCS.	Project requirement
DCS106	The EWS shall not be connected to more than one channel or one division at any time.	Project requirement
DCS107	The EWS shall be at least password protected and shall offer multiple levels of password protected functionality (e.g., view configuration and show data within the program versus change setpoint values versus change the program).	Project requirement
DCS108	The EWS shall not be capable of initiating, terminating, or bypassing safety functions.	Project requirement
DCS109	The EWS shall be capable of displaying data in any DCS equipment.	Project requirement
DCS110	The EWS shall include fully integrated local storage devices to support DCS backup and restore.	Project requirement Backup must be possible on bulk storage devices and copies of these backups must be able to be removed from the system.
DCS111	EWS and DCS real time diagnostic/maintenance utilities shall include the following: System Performance Analysis, Status of PPS and DCS communication links, System Health Displays, Workstation Activity Monitor, and Program Execution Timing and Scheduling	Project requirement
DCS112	The EWS shall be installed in the Auxiliary Equipment Room (AER) and shall provide password protection to preclude malicious use.	Project requirement

Requirement #	DCS Requirement	Source / Basis
DCS113	The DKT shall be powered from the same uninterruptable power as the DCS which is supplied from multiple sources so the loss of a single power source does not result in the loss of multiple DKTs.	Project requirement
DCS114	If a DKT fails, another DKT shall be capable of the same functionality and operation shall be maintained without any functional or operational deterioration.	Project requirement
DCS115	DKT shall support keyboard and mouse inputs in addition to more advanced methods such as touch-screen inputs.	Project requirement
DCS116	All control actions initiated from a HMI shall propagate through the system such that control system signals sent to final plant control elements appear at the control system output interface connected to the associated plant control elements at an established, bounded rate that does not inhibit operator performance or timely operator control actions.	Ensures bounded, repeatable performance over varying plant conditions. This also enables the use of single point plant interfaces to the DCS vs using hardwired controls.
DCS117	No single point of failure within the DKT component and communication design shall disable other / all DKTs in the Main Control Room.	IEEE Std. 603/IEEE Std. 7-4.3.2
DCS118	DCS DKTs shall be switchable so that they can also provide HMI functionality to other connected systems.	Promotes the design objective for a DKT driven end-state control room. This provides for a more compact control room design, reduces equipment and corresponding maintenance costs.
DCS119	DCS DKTs shall be switchable so that they can also provide HMI functionality for the DAS channels and divisions. This switchable feature shall in no way compromise the independent function of the PPS.	IEEE Std. 603/IEEE Std. 7-4.3.2
DCS120	Only one system (PPS or DCS) shall be accessed by the DKT at a time. This switchable feature shall in no way compromise the independent function of the PPS, DAS function within the DCS, or the DCS as a whole.	IEEE Std. 603/IEEE Std. 7-4.3.2

Requirement #	DCS Requirement	Source / Basis
DCS121	No plant control logic of any kind shall be resident within that portion of the DCS architecture that supports DKT functionality and DKT functional switching.	The portion of DCS architecture is only intended to provide Keyboard/Video/Mouse capability for DCS. This is to support to support the DKT driven end-state control room concept. The plant control functions of DKT connected systems are fully contained within those connected system. DKT functionality only provides an HMI interface for the selected system.
DCS122	The DCS HMI design, including DKTs, shall be expandable without impacting the performance of other HMI or the performance of the related channels/divisions functionality. (Vendor to provide a maximum count of DKTs that can be supported.)	Project requirement
DCS123	Documentation of HMI design and communication compliance with DI&C-ISG-04 shall be provided.	DI&C-ISG-04
DCS124	For eventual use, the DCS HMI shall provide the functionality of a typical control room annunciator.	Project requirement
DCS125	The DCS HMI shall include an events page that tracks all alarms.	Project requirement
DCS126	The DCS shall have the capability to support future alarm management, alarm suppression, alarm prioritization, and other modern alarm management schemes and displays.	While not part of this project, eventually alarm management will be provided to reduce and rationalize alarming in the control room.
DCS127	The vendor shall provide a base HFE guide / template for evaluation.	Project requirement
DCS128	Non-DKT operating interface devices (e.g., switches/pushbuttons) that provide digital inputs to the DCS shall only be provided to meet specific regulatory or operational commitments to provide such a feature.	This provides for a more compact control room design, reduces equipment and corresponding maintenance costs. This also provides increased redundancy in that functions not tied to switches can be manipulated from displays presented on multiple DKTs.

Requirement #	DCS Requirement	Source / Basis
DCS129	Non-DKT Operator interface devices (e.g., switches/pushbuttons) that are connected electrically to plant actuated devices (either directly or through a control relay) shall only be employed when required to meet a specific regulatory requirement or commitment to provide such a feature. The few remaining switches and pushbuttons shall be monitored by the DCS and appropriate action taken. All other devices implemented through application logic in the DCS.	Excessive, direct, point-to-point wiring of switches and pushbutton actuators is expensive and inefficient from a human factors perspective. Use of these devices is limited to only the most critical actuation functions. IEEE Std. 603/IEEE Std. 7-4.3.2
DCS130	The existing manual controls for the RRCS shall be retained.	
DCS131	Other than the ATWS function, all DAS functions shall be operated solely by soft controls and by automation within the DAS.	Project requirement
DCS132	Non-DKT parameter displays are not in vendor scope and shall not be driven by the DCS.	Project requirement
DCS133	The DCS HMI shall have interactive displays that automatically pull up procedures, notes, or actions to mitigate the identified issues and convey what actions the system is currently taking.	Project requirement
DCS134	The DCS shall be capable of assembling PPS system data and transmitting that data to the DCS in a format that supports plant needs (e.g., current Operator daily rounds, Reactor Engineering Analysis, heat balances, etc.)	Reduces time required to complete these efforts
DCS135	In the future, the DCS shall be capable of providing data to other systems that automatically generate work packages and schedule work.	Project requirement
DCS136	The DCS HMI shall be capable of logging commands for purposes of data retention and troubleshooting.	Project requirement
DCS137	The DCS HMI shall provide the capability to automate valve lineups to support initiation and restoration operational scenarios.	Project requirement

Requirement #	DCS Requirement	Source / Basis
	Displays, Keyboards, and Trackballs	
DCS138	The DCS DKTs shall be supported by a color, full graphics package that supports: (A) Full color (256 colors at a minimum) (B) Mimic displays of plant systems (e.g., one-line diagrams of plant fluid systems) (C) Logic displays of implemented control logic (D) The ability to depict dynamic graphical objects (e.g., tanks, valves, pumps, logic devices, etc.) that show information as to state (e.g., tank level, valve position, pump running status, logic states, etc.) (E) The ability to control plant processes and equipment through graphical control objects	Provides improved, graphical HMI interface to improve operator performance. Promotes the design objective for a DKT driven end-state control room. This provides for a more compact control room design, reduces equipment and corresponding maintenance costs.
DCS139	The HMI displays shall have a 16:9 aspect ratio regardless of size.	Project requirement
DCS140	The HMI displays shall utilize a pixel geometry resolution of at least 1600 x 900.	The 1600 x 900 pixel resolution also is compatible with most current desktop and wide screen laptops.
DCS141	The DKT shall be capable of displaying any data that is provided from the DCS platform as well as the PPS.	Project requirement
DCS142	The DKT shall be capable of providing an on-screen “logic diagram” which shows state of logic and process values	Project requirement
DCS143	A minimum of 30 pre-configured DAS and DCS graphics shall be provided (mix of low/medium/high complexity)	Project requirement
DCS144	DKT shall support at least 20 additional custom graphics.	Project requirement
DCS145	The Purchaser shall be provided with the tools and instructions necessary to modify or augment the graphics.	NUREG-0711
DCS146	The DKT display convention shall comply with a display style guide (to be developed and provided by Purchaser)	NUREG-0711

Requirement #	DCS Requirement	Source / Basis
DCS147	The HMI display shall include at least one (1) alarm page to display system alarm messages. Alarms should be designated accordingly. Operator command for Acknowledge shall be provided. Alarms shall indicate the date, time, description, state of alarm and if it has been acknowledged. The alarm shall clear when the condition clears or when the Operator has acknowledged the alarm.	NUREG-0711
DCS148	The Operator interactions via the DKT display screen shall be confirmed as "received" by the DKT within the refresh rate.	NUREG-0700, Section 7.3.9-1 (Display screen sensitivity and response)
DCS149	The time to call up any DKT display shall not exceed two (2) seconds under peak loading conditions, which does not require double touch.	NUREG-0700, Section 2.4.3-1 for Response Time Appropriate to Transaction, typical response time for a next page request should be within 0.5 to 1.0 seconds.
DCS150	All HMI displays shall be updated (refreshed) with system data at a rate not greater than once per second so as not to inhibit operator performance.	Ensures bounded, repeatable performance of the HMI over varying plant conditions. NUREG-0700, Section 1.4-1 contains a guideline stating the maximum update rate should be determined by the time required for the user to identify and process the changed features of the display. NUREG-0700, Section 1.4-3 states changing alphanumeric values the user must reliably read should not be updated more than once per second. NUREG-0700, Section 2.4.3-1 states the speed of computer response to user entries should be appropriate to the transaction involved.
DCS151	Touch screen interface shall require double touch action (i.e., separate select and execute touches in disparate screen areas) to initiate a control function.	NUREG-0700, Section 7.3.3-2 Second "touch" provides confirmation that the requested action is indeed intended.

Requirement #	DCS Requirement	Source / Basis
DCS152	The HMI DKT shall be capable of providing soft controls that replicate the functionality provided by existing switches consisting of, but not limited to: 2 position maintained contact Keylock switch – 2 position (administrative control) Keylock switch – 3 position (administrative control) 3 - position spring return to center 3 - position, pull out, spring return to center 3 – position, spring return from stop position	
DCS153	The DKTs shall be configured to comply with Human Factors requirements (e.g., Support peer checking without obscuring the item being peer checked.)	NUREG-0711
DCS154	All HMI shall be designed, implemented, verified, and validated under a Human Factors Engineering program.	NUREG-0711
DCS155	A timeout/reset feature shall be provided for non-executed data entry and commands.	Project requirement
DCS156	A system “Heart Beat” shall be on the HMI display to indicate the display generator is active and not in a frozen or locked state (which shall not be by display of the local time).	Project requirement
DCS157	The heartbeat shall be based on an artifact in the logic solver, which shall demonstrate that the DKT is communicating with the logic solver.	Project requirement
DCS158	To reduce the possibility of data entry errors, the HMI shall provide the capability to use an on-screen numeric keypad in addition to the keyboard, permitting the Operators to keep their view on the display.	Project requirement
DCS159	The DKT displays shall have the capabilities for graphical trending, tabular trending, multiple window display, sizable/scalable windows, animated graphics, historical data retrieval, first out alarm logic, and alarm displays with prioritization and history.	Project requirement

Requirement #	DCS Requirement	Source / Basis
DCS160	The HMI shall provide the DAS with the capability to bypass or trip an individual sensor, a logic channel, or the trip system.	Project requirement
	Data Historian, Sequence of Events, Data Transmission	
DCS161	Data time stamping shall be provided for all DCS related data including all data received from the PPS.	Establishing system time allows for automatic data time stamping of DCS and PPS sensor inputs, control logic actuations, outputs to actuators, and correlation of data for future analysis.
DCS162	The date and time provided shall be used to synchronize all DCS elements with the common provided external time source.	Data time stamping is provided only to support logging and external, correlation of DCS and PPS data. No PPS monitoring or control function shall use system time. Incorrect or missing system time only impacts the data time stamping function.
DCS163	DCS date and time shall be synchronized to an external reference standard (e.g., GPS time) with a minimum accuracy of 1 millisecond.	Promotes data correlation and analysis, which reduced workload.
DCS164	System time should minimize the drift when disconnected from the reference standard.	This ensures that data time stamping correlation is available if connection to the reference standard is compromised.
DCS165	The System shall support re-synchronization to the time source with reconnected, with minimal disruption to data.	This ensures that data time stamping correlation is available if connection to the reference standard is compromised.
DCS166	The date and time shall be maintained in Coordinated Universal Time (UTC), to avoid issues with transitions into and out of Daylight Savings Time (DST).	This ensures that data time stamping correlation is available if connection to the reference standard is compromised.
DCS167	All sensor data, discrete manual control signals, discrete automatic control signals, and safety equipment system health data shall all be time stamped when read by the DCS and be presented with its time stamp for archiving/analysis with 1 millisecond resolution.	This data is used for post-event analysis, plant optimization, DCS and PPS troubleshooting, reducing workload, and improving plant efficiency. This resolution is required to support the fidelity used in the nuclear industry for SOE.
DCS168	SOE input data capture capability shall support synchronized data collection across multiple processors and/or input devices down to a 1ms interval.	This 1 msec resolution across multiple processors and or input devices is required to support the correlation of SOE data within the DCS.

Requirement #	DCS Requirement	Source / Basis
DCS169	The DCS historian shall support use for predictive maintenance software for plant modeling.	Project requirement
	Cyber Security	
DCS170	The DCS shall comply with the requirements of the Secure Development and Operational Environment (SDOE) as defined in Regulatory Guide 1.152, Revision 3, in Regulatory Position C2.	Reg Guide 1.152, Rev 3 Regulatory Position C2.
DCS171	The DCS shall support Purchaser compliance with Reg Guide 5.7 or the Exelon Cyber Security "Constitution."	Project requirement
	Simulator	
DCS172	HMI and logic software shall support direct port translation to the Simulator to facilitate Simulator maintenance and integration.	Project requirement
DCS173	System control logic and HMI software shall support direct use in the plant control room Simulators without translation.	Re-engineering the provided control logic and HMI software to provide a satisfactory mimic of the actual Safety Systems installed in the plant is a costly endeavor and creates significant configuration control issues.
DCS174	System control logic and HMI software for the Simulator shall be able to run on commercially available Information Technology equipment (e.g., physical computers, servers). Any necessary software tools to enable this function (e.g., operating systems, virtualization tools, etc.) shall also be provided.	Minimize costs associated with Safety System integration to the Simulator.
DCS175	System logic and HMI software running in the Simulator shall be capable of being linked dynamically and bidirectionally to software provided by third parties that mimic control processes and physical plant performance outside of bounds of the Safety System.	Provides for the basic function of the Simulator to mimic plant operation within the Main Control Room and plant environment.

Requirement #	DCS Requirement	Source / Basis
DCS176	System logic and HMI software running in the Simulator shall be capable of executing in such a manner that it provides an operating facsimile of the system in the plant to operators in the Simulator. This includes, but is not limited to: (A) No time delay when compared to the operation of the actual system in the plant. (B) Repeatable performance for given scenarios with defined inputs.	Provides for the basic function of the Simulator to mimic plant operation within a Main Control Room environment. (ANSI/ANS 3.5-2009)
DCS177	System logic and HMI software running in the Simulator shall be capable supporting features required for Simulator training as commanded by the Simulator instructor, including: (A) Reset: Setting the Simulator to a pre-defined set of initial conditions (B) Freeze: Halt the Simulator function at any time as commanded by the Simulator instructor (C) Backtrack: To return the Simulator to a previous point in time to permit re-initiation of training using the Simulator from that point in time. (D) Run: Initiate Simulator operation for the purposes of training, either from a “Reset,” “Freeze,” or a “Backtrack” condition.	Provides Simulator features to promote training
	ENVIRONMENTAL CHARACTERISTICS	
	Electromagnetic Compatibility	
DCS178	All platform components Electromagnetic Compatibility (EMC) requirements or characteristics shall meet Reg Guide 1.180, Rev 2 or be mitigated through analysis or design control.	Reg Guide 1.180, Rev 2
DCS179	DCS I/O hardware shall be capable of filtering out noise on plant signal cables.	Plant cables pass by high voltage / current applications and the new I/O hardware shall be capable of filtering out this noise from the actual process signal.

Requirement #	DCS Requirement	Source / Basis
	Cabinet Requirements	
DCS180	All equipment shall be capable of being installed into existing enclosed cabinets	Project requirement
DCS181	All field interfaces shall be compatible with the existing PGCC "Cannon" plugs	Project requirement
	Environmental Parameters	
DCS182	The DCS HMI and any DCS Remote I/O installed in the Control Room panels shall be capable of operating within the following Control Room parameters: Temperature: 65^{o}F (Min) / 78^{o}F (Max) Pressure: +0.25 (in WG) Relative Humidity: 30% (Min) / 50% (Average) / 90% Max) Integrated Dose: 2.64E+02 RADS (Normal) / 2.71E+02 RADS (Total)	Spec M-171
DCS183	The DCS and HMI shall be capable of operating within the following Auxiliary Equipment Room parameters: Temperature: 60^{o}F (Min) / 82^{o}F (Max) Pressure: Atmospheric Relative Humidity: 30% (Min) / 50% (Average) / 90% Max) Integrated Dose: 2.64E+02 RADS (Normal) / 2.77E+02 RADS (Total)	Spec M-171
DCS184	Vibration spectra in the Auxiliary Equipment Room and Control Room	TBD by LGS
	Component Requirements	
	*Hardware	To be populated following vendor selection
	*Intelligent video display switches	To be populated following vendor selection
	*Printers	To be populated following vendor selection
	*Work stations	To be populated following vendor selection
	*Operating System	To be populated following vendor selection

Requirement #	DCS Requirement	Source / Basis
	*Servers / Chassis	To be populated following vendor selection
	*Virtual servers	To be populated following vendor selection
	*Thin clients	To be populated following vendor selection
	*Redundancy Requirement	To be populated following vendor selection
	*Server / workstation performance	To be populated following vendor selection
	*Anti-virus software	To be populated following vendor selection

Appendix C

Vendor-Independent License Amendment Request Framework Document

MPR

1129-0172-RPT-001
Revision 0

Vendor Independent License Amendment Request Framework

Prepared for: Battelle Energy Alliance, LLC

Preparer:	David Herrell	E-signed by: David Herrell on 2020-05-21 18:49:34
Preparer: (Section 3 & Tech Spec)	Bill Jessup	E-signed by: Bill Jessup on 2020-05-21 18:55:34
Reviewer:	Joseph Fougere	E-signed by: Joseph Fougere on 2020-05-21 21:21:31
Reviewer: (Not sect. prepared)	Bill Jessup	E-signed by: Bill Jessup on 2020-05-21 18:55:55
Approver:	R. Jason Gwaltney	E-signed by: R. Jason Gwaltney on 2020-05-22 08:25:05

QA Statement of Compliance

This document has been prepared, reviewed, and approved in accordance with the Quality Assurance requirements of the MPR Standard Quality Program.

Created: 2020-05-21 18:49:34
Project-Task No. 1129G046-0172

MPR Associates, Inc.
320 King St. • Alexandria, VA 22314
(703) 519-0200 • www.mpr.com

Vendor Independent License Amendment Request Framework

RECORD OF REVISIONS		
Revision Number	Pages /Sections Revised	Revision Description
0	All	Initial issue

Table of Contents

Table of Contents (cont'd.)

Table of Contents (cont'd.)

Table of Contents (cont'd.)

Table of Contents (cont'd.)

Table of Contents (cont'd.)

To Be Determined or Confirmed

To Be Determined or Confirmed (cont'd.)

To Be Determined or Confirmed (cont'd.)

To Be Determined or Confirmed (cont'd.)

To Be Determined or Confirmed (cont'd.)

Tables

Figures

Figures (cont'd.)

1 Introduction

TBD/TBC 1: **Anything provided as a "To Be Determined / To Be Confirmed" (TBD/TBC) is something that needs to be tracked to completion.**

TBD/TBC 2: **Conform LAR Framework Document and PPS Functional Requirements, once all FR comments are incorporated.**

TBD/TBC 3: **Throughout this document, ensure that all prescriptive words (e.g., shall, should, must, may) are eliminated in the final text, except in the Technical Specification definition. This document, except for the Technical Specifications, is a statement of facts, not of requirements, permissions, or choices.**

TBD/TBC 4: **In the future, this document will need to be updated to match the capabilities of the selected vendor's platform and the conformed LGS architecture. This document will also need to be split for the Project 1 implementation of RPS, the portions of N4S installed in the RPS cabinet, and the temporary equipment required for integration of the modernized N4S with the analog remnant; and for the Project 2 implementation of the removal of the temporary equipment from the RPS/N4S cabinets, completion of N4S and modernization of ECCS.**

TBD/TBC 5: **Human Factors Engineering is not currently included in this LAR Framework Document, but will need to be included to support video display of safety related system data in the Control Room, considerations for Control Room manual controls and indicators, etc.**

TBD/TBC 6: **This document provides the DI&C-ISG-06 content. Additional content from LGS, including use of the Exelon standard format, is the responsibility of LGS.**

This Vendor-Independent License Amendment Request (LAR) Framework Document is a research product developed for the Idaho National Laboratory Light Water Reactor Sustainability (LWRS) Program. It was developed by MPR Associates, Inc. with technical input from LWRS and Exelon Generation personnel. To accomplish the purpose of this research, an operating plant (Limerick Generating Station [LGS]) was used as a reference to provide a concrete example and to present a "top-down" view of design concepts consistent with the functional requirements baseline documents (Appendices A and B of LWRS report INL/LTD-20-58359) also developed for this research. While this document is written in a framework to support a complete LAR submittal, its purpose is to communicate research concepts and provide an example of how to present the digital information necessary to address expectations with regard to leveraging the Alternate Review Process, as provided in Digital Instrumentation and Controls Interim Staff Guidance #06, Revision 2, "Licensing Process." To leverage that process, this research document presupposes that a utility would select a vendor platform that has been prequalified for safety-related use by the United States Nuclear Regulatory Commission.

While this document is written using the Exelon Generation LGS Units 1 and 2 as a baseline, this document is a research product. This document contains no commitments and makes no binding design decisions for Exelon Generation. Exelon Generation is leveraging this research to support their in-progress LGS Plant Protection System (PPS) upgrade efforts and plans to leverage it for

their Redundant Reactor Control System (RRCS) replacement. The LWRS Program appreciates the research support provided by Exelon Generation in the generation of this document.

This LAR Framework Document was implemented to follow the review outline in the United States Nuclear Regulatory Commission (NRC) Digital Instrumentation and Controls (DI&C) Interim Staff Guidance (ISG) 06 (DI&C-ISG-06), Revision 2 (Reference 1). The LAR Framework Document and DI&C-ISG-06 follow the systems engineering approach defined in the EPRI Digital Engineering Guide (DEG, Reference 2).

1.1 PURPOSE

The purpose of the completed LAR is to provide data sufficient for the regulator to evaluate the proposed safety-related system changes required for the modernization (through replacement) of several safety-related systems. This LAR Framework Document was developed using LGS Units 1 and 2 as an example. This LAR Framework Document provides only the portions of the complete LAR necessary for resolution of the digital issues in NRC DI&C-ISG-06, Revision 2. The utility using this LAR Framework Document is responsible for augmenting this document with the additional materials necessary to generate a complete, plant-specific LAR.

This LAR Framework Document is part of the modernization of the key safety-related systems, and starts the process of transforming the operation of the units to the vision defined in the research document to which this LAR Framework Document is attached.

1.2 ORGANIZATION

To simplify regulatory review, each LAR Framework Document section after Section 1 follows the discussion in the NRC DI&C-ISG-06, Revision 2, Sections D.1 through D.8. This LAR Framework Document applies the Alternate Review (AR) process.

1.3 DEFINITIONS AND ACRONYMS

This LAR Framework Document section provides a set of definitions to ensure the consistent use of terms such as “channel” and “division” throughout the research document to which this LAR Framework Document is attached. This section also provides a comprehensive list of acronyms used in this document.

Table 1-1. Definitions

Channel	An arrangement of components and modules required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined. (Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-2018) [For this LAR Framework Document, the word "channel" refers to the logical group of bi-stables or bi-stable equivalents used to establish a vote to scram or actuate or a vote to not scram or not actuate.]
Division	The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components. NOTE – A division can have one or more channels. (IEEE Std. 603-2018) [For this LAR Framework Document, the word "division" refers to the voting and sequencing logic that takes data comprising votes to scram or actuate from channels and determines whether to scram or actuate based on the voting and channel status. Divisions are defined based on the electrical system grouping from which the division is powered.]
Half Isolation	In the existing design, for isolations that are controlled by logic in more than one electrical division, the Nuclear Steam Supply Shutoff System (N4S) voters in both N4S divisions must actuate to initiate an isolation. If only one division actuates, only one of the two series solenoid valves will move to the actuated position, and the isolation does not occur. This LAR Framework Document refers to this condition as a "half isolation." The modernized design is intended to eliminate half isolations.
Half Scram	In the existing design, both divisions of the Reactor Protection System (RPS) must actuate to initiate a plant scram. If only one division de-energizes one of the series solenoid valves, the control rods do not move. This LAR Framework Document refers to this condition as a "half scram." The modernized design is intended to eliminate half scrams.
Modernization	The term describes the replacement of antiquated technology that performs a particular function with current state technology that performs the same function on a case basis. The process leverages additional features of the current state technology as appropriate.
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 (IEEE Std. 7-4.3.2-2016). For this document, the term software encompasses software, firmware, and programmable logic.
Taken Twice	For this modernization project and this LAR Framework Document, "taken twice" only means taken twice in the logic and not in the field. Using the RPS scram valves as an example, the two-out-of-two actuation voting performed by the scram valves is not considered "taken twice" by this LAR Framework Document.
Transformation	The term describes a holistic approach that replaces obsolete technology across the enterprise with current technology as an integrated set. Additional features of the current state technology are leveraged as a set to achieve the maximum aggregate impact in terms of enterprise: functionality, optimization around a facility operating model, plant data gathering, equipment data gathering, modernized plant and equipment analysis and diagnostics, cyber security, and an equipment lifecycle obsolescence strategy.

Table 1-2. Acronyms

Term	Definitions for this LAR Framework Document
1oo1	One-out-of-One (Voting)
1oo2	One-out-of-Two (Voting)
2oo2	Two-out-of-Two (Voting)
2oo3	Two-out-of-Three (Voting)
2oo4	Two-out-of-Four (Voting)
4oo4	Four-out-of-Four (Voting)
10 CFR 50	Title 10 of the Code of Federal Regulation, Part 50, Energy
10 CFR 50.62	Title 10 of the Code of Federal Regulation, Part 50, Energy, Section 62, “Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants”
ADS	Automatic Depressurization System
AER	Auxiliary Equipment Room
AOP	Abnormal Operating Procedure
APRM	Average Power Range Neutron Monitor
AQ	Augmented Quality
AR	Alternate Review
ARI	Alternate Rod Insertion
ASAI	Application Specific Action Item
ATWS	Anticipated Transient Without Scram
BISI	Bypassed Indication and Status Indication
BWR	Boiling Water Reactor
CASS	Containment Atmospheric Sampling System
CM	Configuration Management
CR	Control Room
CRD	Control Rod Drive
CRDM	Control Rod Drive Mechanism
CS	Core Spray
D3	Defense-in-Depth and Diversity
DAS	Diverse Actuation System (not a system, but a function running in DCS)
DBE	Design Basis Event
DCS	Distributed Control System
DEG	EPRI Digital Engineering Guide
DI&C	Digital Instrumentation and Controls
DI&C-ISG-06	Digital Instrumentation and Controls Interim Staff Guidance 6, Revision 2

Table 1-2. Acronyms

Term	Definitions for this LAR Framework Document
DKT	Display, Keyboard, Trackball
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EHC	Electrohydraulic Controller
EIM	Equipment Interface Module
EMC	Electromagnetic Compatibility
EOC	End-of-Cycle
EOP	Emergency Operating Procedure
EPM	Electric Power Monitor
EPRI	Electric Power Research Institute
EWS	Engineering Workstation
FIC	Flow Indicating Controller
FMEDA	Failure Modes, Effects, and Diagnostics Analysis
GDC	General Design Criteria or Criterion (found in 10 cfr 50 appendix a)
GE	General Electric
HCU	Hydraulic Control Unit
HFE	Human Factors Engineering
HPCI	High Pressure Coolant Injection
HSI	Human-System Interface
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Controls
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INOP	Inoperative
IRM	Intermediate Range Monitor
ISG	Interim Staff Guidance
KVM	Keyboard, Video, Mouse
LAR	License Amendment Request
LCO	Limiting Condition for Operation
LDS	Leak Detection System
LGS	Limerick Generating Station Units 1 and 2
LOCA	Loss Of Coolant Accident
LPCI	Low Pressure Coolant Injection

Table 1-2. Acronyms

Term	Definitions for this LAR Framework Document
LPRM	Local Power Range Monitor (part of the neutron monitoring system)
MSIV	Main Steam Isolation Valve
N4S	Nuclear Steam Supply Shutoff System[1]
NEI	Nuclear Energy Institute
NRC	United States Nuclear Regulatory Commission
NUMAC	Nuclear Measurements, Analysis, and Control (General Electric – Hitachi)
NUPIC	Nuclear Procurement Issues Corporation
OBE	Operating Basis Earthquake
ODA	Operator Display Assembly
OPCON	(Plant) Operating Conditions
OPRM	Oscillation Power Range (Neutron) Monitor
OSD	On-Screen Display
PAM	Post Accident Monitoring
PCIG	Primary Containment Instrument Gas (System)
PCRVICS	Primary Containment and Reactor Vessel Isolation Control System
PGCC	Plant Generation Control Center
PID	Proportional, Derivative, Integral (Control)
PPC	Plant Process Computer
PRNM	Power Range Neutron Monitoring
PPS	Plant Protection System
RPV	Reactor Pressure Vessel
PSAI	Plant Specific Action Item
PVC	Polyvinyl Chloride
PWR	Pressurized Water Reactor
RBM	Rod Block Monitor
RCIC	Reactor Core Isolation Cooling
RCPB	Reactor Coolant Pressure Boundary
RECW	Reactor Enclosure Cooling Water
REECE	Reactor Enclosure Equipment Compartment Exhaust
RG	Regulatory Guideline

[1] N4S functionality is described within the context of the Primary Containment and Reactor Vessel Isolation Control System (PCRVICS) in the Limerick UFSAR. The acronyms PCRVIS and N4S are considered synonymous for this LAR.

Table 1-2. Acronyms

Term	Definitions for this LAR Framework Document
RHR	Residual Heat Removal
RO	Reactor Operator
RPS	Reactor Protection System
RPT	(Reactor) Recirculation Pump Trip
RRCS	Redundant Reactivity Control System
RSS	Remote Shutdown System
RWCU	Reactor Water Cleanup
SAMG	Severe Accident Management Guidelines
scram	Rapid Shutdown (Reactor Trip)
SDOE	Secure Development and Operational Environment
SDV	Scram Discharge Volume
SE	Safety Evaluation (Report, by the NRC)
SGTS	Standby Gas Treatment System
SIL	Software Integrity Level (as defined in IEEE Std. 1012)
SLCS	Standby Liquid Control System
SLD	Steam Leak Detection
SOE	Sequence of Events (secure operating environment – not used)
SOV	Solenoid Operated Valve
SR	Surveillance Requirement
SRM	Source Range Monitor
SRO	Senior Reactor Operator
SRV	Safety/Relief Valve
SSC	Structures, Systems, and Components
SSE	Safe Shutdown Earthquake
SSER	Supplemental Safety Evaluation Report
SSPV	Scram Solenoid Pilot Valve
STS	Standard Technical Specifications
TBC	To Be Confirmed – to be addressed/eliminated by the completed LAR
TBD	To Be Determined – to be addressed/eliminated by the completed LAR
TCV	Turbine Control Valve
TID	Total Integrated Dose
TIP	Traversing In-Core Probe
TS	Technical Specification

Table 1-2. Acronyms

Term	Definitions for this LAR Framework Document
TSV	Turbine Stop Valve
TTL	Transistor-Transistor Logic
UFSAR	Updated Final Safety Analysis Report
UPS	Uninterruptible Power Supplies
V&V	Verification and Validation
VOP	Vendor Oversight Plan
WCAP	Westinghouse Commercial Atomic Power (letter designator)

1.4 SYSTEM SCOPE

The proposed changes modernize the three key unit-specific safety related systems and several ancillary functions provided individually for LGS. The existing individual systems will be replaced by a single Plant Protection System (PPS), using a single prequalified platform suitable for safety-related use, having an NRC Safety Evaluation (SE) Report and suitable for the reactor trip system and engineered safety features system. The RPS, N4S, and Emergency Core Cooling System (ECCS) will be designed and implemented as three separate, independent functions within the PPS. A separate, existing, diverse Redundant Reactivity Control System (RRCS) implements the Anticipated Transient Without Scram (ATWS) function. The RRCS will be modernized under a separate project as a non-safety related diverse system. This LAR Framework Document is restricted to modifications made to replace the existing analog trip units and relay logic. This LAR Framework Document does not change transmitters or actuators in the plant or affect the wiring from the transmitters to the analog trip units or the relay logic to the actuators.

The PPS includes the following existing systems and functions:

1. The RPS, which monitors the reactor parameters (e.g., water level, pressure, power level) in the reactor core and plant parameters indicative of a reactor coolant system leak to determine if conditions merit a rapid shutdown (scram).

2. The N4S, which implements main steam line isolation and other containment and system isolation functions.

3. While not part of the N4S but providing unit status information to the N4S, the Nuclear Measurement and Control (NUMAC) Leak Detection System (LDS) chassis are absorbed into the modernized PPS as part of the N4S.

4. The ECCS, which provides High Pressure Coolant Injection (HPCI); Residual Heat Removal (RHR) including the Low Pressure Coolant Injection (LPCI), shutdown cooling, and several other manual modes; Automatic Depressurization System (ADS); and Core Spray (CS). The HPCI and Reactor Core Isolation Cooling (RCIC) initiation, functional

trip, and isolation functions are included in the ECCS function. The diverse turbine controls located in the RCIC/HPCI pump room and the Elevation 201HPCI cabinet, which are not included in the PPS. The existing HPCI and RCIC controls within the ECCS are augmented to include operator selectable flow, Reactor Vessel Pressure, and Reactor Vessel Water Level control for the reactor.

5. The Emergency Diesel Generator (EDG) start and BWR load sequencing function are installed in the CS cabinets and will be included in the modernization of the ECCS, and thus is included in the PPS. The EDG controls themselves are not part of this modernization.

1.5 LAR FRAMEWORK DOCUMENT ORGANIZATION

This document follows the review scope outline in DI&C-ISG-06, Revision (Rev.) 2 (Reference 1). This document was also developed with the guidance in Nuclear Energy Institute (NEI) 06-02, Rev. 6 (Reference 3).

TBD/TBC 7: **NEI 06-02 has not been incorporated. The ISG-06 scope is provided.**

TBD/TBC 8: **Do not move LAR Framework Document sections, combine LAR Framework Document sections, or otherwise perturb the order of discussions without providing appropriate pointers within the LAR text to the location where the text was moved. Since this will make regulatory review more difficult, please do not do this unless absolutely necessary. Section references within the LAR Framework Document to locations where additional information is provided are included to attempt to eliminate reviewer confusion.**

Since this LAR Framework Document covers three systems and provides data for the ATWS function in the Diverse Actuation System (DAS), where the DAS is a function running in the non-safety related distributed control system, the LAR Framework Document either subdivides individual DI&C-ISG-06 sections four ways, or discusses safety-related systems and then provides a similar discussion for the modernized ATWS.

1.6 SUMMARY OF CHANGES

The following features are included in this LAR Framework Document for the RPS, N4S, and ECCS systems, which are incorporated into the modernized PPS as functions:

1. Using the existing architecture, the modernized PPS will be created on an NRC prequalified platform, applying the DI&C-ISG-06, Rev. 2, AR process (Reference 1). The RPS, N4S, and ECCS software functions will be segmented and separated logically within the PPS, using common data sampled by the PPS channels from the remaining field sensors.

2. Since field wiring, sensors, switches, transmitters, and actuated equipment are not changed, the modernized PPS will continue to use the capabilities provided in much of the scram and engineered safety features actuation equipment.

3. The regulatory basis for LGS remains unchanged up to the field side of the Plant Generation Control Center (PGCC), including the circulator field wiring connectors in

the RPS, N4S, and ECCS cabinets. At that point, modern regulations will be used for the connections to the field wiring (within the limits established by the existing PGCC connectors), added wiring within the cabinet, and the PPS equipment. As explained in LAR Framework Document Section 3.1.1, the logic solvers will comply with current regulatory guidance, rather than the original plant licensing basis, including IEEE Standards (Stds.) 603-1991 (Reference 4) as incorporated in regulation and 7-4.3.2-2003 (Reference 5) as endorsed by NRC Regulatory Guide (RG) 1.152 (Reference 6).

4. In the existing design, the RPS, ECCS, N4S, and RRCS have duplicate channel-specific transmitters for the same range of a measured variable. The modernization will eliminate duplicated, similarly ranged sets of transmitters and use one set of similarly ranged transmitters in the PPS, rather than duplicating similarly ranged transmitters for each system. There are many sets of identical transmitters, which provide no benefit to the modernized PPS and DAS function in the DCS. Until the RRCS is replaced by a separate project, the RRCS transmitters are retained. To the extent practicable, the modernization will eliminate redundant transmitters and bi-stables (analog trip units) in the existing RPS, N4S, and ECCS systems.

5. The modernization will use the existing hardwired connections for field input wiring to provide hardwired connections to the new PPS logic solver inputs and outputs. The modernization will also use the existing hardwired connections between the Control Room (CR) and the Auxiliary Equipment Room (AER), where the PPS will be installed.

6. The modernization will augment the existing field input wiring for selected RPS input transmitters to include qualified safety to non-safety related isolators that will provide non-safety related wiring and data to the replacement DAS, eventually including the ATWS functions.

7. The modernization will replace the existing Rosemount Analog Trip Units, pneumatic timing relays, relay logic, NUMAC chassis, and other hardware in the existing cabinets with software that performs the same functions within the new PPS logic solvers. The modernization will replace the hardwired channels and divisions of RPS, N4S, and ECCS with separate, independent PPS logic solvers for each of the four separate PPS channels and divisions. Each PPS logic solver will provide the bi-stable logic for all RPS, N4S, and ECCS inputs, providing the votes to scram or actuate (or not scram or not actuate) to both divisional logic solvers. All discrete outputs will be constructed to be single-failure tolerant, reducing the potential to either inadvertently actuate or fail to actuate.

8. Each PPS logic solver will provide the same, or improved, logic to scram or actuate. This will replace the relay logic used in the legacy design for the voters in the existing RPS, N4S, and ECCS.

9. The existing RPS scram occurs if any single scram initiator occurs in one division combined with any single scram initiator in the other division. The modernization will ensure that the same scram initiator is required from more than one channel and that the scram will no longer occur if the channels produce different scram initiators. The same changes will be implemented, as appropriate, in the ECCS and N4S.

10. This modernization will replace the RPS one-out-of-two (1oo2) taken-twice voting scheme with a more conservative two-out-of-four (2oo4) voting scheme. All four channels will provide votes to scram or actuate from the bi-stable channels to both RPS logic solver divisions, thus eliminating the scenario when two channels (e.g., A1 and A2) could vote to scram while the other two channels (e.g., B1 and B2) do not vote to scram resulting in only a half scram. With the modernized PPS, in the example, the votes from existing Channels A1 and A2 will be provided to both sets of voting logic thus initiating the required scram. The modernized design will make similar modifications to the voting schemes within the N4S and ECCS.

11. As required by the Defense-in-Depth and Diversity (D3) Analysis (Reference 7), the modernization will install a non-safety related, augmented quality (AQ) DAS, with qualified isolators on inputs and outputs as necessary. If the D3 Analysis determines that DAS functions for the N4S and ECCS are not necessary, then the only function residing in the DAS is ATWS.

12. This modernization includes a design to replace the RRCS with an ATWS function in the modernized non-safety related DAS function in the DCS.

13. This modernization will make use of the hardwired PGCC connections between the existing, retained field input and output wiring terminals and the new PPS logic solvers and termination panels.

14. The modernization will install new two-way redundant fiber-optic cabling between each safety-related channel and division and to safety-related display generators. This LAR Framework Document refers to the safety-related display generators as Display, Keyboard, and Trackball (DKT) Interfaces, and the video display and user input devices as DKTs. The DKTs will provide safety-related and non-safety data display and soft controls in the CR and AER.

15. The CR will be equipped with distributed sets of safety-related DKTs for data display and soft controls. The safety-related DKTs can be used for non-safety related use (LAR Framework Document Section 3.3.5 and subsections describe the application, design, and use of the DKT). The CR will use the DKT Switch software to switch the safety-related DKTs between PPS, DAS, and non-safety related uses. (An evaluation of the DKT system is provided in Section 3.3.5.2.) There will be no dedicated divisional safety-related video displays in the CR. Continuously visible data will be displayed on one or more selected DKTs, under administrative control. The DKTs will be configured to restrict certain locations in the CR and AER from performing control actions.

TBD/TBC 9: The DKT architecture is a new design concept that has not been reviewed by the NRC for safety-related use. Use of the DKT architecture in this document will set precedent for the nuclear industry.

16. The DKTs will not totally replace the existing indicators and meters in all applicable Operations procedures, including accident, transient, and Severe Accident Management Guidelines (SAMG). The modernization will retain meters and recorders not part of the RPS, N4S, and ECCS modernization. The modernization will eliminate those meters and

recorders that provide RPS, N4S, and ECCS data and provide modernized safety-related display through the PPS DKTs. The modernization will remove all indicating lamps for the PPS, N4S, and ECCS and place that indication on DKTs.

17. The wiring of the manual scram buttons will be changed to affect the outputs of the divisions, to support the requirements that manual actions are not subject to a common cause failure of the PPS software logic. Reset and other less time-sensitive actions will be incorporated into the PPS and into the DAS soft controls on the DKTs, based on decisions documented in various sections of this LAR Framework Document. The state of the retained manual controls will be sampled by the PPS, with appropriate automatic actions initiated based on operator manual control actions. All retained manual operator controls will be duplicated in soft controls on the DKTs, for diversity. All eliminated manual operator controls will be provided solely as soft controls on the DKTs. The wiring for these manual controls will be modified, and interposing relays will be incorporated as needed to support current needs, especially for the reactor scram solenoid pilot valves (SSPVs).

18. The modernized PPS will retain and modify the existing manual controls as required, such as reducing from four to two Reactor Scram pushbuttons. The modernized design will ensure that the manual controls are wired to preclude a software common cause failure or other failure in the PPS from disabling the manual initiation of this safety functions. Those manual controls that are not required by regulation will be evaluated for replacement (or at least duplication) in soft controls on safety-related DKTs. The CR retains manual actuation switches when required. The hardwired reset and manual bypass switches will be removed to soft controls on the PPS and on the DAS. Manual actuations will be duplicated as soft controls on the PPS and DAS to implement the manual initiation of automated protective functions at the division-level requirement of IEEE Std. 603-2018 Clause 6.2 Item a.

19. For the DAS function (not including the ATWS function, which is part of a separate LGS project), the modernization will provide division-level soft actuations as soft controls on the PPS and as required in the DAS, implemented in the same DCS platform used for most of the non-safety related controls. The DAS will be composed of two segmented, internally-redundant controllers and redundant data acquisition, to maximize reliability and minimize the potential for inadvertent actuations by the ATWS.

20. The modernization will ensure that the PPS design supports providing all data to the Distributed Control System (DCS) and thus to Plant Process Computer (PPC).

21. As part of the process of changing 1oo2 taken twice to modern 2oo4 or similar voting schemes, the modernization will provide redundant, one-way fiber optic communication cables from each of the four PPS channels to all PPS divisions.

22. The modernization will install redundant, one-way fiber optic cabling from each PPS channel and division to the non-safety related DCS data backbone, which will provide diverse display of all PPS data and status on the PPS, DCS, and PPC displays. The design will provide PPS channel and division data to the non-safety related data network

through fiber optic serial communication links. The design also will provide DAS data to the data network through bidirectional communication, since the DAS and the data network will be built of the same technology

23. Software in a server on the data network will replace the existing manual operator channel checks with automated instrument checks, providing continuous surveillance of the channel inputs used by the bi-stable logic, replacing the manual diagnosis of failed sensors or analog trip module inputs.

24. Existing Bypassed Indication and Status Indication (BISI) lamps and annunciator panels will be eliminated and replaced with BISI displayed on one or more administratively controlled, continuously visible DKTs.

25. The modernization is intended to ensure that the platform design does not preclude future migration of other safety-related systems and functions to the platform. However, this LAR Framework Document does not include the migration of other safety-related systems and functions beyond those defined in the LAR Framework Document.

26. The modernization considers the architectural considerations for replacing the obsolete safety-related digital RRCS with a highly reliable, four channel, internally redundant, non-safety related DCS solution as a DAS for the PPS, which meets the ATWS requirements established in Title 10 of the Code of Federal Regulation, Part 50, Energy (10 CFR 50) Section 62 (10 CFR 50.62, Reference 8), including AQ. The RRCS replacement is not part of this LAR Framework Document, but a discussion of the plans for the separate LGS project is included to discuss aspects of ATWS and RPS DAS. The modernized DAS design will retain the four sets of DAS sensor inputs and provide redundant channel logic in each of the two redundant implementations of the DAS logic in separate DCS controllers. The modernized design will include appropriate, qualified isolators between the safety-related field transmitters and the non-safety related DCS inputs as well as isolators between the non-safety related DCS outputs and the safety-related actuated devices. The modernized design will use single-failure tolerant, diagnosed discrete output switching, to ensure that no single failure in an output switch disables or falsely initiates protective actions. The modernized ATWS will eliminate the feedwater flow runback from the RRCS, as this runback is not consistent with the ATWS requirements in 10 CFR 50.62 and has been demonstrated to challenge plant operations staff.

27. Due to the extensive use of self-tests and self-diagnostics and other features within the PPS logic solvers and the non-safety related DCS, instrument channel checks and logic system functional tests, including channel functional tests, will be eliminated as a surveillance activity. Modern equipment and automated comparisons of the analog inputs in non-safety related equipment will reduce the frequency of analog-to-digital converter channel calibration checks.

28. Various functions included in the existing RPS and N4S cabinets will be absorbed into the PPS. This will include combining the LDS in the four dedicated function NUMAC chassis, which currently provides data display only in the AER, into the N4S function of

the PPS, providing CR data display through the DKTs. This will also include incorporating initiating the four EDGs in the ECCS cabinets with the CS subfunctions as well as incorporating flow measurement for the Reactor Water Cleanup System (RWCU) into the N4S.

2
Plant Systems Descriptions (DI&C-ISG-06 D.1)

This section provides text and drawings to describe the unit's existing RPS, ECCS, and N4S. This section identifies, documents, and describes the scope and boundaries of the existing systems.

2.1 Description of the Existing Systems (DI&C-ISG-06 D.1)

The RPS, N4S, and ECCS are separate systems, and support one of the two Limerick Generating Station units. There are no ties between the existing safety systems for Unit 1 and Unit 2. The PPS will maintain the existing system separation design and will not provide any ties between the PPS installed in Unit 1 and the PPS installed in Unit 2. There will be no multi-station attributes associated with these safety systems.

The existing RPS, N4S, and ECCS are comprised of analog trip units (channels) and wiring between the trip units and relay logic within the electrical divisions. The electrical divisions perform voting, time delays, and logic. The existing RPS and most of the N4S are installed in four cabinets in the AER, with additional N4S and all of the ECCS installed in additional cabinets in the AER. The wiring connects channels within an electrical division to the relay logic within that electrical division.

The existing safety-related RRCS (ATWS logic) is implemented in transistor-transistor logic (TTL) in RRCS-specific, safety-related, General Electric (GE) designed, redundant processors. The digital RRCS samples analog inputs and implements the ATWS logic in this microprocessor-based system. This obsolete digital equipment is equipped with self-tests and self-diagnostics. Maintenance of this equipment is increasingly difficult, since TTL integrated circuits are no longer widely available and two of the known units in the world are installed at LGS.

The existing design provides the RPS, N4S, and ECCS indications on lamps, annunciator windows, meters, and recorders in the CR. The existing design provides LDS annunciation in the CR but only provides LDS data displays in the AER. To determine the location of an annunciated, detected leak, the CR staff dispatches an Equipment Operator to the AER to read and relay temperatures and status from the NUMAC displays in the AER back to the CR. For channel checks, an operator uses the analog trip unit displays to gather data, since almost none of the data is available in the CR.

2.1.1 Description of Existing RPS (DI&C-ISG-06 D.1.1)

The primary function of the RPS is to initiate a scram of the reactor through insertion of the control rods in order to:

- Prevent or limit fuel damage following abnormal operational transients
- Prevent damage to the Reactor Coolant Pressure Boundary (RCPB) as a result of excessive internal pressure, and
- Limit the uncontrolled release of radioactive materials from the fuel assembly or RCPB.

The RPS provides this function by monitoring certain plant parameters and, if one or more parameters exceed a specified limit, the RPS system functions to automatically insert control rods to terminate power production in the core. Control rod movement is performed by the Control Rod Drive (CRD) system. When power is removed from the SSPVs, the de-energized valves exhaust air, causing the control rods to scram. The automatic scram function of RPS is accomplished by monitoring the following plant parameters:

- Scram Discharge Volume (SDV) Water Level
- Main Steam Line Isolation Valve (MSIV) Position
- Main Turbine Stop Valve (TSV) Position
- Main Turbine Control Valve (TCV) Fast Closure
- Reactor Vessel Water Level
- Neutron Flux
- Drywell Pressure
- Reactor Vessel Pressure

Setpoint values used to generate an automatic scram signal are documented in the PPS Functional Requirements document (Reference 9). In addition to generating automatic reactor scram signals in response to the conditions described above, the RPS provides the capability to manually scram the reactor through the use of Manual Scram Pushbutton switches or by placing the Reactor Mode Switch in the “Shutdown” position.

The RPS consists of two trip systems (A and B) each containing two channels of sensors and logic, for a total of four logic channels. The monitored parameters each have at least one input to each of the logic channels. The overall RPS logic requires that at least one channel in each of the two trip systems must be tripped in order to turn off the field power and open both paired solenoid valves in the field to cause a scram. This is referred to as 1oo2 taken-twice voting logic.

The RPS is a normally energized system. De-energizing any channel or the relay trip system in an electrical division places the trip system in that electrical division in a tripped condition (i.e., half scram). This makes the RPS fail-safe on loss of electrical power. For this reason, each electrical division is powered by two independent power sources so that failure of one power source does not cause a half scram.

In addition to the various sensors, relays, and switches, the RPS includes the RPS inverter power sources, which provide the RPS with the ability to remain energized (prevent spurious trips) during short power loss transients, and the RPS bus protective devices, which ensure that when power is available it is within the requirements of the bus loads.

2.1.2 Description of Existing N4S (DI&C-ISG-06 D.1.1)

The N4S initiates the closure of various automatic isolation valves if monitored system variables exceed preestablished limits. This action limits the loss of coolant from the RCPB and the release of radioactive materials from the RCPB, the primary containment, and the reactor enclosure. The functional requirements associated with the N4S and its interfacing systems necessitate the following:

1. Pipes or vents that penetrate primary containment and communicate directly with the reactor vessel have two isolation valves: one inside primary containment (i.e., inboard) and one outside primary containment (i.e., outboard).

2. Pipes or vents that connect directly to the containment atmosphere and penetrate primary containment have two valves outside containment (i.e., inboard closest to containment and outboard further away from containment).

The N4S consists of seven functions (see Table 2-1, Technical Specification Section 3/4.3.2) implemented using eight logical isolation groups (see Table 3-5). These functions and groups are largely divided by the interfacing systems, which are isolated by the actuation of the N4S (e.g., Group I provides main steam isolation, Group II provides isolation of the RHR system, etc.).

Table 2-1. Isolation Functions

Function	Provides Isolation For
1.	Main Steam
2.	Residual Heat Removal Shutdown Cooling Mode
3.	Reactor Water Cleanup
4.	High Pressure Core Injection
5.	Reactor Core Isolation Cooling
6.	Primary Containment
7.	Secondary Containment

2.1.3 Description of Existing ECCS

The ECCS is comprised of independent core cooling systems that ensure the requirements of 10 CFR 50.46, "Acceptance criteria for emergency core cooling systems for light-water nuclear power reactors," are satisfied if a breach in the RCPB results in a loss of reactor coolant. The following systems are included in the ECCS, except where noted:

- HPCI: The HPCI system provides and maintains an adequate coolant inventory inside the reactor vessel to limit fuel clad temperatures resulting from postulated small breaks in the RCPB. HPCI uses a large steam-driven pump to inject water to the Reactor Pressure Vessel (RPV) through the feedwater and the Core Spray spargers.

- ADS: The ADS acts to rapidly reduce Reactor Vessel Pressure in a Loss-of-Coolant Accident (LOCA) situation in which the HPCI system fails to maintain Reactor Vessel Water Level. Under certain circumstances, HPCI may be unable to provide sufficient inventory to recover from a LOCA. However, if Reactor Vessel Pressure remains high concurrent with the LOCA, then the high-capacity, low-pressure ECCS pumps cannot inject until the Reactor Vessel Pressure has been lowered below the pump's shutoff head pressure. This depressurization function is executed by the simultaneous opening of five Safety/Relief Valves (SRVs) by the ADS, based on conditions that indicate HPCI cannot maintain Reactor Vessel Water Level sufficiently high while the RPV is still pressurized.

- CS: The CS system cools the fuel by spraying water on the core in the event of a LOCA associated with a wide range of pipe break sizes. This function is executed through two mechanical divisions of two pumps each along with the requisite piping and valves. The existing CS system is divided into four electrical divisions where each pump is powered from one emergency 4 KV bus, which can also be powered by an EDG. Each division of CS also includes a separate instrumentation and controls (I&C) architecture.

- RHR: The RHR system provides a number of different operating modes. The LPCI mode is credited as part of the ECCS. LPCI acts to mitigate the consequences of a large-break LOCA by injecting to the RPV at low Reactor Vessel Pressure. The RHR system also has non-ECCS modes that support containment cooling (Suppression Pool cooling, containment spray), shutdown cooling for decay heat removal, and other support functions (e.g., fuel pool cooling assist, alternate decay heat removal, and Suppression Pool level control through a radioactive waste system interface). The RHR system executes this function through the use of four divisions, each containing a pump along with the requisite piping, valves, and control systems. Two heat exchangers are also provided to support cooling capabilities.

- RCIC: The RCIC system provides makeup water to the reactor vessel whenever the vessel is isolated from the main condenser and feedwater system. RCIC is not credited as an ECCS system, although RCIC performs similar functions. RCIC executes its safety function in a manner similar to HPCI, through the use of a steam-driven pump that injects into one of the main feedwater lines associated with the RPV. However, RCIC operates with a much smaller capacity than the HPCI system.

For the purposes of simplification, RCIC and non-LPCI modes of RHR are included within the scope of ECCS for this LAR Framework Document. However, non-ECCS requirements for these systems (e.g., those associated with 10 CFR 50.46) that do not apply to ECCS are not documented in the LAR Framework Document.

2.1.4 Description of Existing RRCS (DI&C-ISG-06 D.1.1)

The RRCS provides a diverse means of shutting down the reactor in the event of an ATWS to satisfy the requirements of 10 CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants" (Reference 8). The RRCS accomplishes this function by shutting down the reactor, using diverse methods, at pressures above and reactor water levels below the pressure and level at which the RPS should have scrammed the reactor.

The diverse methods of power reduction and reactor shutdown executed by the RRCS include the following:

- Initiation of Alternate Rod Insertion (ARI) to vent the scram air header and insert control rods
- Stopping the reactor recirculation pump motors by tripping their breakers upon receipt of ATWS indications
- Automatic runback of reactor feedwater pumps to support terminate-and-prevent actions, which leverage reactor thermal-hydraulics to reduce power
- Initiation of the Standby Liquid Control System (SLCS) following receipt of ATWS conditions (i.e., reactor at high pressure, low level, and sustained high-power conditions).

The existing RRCS is safety-related and comprised of four channels and two voters. Each of the four channels is completely independent of the other channels. Figure 2-1 below illustrates the existing RRCS.

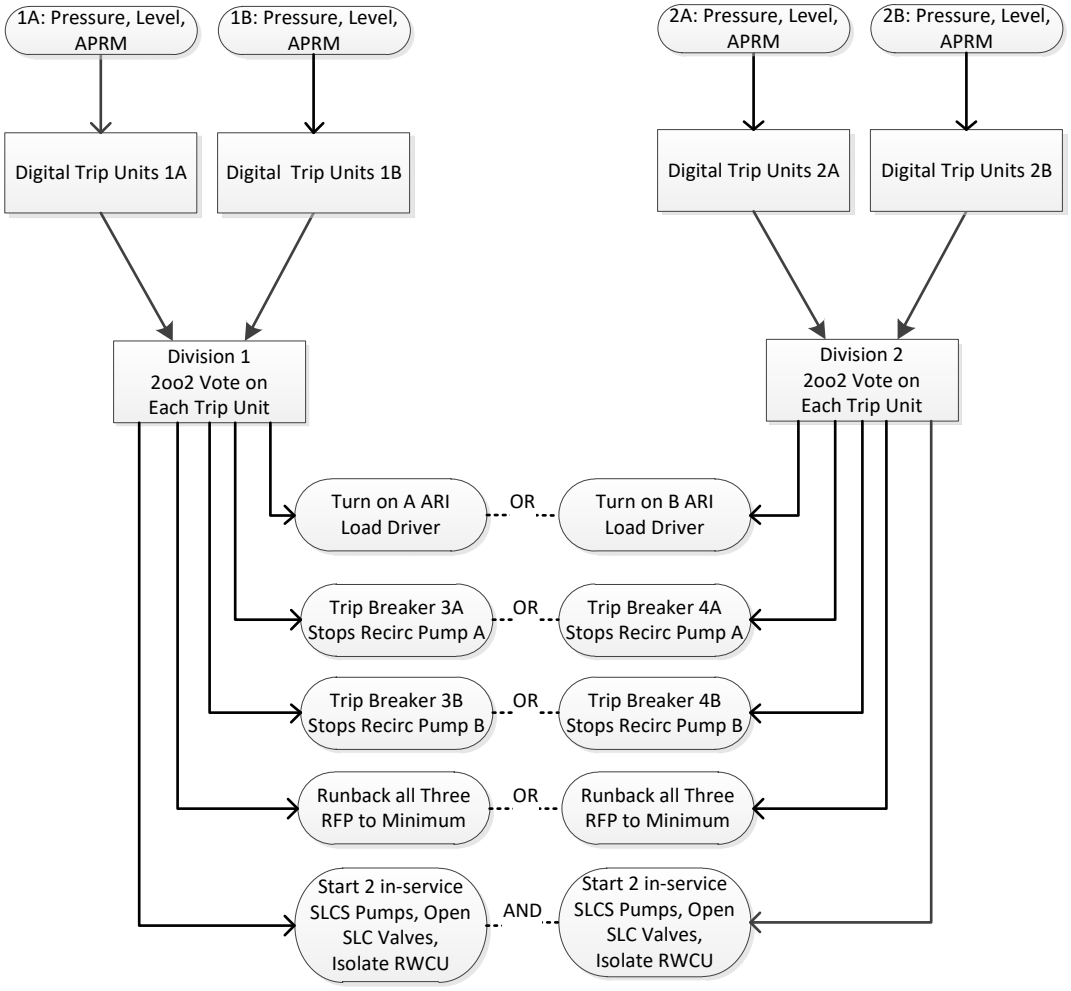

Figure 2-1. Existing RRCS Functional Block Diagram

3
Plant Systems Architecture (DI&C-ISG-06 D.2)

3.1 DESCRIPTION OF THE NEW PPS (DI&C-ISG-06 D.2.2)

This LAR Framework Document describes the modernization of the existing RPS, N4S, and ECCS into the PPS. This section describes the replacement PPS, showing the changes introduced by the modernization in the existing system described in Section 2.1 above.

The PPS will provide the functions formerly performed by separate RPS, N4S, and ECCS systems. The existing RPS, N4S, and ECCS systems will become segmented functions running on the PPS. The modernized design will retain the four-channel architecture common to the RPS, N4S, and ECCS, where the channel functions perform all RPS, N4S, and ECCS sensor and bi-stable functions in separate, segmented applications/functions. The modernized design will retain the two division architecture in the RPS as well as the two or four division architecture in the N4S and ECCS, but each division will perform the RPS, N4S, and ECCS voting, operational bypass, and maintenance bypass functions in separate, segmented applications, which this LAR Framework Document refers to as functions. The existing scram, bypass, inhibit, permissive, and similar manual CR capabilities will be included in the PPS functions, although some will be modernized to soft controls. This LAR Framework Document considers the Technical Specification (TS) functions (also referenced as isolation groups in the operating procedures) in the N4S to be subfunctions within the N4S function of the PPS. This modernization will also consider the various systems within the ECCS as subfunctions within the ECCS function of the PPS.

TBD/TBC 10: New decision – LGS to specify which manual controls remain in the CR. Which are credited in the Abnormal Operating Procedures (AOPs) or Emergency Operation Procedures (EOPs) or potentially used in the SAMG, which must continue to be hardwired, such that SCCF does not disable the manual controls? Anything not required for coping with accidents can be absorbed into soft controls and hardwired controls eliminated.

3.1.1 PPS Licensing Design Basis (DI&C-ISG-06 D.2.2)

Based on the LGS Updated Final Safety Analysis Report (UFSAR), the existing RPS, N4S, and ECCS are licensed to the following IEEE standards and endorsements in the Regulatory Guides to which LGS is committed:

1. IEEE Std. 279-1971 (Reference 10)
2. IEEE Std. 308-1971 and -1974 (References 11 and 12)
3. IEEE Std. 317-1972 (Reference 13)
4. IEEE Std. 323-1971 (Reference 14)

5. IEEE Std. 336-1971 (Reference 15)

6. IEEE Std. 338-1971, -1975, and -1977 (References 16, 17, and 18)

7. IEEE Std. 344-1971 and -1975 (References 19 and 20)

8. IEEE Std. 379-1972 and -1977 (References 21 and 22)

9. IEEE Std. 382-1972 (Reference 23)

10. IEEE Std. 383-1974 (Reference 24)

11. IEEE Std. 384-1974 and -1977 (References 25 and 26)

Within the limitations imposed by the existing field wiring at the input and output terminations within the existing RPS, N4S, ECCS, and DAS cabinets, LGS will implement the PPS in compliance with endorsed IEEE standards, but the design process will also consider guidance from current IEEE standards in the design. A primary example of an unendorsed standard is the informational fiber optic separation criteria provided in IEEE Std. 384-2018. These considerations will be incorporated in the design appropriately. These standards include, but are not limited to:

1. IEEE Std. 603-1991 (Reference 4), as endorsed in 10 CFR 50.55a(h)(2) and RG 1.153 Rev. 1, with updates and clarifications from IEEE Std. 603-2018 (Reference 27);

2. IEEE Std. 7-4.3.2-2003 (Reference 5), as endorsed in RG 1.152 Rev. 3, with updates and clarifications from IEEE Std. 7-4.3.2-2016 (Reference 28);

3. IEEE Std. 308-2001 (Reference 29), as endorsed by RG 1.32 Rev. 3, with updates and clarifications from IEEE Std. 308-2012 (Reference 30);

4. IEEE Std. 323-2003 (Reference 31), as endorsed by RG 1.209 Rev. 0, with updates and clarifications from International Electrotechnical Commission (IEC) / IEEE 60780/323-2016 (Reference 32);

5. IEEE Std. 336-1971 (Reference 15), as endorsed by RG 1.30 Rev. 0, with updates and clarifications from IEEE Std. 336-2010 (Reference 33);

6. IEEE Std. 338-1987 (Reference 34), as endorsed by RG 1.118 Rev. 3, with updates and clarifications from IEEE Std. 338-2012 (Reference 35);

7. IEEE Std. 379-2003 (Reference 36), as endorsed by RG 1.153 Rev. 2, with updates and clarifications from IEEE Std. 379-2014 (Reference 37);

8. IEEE Std. 383-2015 (Reference 38), as endorsed by RG 1.211 Rev. 0; and

9. IEEE Std. 384-1992 (Reference 39), as endorsed by RG 1.62 Rev. 1 and RG 1.75 Rev. 3, with updates and clarifications from IEEE Std. 384-2018 (Reference 40).

This LAR Framework Document does not change the unit's licensing basis standards for equipment outside the RPS, N4S, and ECCS cabinets in the AER and for equipment installed in the CR. For this reason, IEEE Std. 317 (on mechanical, electrical, and test requirements for containment penetrations) and IEEE Std. 382 (on qualification of field actuators) are not included in the list above.

The installation will comply with the IEEE standard separation criteria in IEEE Std. 384 to the extent practicable, limited only by any separation limitations present in the field wiring terminations. LGS will apply the fiber optic cable separation guidance in informative Annex C of IEEE Std. 384-2018 (Reference 40).

IEEE Std. 338-1987 (Reference 34) provides guidance for the types of testing previously required, but this LAR Framework Document considers the rationale for the requirements in the current version of IEEE Std. 338-2012 (Reference 35), and eliminates those channel functional tests, instrument channel checks, and the logic solver portion of channel calibration no longer required, which have been superseded by self-tests, self-diagnostics, and other features within the PPS logic solvers and the non-safety related DCS. Elimination of these testing requirements is based on the self-test and self-diagnostic capabilities of the system in both the platform and in application logic added to support testing and diagnostics for the inputs and outputs.

The PGCC design provides standard circular connectors for the field wiring, with the connections between field wiring and internal cabinet wiring using the standard circular connectors. The modernization will start at the circular PGCC connections within the existing cabinets. The PGCC field wiring, including field wiring connectors, will not be modified. The existing wiring between the circular PGCC connectors and the trip units and relay logic will be removed. The new wiring connections and new programmable, digital logic solvers will be made using current IEEE standards, rather than the original LGS licensing standards. Since part of the PGCC connections include CR switches and indicator lamps, the design will abandon wiring for some CR switches and all the CR indicator lamps for the RPS, N4S, and ECCS. Portions of the existing PGCC wiring to the CR for the RPS, N4S, and ECCS will be retained and used by the PPS.

The existing licensed standards for LGS are not sufficient or appropriate for modern digital systems. The new licensing basis for only the replaced bi-stable and logic solving portions of the RPS, N4S, and ECCS will use a licensing basis appropriate to modern digital equipment. However, the modification will not rework the existing field wiring and field wiring terminations in the RPS, N4S, and ECCS cabinets to provide separation required in modern standards. Rather, the modification will implement the new licensing separation requirements in wiring added to connect the digital equipment to the existing terminations as close to the existing terminations as possible, without modifying the existing field wiring terminations. This change in licensing will assure that the installation is in accordance with the same licensing basis the vendors and NRC used to evaluate the prequalified equipment against then-current standards at the time of NRC approval. The modification will install the equipment in accordance with the standards to which the NRC evaluated and accepted the prequalified platforms.

Exelon will update the LGS UFSAR (Reference 41) to reflect these changes specific to the RPS, N4S, and ECCS systems:

TBD/TBC 11: **The UFSAR will be updated to state: Modernization of the RPS, N4S, and ECCS does not change the LGS licensing basis outside of the PPS cabinets. Within the limitations imposed by the existing field wiring at the input and output terminations within the RPS, N4S, and ECCS cabinets, the modernized PPS complies with the current regulatory guidance and endorsed IEEE standards. These standards include, but are not limited to, IEEE Standards Stds. 603-1991 and -2018, 7-4.3.2-2003 as well as additional clauses from IEEE Stds. 7-4.3.2-2016 , 379-2014, 384-2018, and IEC/IEEE 60780-323-2016.**

TBD/TBC 12: **The UFSAR will be updated to state: To the extent practicable, the modernization separated the system wiring attached to the input and output terminations, based on the limitations present in the field wiring terminations. Fiber optic cables use the separation guidance in IEEE Std. 384-2018.**

TBD/TBC 13: **The UFSAR will be updated to state: The LGS UFSAR provides the rationale used to replace performance of some of the surveillance tests required in IEEE Stds. 338-1987 and 338-2012 with PPS self-tests and self-diagnostics. The LGS UFSAR explains that the PPS modernization eliminates channel functional tests, instrument channel checks, and the logic solver portion of channel calibration based on the capabilities designed into the self-tests and self-diagnostics and other features within the PPS logic solvers and the non-safety related DCS platform and application software.**

3.1.2 Modernization of RPS, N4S, and ECCS into Combined PPS (DI&C-ISG-06 D.2.2)

The modernization will focus on the analog trip units and relay logic for the RPS, N4S, and ECCS. A separate project will remove the safety-related RRCS and install a non-safety related ATWS. The modernization will include a DAS for the appropriate portions of the N4S and ECCS. This LAR Framework Document concludes that either the existing RRCS or the modernized ATWS incorporated into the DAS provides sufficient diversity for the RPS. The DAS design will be based on the D3 Analysis (Reference 7) for the N4S and ECCS.

In order to use the DI&C-ISG-06 AR process, LGS has selected one of the prequalified platforms for this modernization. The PPS design considers the vendor's licensing topical report (Reference 42) and the platform evaluation and application items in the NRC's SE Report (Reference 43). This LAR Framework Document is based on the vendor's licensing topical report and NRC's SE Report described and evaluated in Section 6.1. Any changes to the vendor equipment as described and evaluated in the vendor's licensing topical report and NRC's SE Report are described and evaluated in Section 6.2.

The new PPS will provide the RPS, N4S, and ECCS as segmented functions in the PPS, running on a common platform. These three functions will retain their existing logic separation, but all three will operate on a common platform, with clear differentiation between channels and electrical divisions. The LAR Framework Document discusses each of these three functions, either separately or as the combined PPS. The new PPS will be installed in the same cabinets from which the RPS, N4S, and ECCS were removed, which retains the licensed, appropriate physical separation.

The ATWS functions will provide the only required DAS for the RPS functions. The N4S and ECCS functions will be evaluated in a D3 Analysis (Reference 7). Only those functions required by the D3 Analysis will be included in the DAS. The CR DKTs will provide access to the DAS functions and DAS data. The DAS primarily will use soft controls on the DKTs.

The modernized design in this LAR Framework Document refers to divisions, which take the channel votes to scram and determine whether sufficient votes to scram exist to initiate the appropriate protective action. In the existing design, the divisions are referred to as the Trip System or the Voters. The existing bi-stable analog trip modules will be replaced with application software in the modernized PPS channels.

The PPS will consist of four independent channels and four independent divisions. For some functions, only two divisions will be used (e.g., RPS and portions of the N4S and ECCS). Each channel is physically and logically separated from the other three channels. Each division is physically and logically separated from the other three divisions. The electrical divisions and mechanical trains from the existing RPS, N4S, and ECCS are retained in the PPS.

Data communication over fiber optic data links is a basis for this design, as shown in Figure 3-3 and Figure 3-4 below. To enhance reliability, all fiber optic links within and from the PPS will be redundant. The point-to-point data communication links will not be connected or networked in any way. Each fiber optic link will provide data from one source to one or many destinations. The data links will have the following attributes:

- There will be one-way redundant fiber optic links from each safety-related channel to each safety-related division.

- To ensure that the same data is provided from each channel to each division, each of the fiber optic transmitters in each division will provide data to a passive fiber optic splitter, which then provides identical data streams to each division.

- There will be two-way redundant fiber optic data links from each channel and each division to the DKT Interfaces.

- The communication of video and data packets within the DKT system is described in Section 3.3.5.

- There will be one-way redundant fiber optic links from each safety-related channel and safety-related division to the non-safety related DCS data network, which allows for the diverse display of all PPS and DAS data and status by non-safety related displays.

- The DAS will be an integral part of the non-safety related DCS data network, which provides redundant communication networks.

This design will not include any communication links between safety-related channels or between safety-related divisions, including the links to an Engineering Workstation (EWS). The design will separate RPS, N4S, and ECCS functions logically into separate tasks, each using the channel's sampled set of common inputs from field transmitters. Section 3.3.6.3 discusses the design functions implemented. The design will maintain the original design functions, with additional automation provided to support Operations, Maintenance, and Engineering staff.

Due to the extensive use of self-tests, self-diagnostics, and other features within the PPS logic solvers and the non-safety related DCS and an extensive evaluation of fault and failure coverage

against the faults and failures that would be detected by surveillance tests, logic system functional tests (including channel functional tests) and instrument channel checks will be eliminated, and channel calibration for the analog inputs to the channels will be significantly reduced. A significant reduction in the effort required to execute response time testing also will be provided with the digital platforms. The remaining response time testing effort will be limited to the calibration of field devices, which this modernization does not eliminate.

The process described in Section 8.1.1 supports the elimination of channel checks as surveillance tests. The elimination of channel checks is consistent with the Vogtle Units 3 and 4 LAR and the WCAP that eliminate channel checks as surveillance tests from the Vogtle Units 3 and 4 Technical Specifications.

The original design used several different numbering schemes for channels and divisions. The modernized design will normalize the channel and division nomenclature within the PPS as shown in Table 3-1 and Table 3-2 below.

Table 3-1. Channel Nomenclature

Item	Current System	Transmitter	Existing Channel	Modernized Channel
1.	RPS	A	A1	A
2.	RPS	B	A2	B
3.	RPS	C	B1	C
4.	RPS	D	B2	D
5.	ECCS	A	A	A
6.	ECCS	B	B	B
7.	ECCS	C	C	C
8.	ECCS	D	D	D
9.	N4S	A	A	A
10.	N4S	B	B	B
11.	N4S	C	C	C
12.	N4S	D	D	D

Table 3-2. Division Nomenclature

Item	Current System	Existing Division	Modernized Division
1.	RPS	A	1
2.	RPS	B	2
3.	PPS	C	3
4.	PPPS	D	4

This design will construct the modernized PPS on the vendor's standard platform and software tools. Figure 3-1 below provides a platform level view of the replacement system. The modernized PPS will retain most of the same architecture but replace the hardware implementations of the analog trip units (i.e., channels) in the RPS, N4S, and ECCS with four separate digital platforms implementing the separate, independent channel functions. The modernized design will replace the relay voting logic with separate, independent divisions in separate, independent digital platforms.

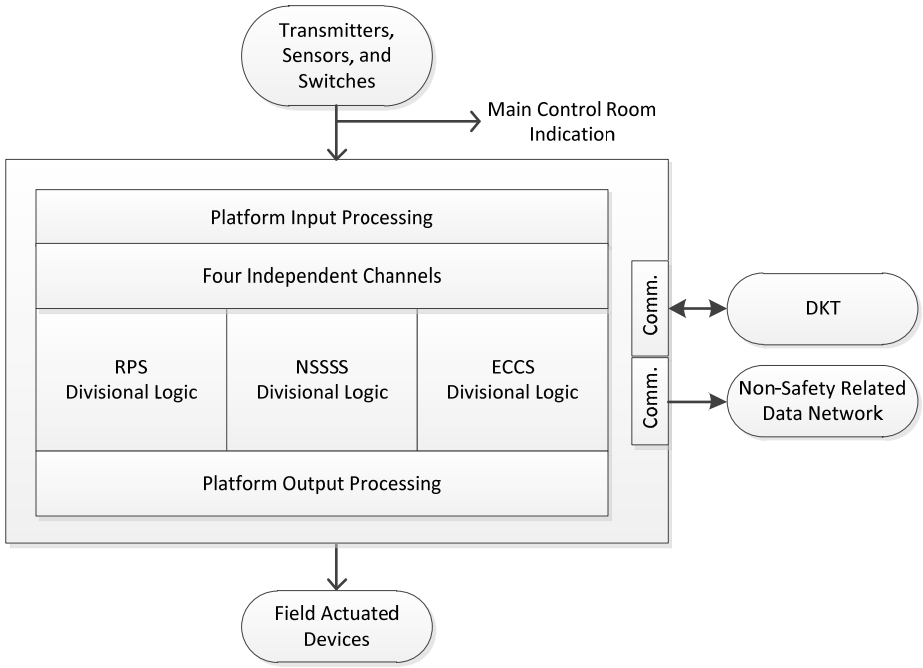

Figure 3-1. Modernized Single Division of PPS Logical Architecture

Figure 3-2 below shows a channel-specific view of the PPS, including the DAS and signal interfaces from the safety-related field sensing elements to the non-safety related DAS inputs. A bidirectional arrow is shown between the two segmented controllers implementing the DAS function to indicate that each controller samples two channels of information and then shares the channel information through communication links between the two DAS segments. The DAS is shown here solely for understanding the interface between the DAS and the PPS. The DAS is described in Section 3.1.6.

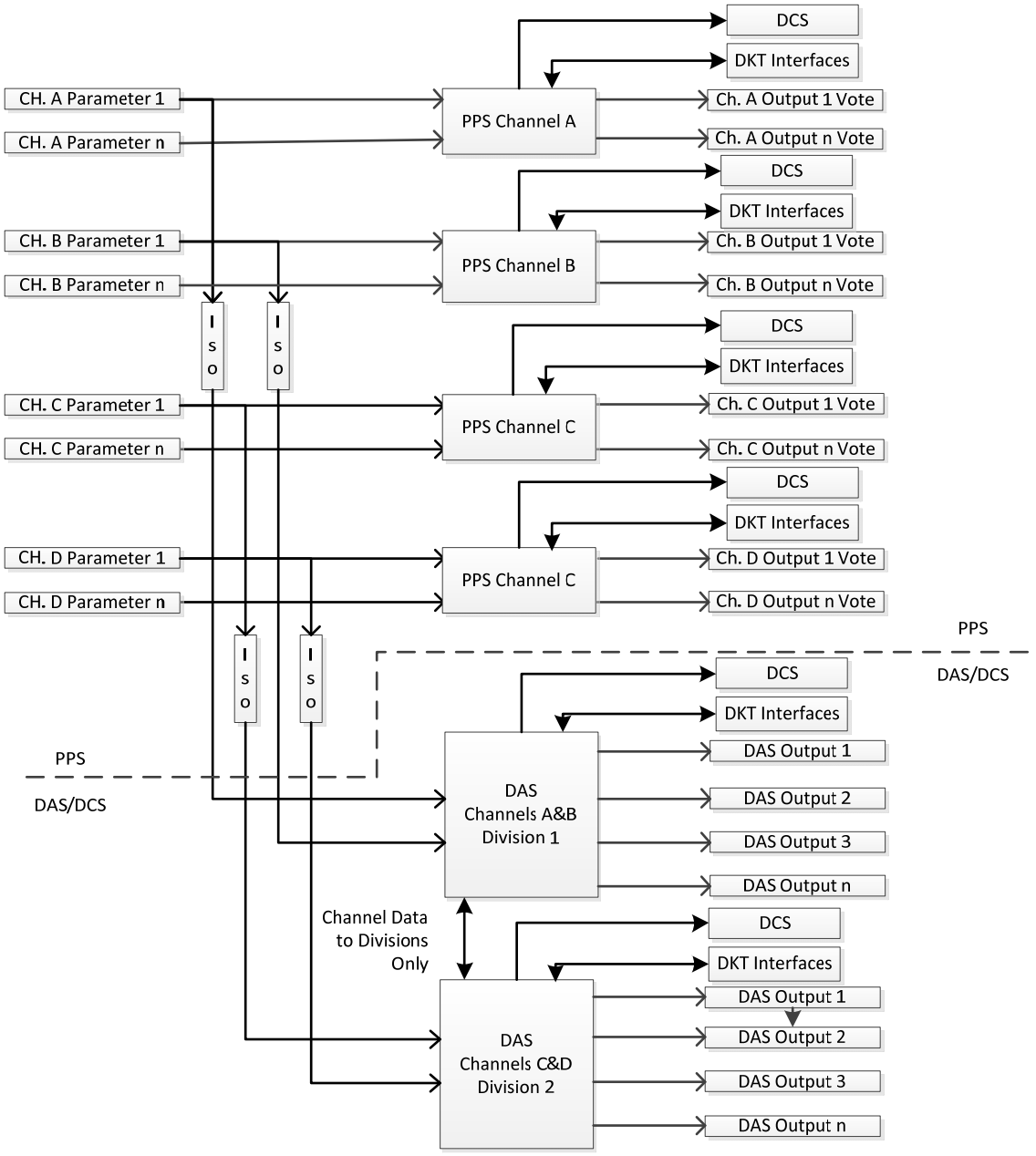

Figure 3-2. Modernized PPS and DAS Channels[2]

Each PPS channel within a PPS division will consist of one or more (if necessary) totally independent copies of the standard platform, although portions of the N4S design force each channel's application software to be different. The PPS channel in each platform will independently sample the required PPS channel-specific analog and discrete inputs hardwired to that channel. Each channel will independently convert the analog inputs to engineering units and compare the engineering units to the setpoint values for trip or actuations, implementing the required bi-stable function with preset hysteresis. Each channel will have no communication or

[2] Note that signal lines in this figure only connect where the lines terminate. Crossing lines are not connected.

knowledge of the actions or votes from the other three independent channels. Each channel will independently provide votes to scram or not scram, to isolate or not isolate, or to actuate or not actuate for each input. If multiple copies of the platform are necessary to implement channel functions, these separate platforms within that particular channel will communicate within each channel but will not communicate between independent channels. Each channel will communicate with all divisions.

If multiple copies of the platform are necessary to implement division functions, these separate platforms within each division will be able communicate to other platforms within the same division, but not between independent divisions.

The existing RPS, N4S, and ECCS had many sets of four-way redundant transmitters on the same instrument taps, calibrated with the same range, feeding identical trip units. To simplify the system, and to ensure that the PPS is working with a consistent set of process parameters, duplicate copies of multiple sets of four-way redundant transmitters will be eliminated, leaving one set of four-way redundant transmitters for each measured parameter used by all PPS functions. The LAR Framework Document does not include transmitter removal. Rather, the LAR Framework Document merely determines which transmitters will be retained. A separate Design Change will terminate the instrument tubing and determine a final disposition for the transmitters.

Each channel will convert the measured variables to engineering units. The actuation setpoint values will be in engineering units. The video generators and its associated interface (with the video generator and interface referred to as the DKT Interface) and data network will receive engineering unit values and status from the channels and actuation and other status from the divisions.

The modernized PPS will provide the same automatic and manual design functions as the existing equipment, with minor enhancements to the logic design and the elimination of no longer required manual switches with soft controls. The modernized design will also automate some manual actions to reduce the potential for human performance errors, as described in Sections 3.1.5, 3.3.1, 3.4.1, 3.4.4, and 3.8.5.

The design eliminates many existing RPS, N4S, ECCS, and DAS manual CR switches, while maintaining those switches that are required. The switches that will be replaced by soft controls include switches used for testing and manual operator actions that terminate conditions (e.g., resetting a scram). Retained switches will include those required for manual initiation and accident conditions defined in regulatory guidance. The ADS Inhibit switches are left as manual switches in the CR, to aid in post-accident use. SLCS Inhibit switches will be provided in the CR for maintenance.

The voting logic (i.e., divisions) will use the same platform. The divisions will modernize the existing timing relays and relay logic into software. Outputs from the divisions will be electronic single-failure tolerant solid-state switches, with diagnostics. The individual divisions will not communicate with each other and will operate totally independent of all other divisions. The design will provide individual functions (i.e., RPS, ECCS, and N4S) as separate tasks within the PPS platform environment. Individual subfunctions within ECCS and N4S may be designed as

separate tasks for ease of maintenance. For the PPS, the functions will be segmented into separate processors within the division only to the extent that the platform requires, based on the platform communication and logic loading and capabilities.

The existing RPS implements the more significant actuation logic as negative logic, where a logical low input signal represents a vote to scram, a logical low output signal initiates a scram or actuation, and the relay logic uses open (i.e., logical low) contacts to indicate a positive (i.e., true) logical signal.

All PPS software will use positive logic. Software inside the PPS will not lose signal power to elements within the logic-like functions built of individual trip units and relays. The PPS will detect faults and failures in software logic by ensuring that the software is running and that the software and configuration are not changed. There are no benefits to negative logic in digital implementations. The complexity of negative logic will be eliminated in the modernized design. The positive logic implementation will simplify the implementation (including design, review, and test) and maintenance tasks for the PPS software.

For those functions within the existing PPS that use negative (low true) logic, the modernized PPS design will convert negative logic contact closure inputs to a positive representation, perform all logic operations in positive logic, and only change the positive logic software outputs to negative logic at the point where the outputs are driven. The positive logic implementation simplifies the design, development, implementation, verification, validation, and maintenance tasks for the PPS software.

TBD/TBC 14: Negative logic is appropriate for relay-based implementations, where a loss of power or failed-open relay contacts result in appropriate protective action. The software inside the PPS does not lose signal power to elements within the logic like functions built of individual trip units and relays. There are no benefits to negative logic in digital implementations.

The modernized PPS depends on serial data communication. The issues identified in all items in DI&C-ISG-04 Section 1 (Reference 44) will be resolved using the information and requirements provided in DI&C-ISG-04 Section 1. The design will apply the guidance in DI&C-ISG-04, Rev. 1, Section 1, "Interdivisional Communications," to the communication from channels to divisions and communication between DKTs and channels/divisions. The design will apply specific emphasis on the "black channel" communications requirements listed in DI&C-ISG-04 Section 1, Item 12.

In order to implement PPS voting, as shown in Figure 3-3 below, all channels will have redundant, one-way communication links to each of the divisions. This figure shows the channel to division connections, which are not shown in Figure 3-2 above to minimize complexity. The channels will not provide the divisions with raw analog or discrete input data or with engineering unit data. There are two exceptions, described in Section 3.1.5, where the HPCI and RCIC turbine speed demand outputs require analog values, which will be provided to the division for use only in the HPCI and RCIC speed control algorithms. The channels will only provide the divisions with status information and votes to scram or actuate. The design will implement measures to ensure that the divisions use only valid data and detect the identified communication faults and failures (e.g., loss of communication on one link, loss of both links, restoration of one link, restoration of both links, different information between the links, different information in

the redundant information provided within a message from one link, etc.) found during design and implementation.

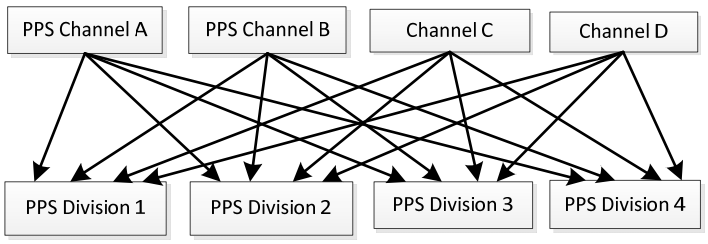

Figure 3-3. Modernized Channel and Division Communication

As shown in Figure 3-4 below, the PPS design will include two separate communication modules from channels to divisions, with redundant links split between the modules, to support the maintenance and replacement of a single failed module. Figure 3-4 provides implementation details for the functional signal flow shown in Figure 3-3. In all cases, each of the redundant communication links will be assigned to the same inputs (e.g., channel transmitter A to division receiver A and channel transmitter B to division receiver B) to simplify troubleshooting and diagnostics. To ensure that the same information is provided to all divisions, a passive splitter will be used to divide the output signal for input to the divisions and to the DCS. This design will eliminate the potential for channels to transmit different messages to the divisions or fail to transfer messages to some of the divisions. This design also simplifies the hardware, by eliminating multiple communication link modules from the channels.

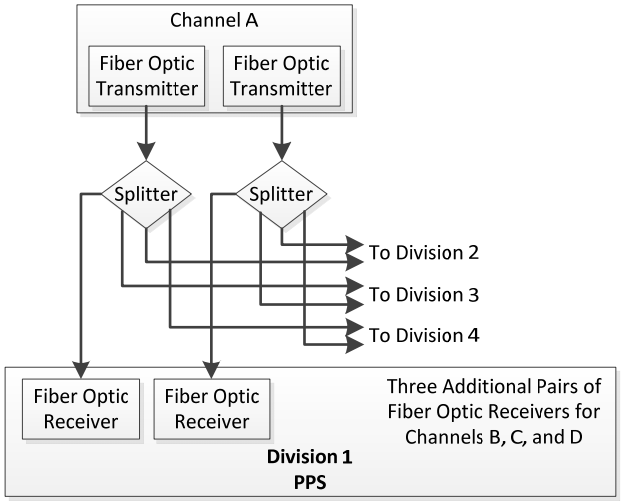

Figure 3-4. Redundant Channel and Division Communication Links

In the existing system, there are bi-stables and relay logic in one system that immediately pass data to another system. In the modernized PPS, any functionality associated with a system will be designed into the system. As an example, in the existing system, high-high radiation on the main steam lines passes through an RPS trip module and is used in N4S. All bi-stables and logic that are installed in the RPS, N4S, or ECCS cabinets will be removed by this modernization. The design will implement any remaining bi-stables and logic that are not assigned to the RPS, N4S, or ECCS in a standalone function within the overall PPS design. This standalone function

will be documented in the PPS systems, hardware, and software documentation and implemented using the same software lifecycle processes as the main PPS systems.

The PPS design will consider all the existing meters, recorders, indicating lamps, and annunciator windows in the CR that provide RPS, N4S, and ECCS data. The design will eliminate those meters and recorders associated with the RPS, N4S, and ECCS functions and provide the data on PPS and DAS DKTs (see Sections 3.3.5 and 3.4.5), which will provide the indications required to support abnormal and emergency procedures, including compliance with the version of IEEE Std. 497 (Reference 45) to which LGS is committed. The design will replace the lamps and annunciator windows with continuously visible video data displays. The design will provide continuously visible data in the CR for all required PPS and DAS data, including bypassed information and status information, on video displays. Where possible, the design will eliminate the existing lamps and annunciator windows used to provide status information to the watchstanding Reactor Operator (RO) and Senior Reactor Operator (SRO), to the extent allowed by regulation. LGS will add administrative controls that require the watchstanding operators to agree on one or more video display(s) to display this information and ensure that the appropriate display or displays containing that information are always displayed in the CR.

For the modernized PPS, the primary PPS indication in the CR and in the AER will be through the video displays of the DKTs. The DKTs will be appropriately distributed and accessible throughout the CR and in the AER. For this modernization, DKTs will provide RPS, N4S, and ECCS information, with the intent that eventually all safety-related and non-safety system information (including the DAS) will be available on each DKT. DKT locations will be defined based on Human Factors Engineering (HFE) analyses, close to the manual controls used by the watchstanding RO and SRO. As defined in Section 3.3.5, the DKT installed location will determine whether the user can issue commands that control the safety-related and non-safety functions (i.e., initiate, bypass, terminate, start, stop, open, close). The CR will still maintain the functionality of the remaining individual meters and recorders required by various regulations or analyses, including for post-accident use.

The CR display of BISI on DKTs will eliminate the separate lamp-based scram, status, and bypass indicators and annunciator windows. A continuously visible video display will be provided but not on a dedicated display. The continuously visible display in the switched DKT environment will be an administratively controlled function, where the SRO will be required to maintain at least one, and preferably two, CR DKTs displaying BISI data. BISI data will also be available on the non-safety related data network. The HFE process may determine that one or two large displays can replace existing annunciator windows, making BISI data accessible in one overhead location. The modernized DKT design will provide the ability to move the BISI data to a working DKT, if one or both of normal displays are unavailable, which will provide the required continuously visible regulatory requirement even during equipment failure.

The modernized design will reuse the existing cabinets and field wiring terminations in the AER for the logic solvers, along with consolidating the separate systems in the PPS. The design will include remote data acquisition in the CR, to acquire the field status information that is wired only to the CR. The LAR Framework Document provides the rationale for individual design

requirements to support individual RPS, N4S, and ECCS functions, which is provided in subsequent LAR Framework Document sections.

The modernized design will provide the watchstanding RO with the ability to bypass one entire PPS channel for maintenance using a hardwired switch in the CR, leaving the other three PPS channels in operation. The modernized design will also provide the ability to bypass any input to the PPS individually, using soft controls on the Human-System Interface (HSI). The modernized design will automate the insertion and removal of all operational bypasses in the logic, as is done in the existing systems. The PPS will provide all channel- and division-specific bypass status to the DCS, where the DCS software will compare the operational bypass and maintenance bypass status across channels and divisions and annunciate persistent differences for resolution. The modernized PPS will provide sensor bypass and maintenance bypass capabilities at the channel level. The modernized PPS will eliminate most of the periodic TS surveillance test requirements through self-tests and self-diagnostics, as described in Sections 8.1 and 8.2.

The modernized PPS and DKT system will use the electric power sources provided for the existing RPS, N4S, and ECCS. The modernized PPS design, like the existing RPS, N4S, and ECCS, will use only electricity for power.

3.1.3 Modernized RPS Function in PPS (DI&C-ISG-06 D.2.3)

The modernized RPS safety functions will be unchanged from the existing RPS. The modernized RPS will monitor the same points that the existing RPS monitors. The modernized RPS will replace analog trip units and relays with software. The RPS voting structure will be modernized, and the channels and divisions will remain clearly separated.

The SSPV and Backup scram solenoid valves will not be altered, and both the A and B channel valves will be required to change to the venting state to insert the control rods. As in the existing system, the modernized PPS will be normally energized with control rods withdrawn and de-energize to scram. The modernized PPS will de-energize the RPS outputs on faults or failures within the platform hardware.

Unlike the existing RPS, the modernized RPS divisions each will consider each of the specific votes to scram provided by all four channels (not just the two channels in the division) and will perform a 2oo4 vote on each specific vote to scram. Thus, the modernized RPS will require two or more similar sensors in any of the divisions to exceed the setpoint value before initiating a scram. The modernized RPS will eliminate half scrams based on one sensor failing in one division but cannot eliminate half scrams associated with events such as divisional power failure. Sharing four channels of data and requiring two or more of the same sensor to exceed the setpoint value will eliminate the potential for a single sensor failure to initiate a half scram or for two random sensor failures to initiate a full scram.

The modernized PPS design will provide the end-of-cycle (EOC) recirculation pump trip (RPT) described in Section 3.2.1.7, as described in the context of the existing system. The EOC-RPT trip uses separate controls than non-safety related RRCS RPT trip described in Sections 2.1.4 and 3.1.6.

The modernized design will provide the anticipatory turbine trips for TSVs and TCVs described in Section 3.2.1.7, as described in the context of the existing system

The CR DKTs will provide the RO and SRO access to the complete RPS engineering unit and alarm data. The DKTs will provide meaningful descriptions and values for all data. The N4S data will also be available in the non-safety related DCS and saved as long-term historical data.

The setpoint values for the modernized RPS will be recomputed based on the uncertainties in the modernized platform, using approved methods.

3.1.4 Modernized N4S Function in PPS (DI&C-ISG-06 D.2.3)

The modernized N4S safety functions will be unchanged from the existing N4S. The N4S voting structure will be modernized, and the channels and divisions are clearly separated, as explained in the N4S architecture.

For the existing N4S, there are four sensors, fed into two independent channels within each division. For the modernized N4S, all four channels will provide data to all four divisions. For each set of sensors, the application software will implement 2oo4 voting within each division. Since the divisions will be working with the same votes to isolate, the divisions work as two independent parts of a single unit. Each channel implements the logic required to sample the inputs provided to that channel. Each division implements the logic required to drive the isolation outputs, based on selecting appropriate data from the channels.

The N4S voting will be similar to the RPS, using all data from all channels (i.e., bi-stables) to all divisions (i.e., voting logic), to ensure that no half-isolations occur, just like the RPS ensures that no half scrams occur from software logic. If an inboard valve isolates, then the outboard valve will also isolate, based on the modernized architecture and logic. The difference between the N4S voting is dependent on the risk associated with the function, as shown in Table 3-7 below. The existing sensors are retained, and voting is limited by the field sensing to that provided in the currently LGS licenses. Voting will range from four-out-of-four (4oo4) through 2oo4 down to one-out-of-one (1oo1). Some of the limited, unchanged, existing 1oo1 actions are implemented in logic in the field, with only the status fed back to the CR and thus into the N4S.

For some of the N4S subfunctions, there are two sensors, fed into the independent channels within a division. For those sensors, 1oo2 voting will be provided within the division, as there is no reason for the other division to vote on actuations which the other division cannot control. In order to meet the single-failure criterion, the single division will be split into two autonomous subdivisions, with each subdivision voting and controlling either the inboard or outboard isolation.

The LGS UFSAR (Reference 41) describes seven N4S functions. The eight isolation groups will implement the seven functions described in the UFSAR and Table 3-5 below, which also documents the existing subdivision of the eight isolation groups necessary to fulfill the required seven functions. Groups I through VI are implemented in Functions 1 through 6, respectively. Group VII is implemented in Functions 7 and 8. The modernized PPS will retain the isolation functions and isolation groups but will replace the analog trip units and relay logic with analog inputs, discrete inputs, application logic, and discrete outputs in the vendor platform. Internally,

the divisions will be segmented such that the logic or hardware failure of a division does not disable both the inboard and outboard isolation.

To resolve the identified issues with the existing four divisions of NUMAC LDS chassis, the four divisions of NUMAC chassis functions will be incorporated into the four channels in the modernized N4S. The Type T Copper Constantan thermocouples and cold junction compensation of the thermocouple inputs from the existing NUMAC chassis will be sampled in the N4S, converted to engineering units, compared to alarm limits, and alarmed in the CR. The RWCU differential pressure inputs will also be sampled, converted, compared, used appropriately, and alarmed.

The CR DKTs will provide the RO and SRO access to the complete N4S engineering unit and alarm data. The DKTs will provide meaningful descriptions and values for all data. The N4S data will also be available in the non-safety related DCS and saved as long-term historical data.

The setpoint values for the modernized N4S will be recomputed based on the uncertainties in the modernized platform, using approved methods.

3.1.5 Modernized ECCS Function in PPS (DI&C-ISG-06 D.2.3)

The modernized ECCS safety functions will be unchanged from the existing ECCS. The ECCS voting structure will be modernized, and the channels and divisions will be clearly separated, as explained in the ECCS architecture. This will change the operation of the ECCS away from a design where Division 1 and Division 2 initiate separately by one of the two channels in the division, indicating the need for an actuation. The modernized design will ensure that all divisions initiate when needed.

The ECCS voting will be the same as the RPS, using all data from all channels (i.e., bi-stables) to all divisions (i.e., voting logic), to ensure that the ECCS implements emergency core cooling consistently in all divisions through software logic.

For the existing ECCS, there are four sensors, fed into two independent channels within each division. For the modernized ECCS, all four channels will provide data to all four divisions. For each set of sensors, the application software will implement 2oo4 voting within each division. Since the divisions will be working with the same votes to actuate, the divisions work as two independent parts of a single unit. Each channel implements the logic required to sample the inputs provided to that channel. Each division implements the logic required to drive the actuated outputs, based on selecting appropriate data from the channels.

The CS function initiates the four EDGs. The four sets of EDG initiation logic are implemented in time delay relays and logic in the ECCS cabinets. The modernized PPS will absorb those functions into the ECCS application software. For modularity reasons, the EDG initiation logic are separate functions within the PPS.

For HPCI and RCIC, the existing Flow Indicating Controllers (FIC) will be replaced by modernized logic. In an accident condition using the existing systems, the ROs manually control the operation of HPCI or RCIC to maintain Reactor Vessel Pressure, Reactor Vessel Water Level, or flow into the reactor. Additional ECCS software for the HPCI and RCIC will provide

the operator a selection of Reactor Vessel Pressure, flow, or Reactor Vessel Water Level control, which will then be maintained automatically by the PPS application software. In order for the divisions implementing the new control algorithms to function, the required engineering unit data will be provided to the divisions that implement the HPCI and RCIC speed demand controls for purposes of the speed controls only. No other use will be made of that data.

The HPCI and RCIC control equipment in the CR will be replaced, including the flow controller, square rooter, power supplies, control, alarms, and indications. The field equipment mounted in the HPCI/RCIC room and in the Elevation 210 HPCI cabinet is not affected. The Woodward governors, including power supplies, ramp generators, signal converters, electric governor magnetic pickup, magnetic speed pickup, bias speed setting potentiometer, electric governor-remote hydraulic actuator, and remote servo are not changed or modified by this modernization.

The CR DKTs will provide the RO and SRO access to the complete ECCS engineering unit, status, and alarm data. The DKTs will provide meaningful descriptions and values for all data. The ECCS data will also be available in the non-safety related DCS and saved as long-term historical data.

Local control actions will not be affected. As examples, the CS Pump Room Fans retain their existing automatic fan controls. The CS pump minimum flow controls are retained unchanged.

For RHR, the LPCI mode was already automated in the ECCS. The automation provided supports the operator, in that the operator uses soft controls on video displays to initiate functions. The automation does not replace the operator, who is still required to initiate an operator-defined function. To eliminate manual operator actions for a very complex system, all retained modes of RHR operation will be automated and initiated by the operator using soft controls within the PPS, which checks interlocks and manipulates the pumps and valves in the RHR system to set the RHR into the RHR mode selected by the operator and start or stop that mode based on operator commands. By automating setup of all safety-related and non-safety RHR modes, the potential for human performance error is reduced.

The CR DKTs will provide the RO and SRO access to the complete ECCS engineering unit and alarm data. The DKTs will provide meaningful descriptions and values for all data. The N4S data will also be available in the non-safety related DCS and saved as long-term historical data.

The setpoint values for the modernized ECCS will be recomputed based on the uncertainties in the modernized platform, using approved methods.

3.1.6 Modernized DAS (DI&C-ISG-06 D.2.3)

The modernized non-safety related DAS is shown in Figure 3-5 below. The modernized DAS will perform the same ATWS functions as the existing safety-related RRCS, but the DAS will use an AQ, non-safety related DCS instead of the safety-related RRCS-specific equipment. AQ is required to maintain compliance with 10 CFR 50.62 (Reference 8). The LGS expectations for AQ are defined in the Vendor Oversight Plan for the non-safety related DAS in Section 5.2. The analog isolators that serve as the interface between the PPS field sensors and the DAS are shown in Figure 3-2 above.

The N4S and ECCS functions will be analyzed in the PPS D3 Analysis (Reference 7). Only the N4S and ECCS functions that the D3 Analysis requires in the DAS will be designed into the DAS. The ATWS function will be incorporated in the DAS in a future project.

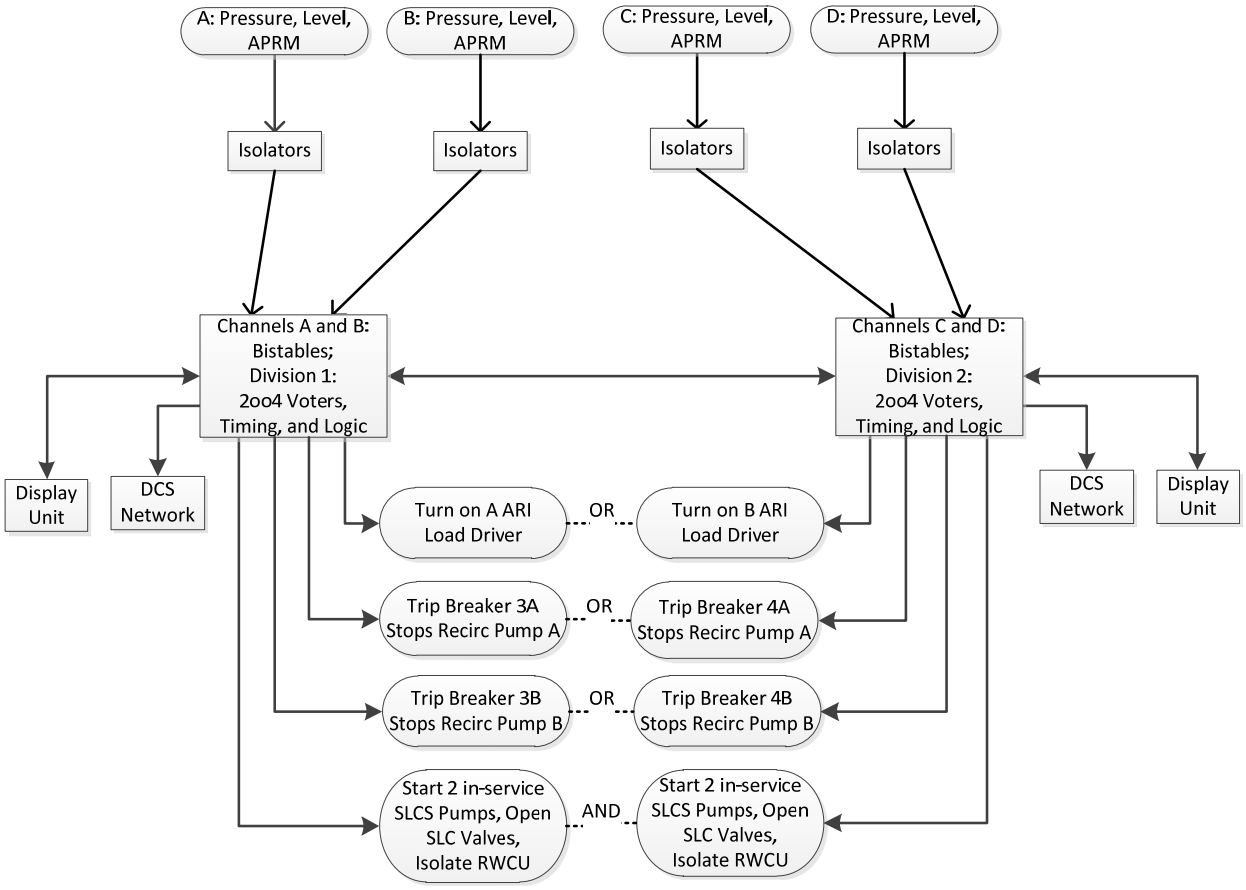

Figure 3-5. Modernized ATWS Portion of DAS

The DCS selected has been demonstrated through use to be highly reliable. The ATWS function (i.e., DAS function in the DCS providing diversity for the RPS function) will be incorporated into the DAS in a separate project. This modernization incorporates selected N4S and ECCS functions into the DAS function in the DCS. This modernization will leverage the DCS reliability and reduce the burden on operations and maintenance that exists for the obsolete RRCS, which the ATWS function in the DCS will replace. The self-test features in the existing design have proven to be sources of faults and failures in the existing RRCS. The self-test and diagnostics features to be provided in the DAS function are known working, proven-in-use features that already exist in the DCS platform.

The DAS function design will use the same voting scheme as the PPS systems that the DAS function backs up. The modernized design will segment two sets of channel functions and one division function into one DCS processor, duplicate the channel and division functions in a segmented DCS processor, use the DCS data connection between divisions to share all channel data between the two division functions, and vote independently.

The modernized design ensures that, like the PPS, votes to trip or actuate will be generated only when four channels to agree similar conditions exist. As an example, the ATWS function will require four high Reactor Vessel Pressure signals, four low Reactor Vessel Water Level signals, or both high pressure and low water level to exist, to initiate the ATWS function.

Using ATWS as an example, each functional software ATWS channel in each of the two DCS segments will read the one set of analog signals, appropriately externally isolated, used by the PPS for Reactor Dome Pressure and Reactor Vessel Water Level, as well as the APRM power level. Each ATWS software channel will make an independent decision concerning pressure, independent decision concerning water level, and independent decision concerning neutron power. The ATWS divisions cross-share only the software channel votes and channel status. If either ATWS division determines that protective action is required based on individual voted 2oo4 evaluation of Reactor Dome Pressure and Reactor Vessel Water Level, then each ATWS division starts implementing the protective actions. Either ATWS division can initiate ARI and reactor recirculation pump trips. The ATWS outputs do not require Equipment Interface Module (EIM) isolation, since the ATWS outputs are diverse from the RPS outputs, with the only commonality between RPS and ATWS being field sensors and APRM measurement chassis.

The modernized non-safety related DAS for the N4S and ECCS is shown in Figure 3-6 below. All application software for the modernized DAS will be designed, developed, implemented, reviewed, and tested using the AQ requirements. The LGS expectations for AQ for the DAS are defined in the Vendor Oversight Plan for the non-safety related DAS in Section 5.2.

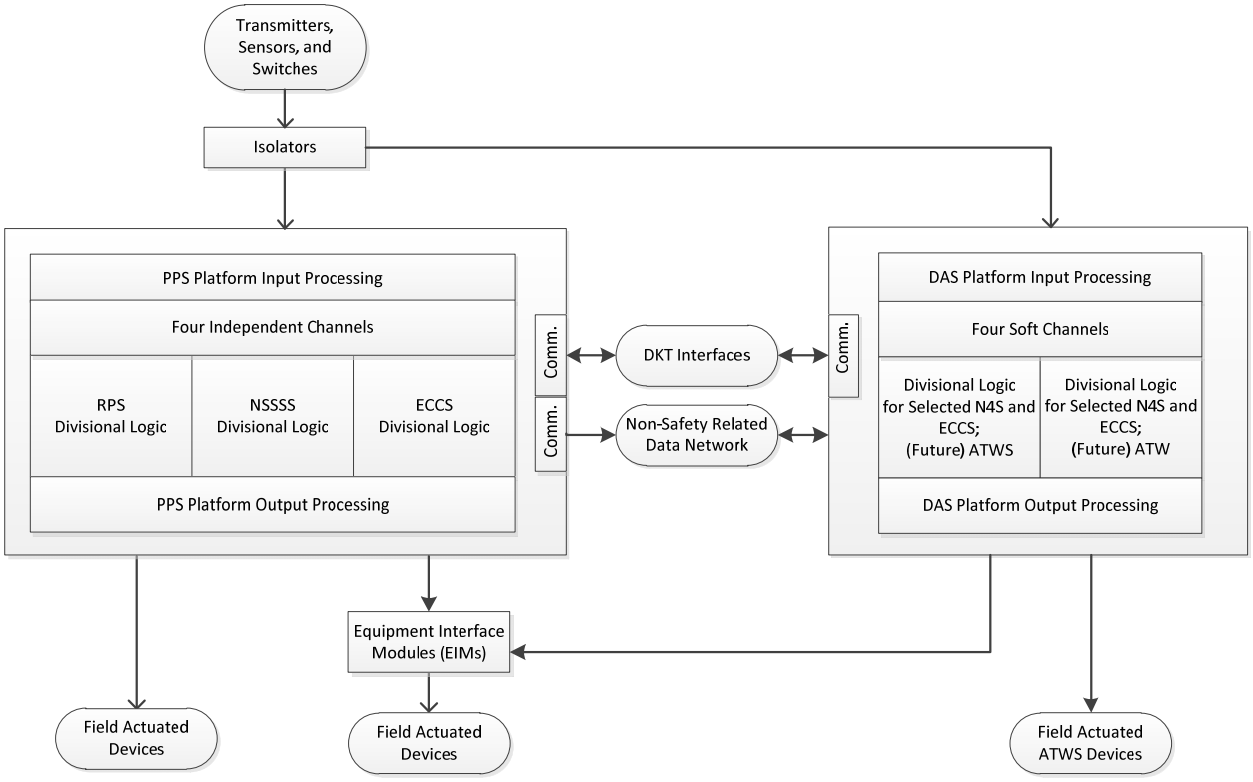

Figure 3-6. Modernized DAS for Future ATWS and Selected Portions of N4S and ECCS

The DAS for the N4S and ECCS will use the same field inputs, setpoint values, software logic including modernized voting scheme, and outputs as the modernized PPS design. The N4S and ECCS will be implemented completely in the PPS. The D3 Analysis (Reference 7) will require portions of the N4S and ECCS to be duplicated in the DAS function. The PPS and DAS function portions of the N4S and ECCS will require priority logic to ensure correct operation of the safety systems. The common EIMs will be used by both the N4S and ECCS portions of the PPS and by the DAS for the required safety-related discrete outputs to the controlled safety-related equipment. The ATWS portion of the DAS function does not require EIMs, since the controlled outputs are all diverse from those used by the RPS function of the PPS.

3.1.7 Automation of Channel Checks (DI&C-ISG-06 D.2.3)

Manual channel checks are used to detect issues with field instruments or analog trip units across redundant sensed variables. These labor-intensive manual channel checks are being replaced with automation to provide the rapid detection of calibration or drift in redundant sensed variables. Automating this function provides a set of data from a single point in time, rather than spread across the roughly two hours required to gather manual data and eliminates significant labor on review and data retention.

The PPS and DCS will provide automated channel checks for the rapid detection of issues with field transmitters or PPS analog inputs, compensating for the reduction in the number of duplicated field transmitters. The PPS will provide the safety-related data, which operators currently collect manually, to a non-safety related computational server in the DCS. The DCS will retain the data in a long-term non-safety related historian. Continuously, non-safety related software in the DCS will compare the redundant data from all channels and divisions as well as from the DAS and alarm on persistent error outside the calibration error band. This automation will eliminate the manual operator channel checks function from the TS, based on automating this function. No printed or signed reports will be prepared. The non-safety related comparison will be alarmed in the CR when errors are detected. The long-term historian retains all data, along with alarms and selected status.

TBD/TBC 15: Project team to establish data lists during detailed design

3.2 EXISTING RPS, N4S, ECCS, AND RRCS ARCHITECTURE (DI&C-ISG-06 D.2.1)

The physical and functional architecture of the existing RPS, N4S, ECCS, and RRCS I&C features are documented in subsequent LAR Framework Document sections. These sections also document where the proposed plant modifications would impact the existing features, as applicable.

A single line drawing, Figure 3-7 below, shows an example of an existing transmitter, sensor, or switch feeding the analog trip unit (bi-stable) or discrete input on the channel. The channel provides a vote to scram or actuate to the relay logic in the voter, which may also combine additional inputs to determine if the protective action is required. In this design, primarily set up to implement 1oo2 taken-twice voting, no data crosses the boundary between electrical divisions. The channels consist of third-party implementations of the Rosemount 510 and 710 analog trip

units. Relay logic in the voters is built of pneumatic time delay relays and relay logic. The CR has limited display of input data, no visibility into the internal decisions inside the trip units or relay logic, and limited visibility into the actual state of the in-field actuated devices.

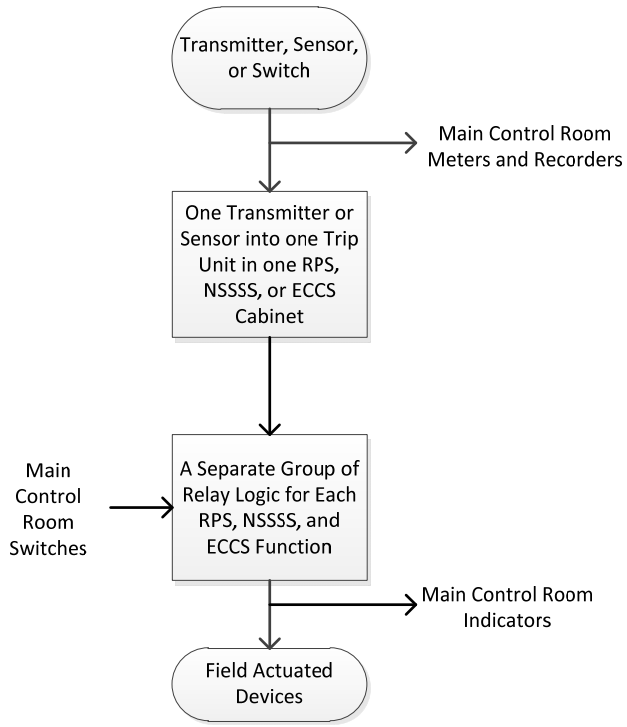

Figure 3-7. Existing RPS, N4S, and ECCS Architectural Detail

This simple bi-stable and relay logic of Figure 3-7 is duplicated to implement the existing RPS, N4S, and ECCS as separate systems. The design includes two logical groups of bi-stables in each of the two electrical divisions. For the RPS and ECCS, as well as a significant part of the N4S, the scram and actuation outputs are voted in the field actuated hardware, which requires both divisions to request a scram or an actuation before the field equipment performs the requested action. The N4S has additional voting schemes, which are explained later in the LAR Framework Document.

3.2.1 RPS Existing Architecture (DI&C-ISG-06 D.2.1.1)

The current RPS scram functions are carried out using an analog I&C architecture that consists of trip units, wiring, relay logic, and output devices that interface with various other equipment in the RPS and other plant systems. As shown in Figure 3-8 below, a scram signal generated by the RPS de-energizes a pair of SSPVs on each of the individual control rod drive mechanisms (CRDMs). When power is removed from the pair of SSPVs, exhaust air is ported from the scram valve air actuators causing the control rods to insert into the core. Control rods are hydraulically driven into the core through the use of CRDMs which are discussed further below.

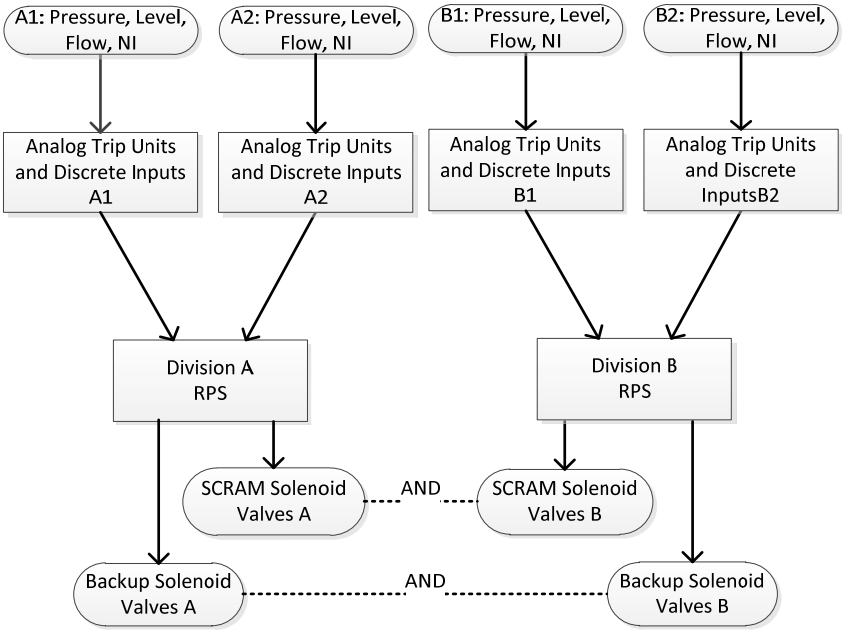

Figure 3-8. Existing RPS System Signal Flow

Each LGS unit uses 185 control rods and corresponding CRDMs to provide control over reactor power during normal plant power changes and in the event of a reactor scram. The 185 CRDMs are split into four groups. Each control rod is provided with a CRD Hydraulic Control Unit (HCU), which interfaces with the SSPVs to support control rod scram functionality. The two SSPVs shown in Figure 3-9 below de-energize upon receipt of a scram signal in their respective RPS divisions. This is executed using the K14 contactors in the RPS (discussed further below in Section 3.2.1.1). Note that de-energizing only one SSPV (a half scram) does not result in control rod motion, as instrument air is still ported to the air actuators through the remaining SSPV.

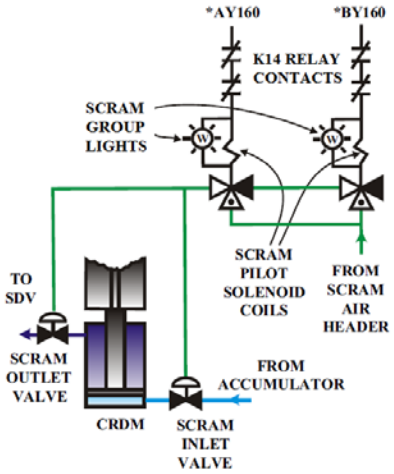

Figure 3-9. RPS Interface with CRD System (Reference 46)

The RPS also includes a backup to the 185 pairs of CRDM SSPVs. When both Division A and Division B logic strings de-energize (i.e., both SSPVs are de-energized), backup scram SOVs are concurrently energized. Energizing the backup SOVs provides a diverse method of venting the scram air header and opening the scram valves associated with each CRDM. If no SSPVs operated, the backup SOVs ensures all control rods are inserted by venting the scram air header. However, insertion of all control rods using this method is slower than when the individual SSPVs are used to insert each control rod.

A reactor scram also results in the isolation of the SDV. The SDV provides a contained location for the reactor coolant, which is normally contained in the over-piston area associated with each CRDM (shown in Figure 3-9). This over-piston volume is forced out during a scram when the control rod is inserted. As indicated in Table 3-3 below, high water level in the SDV is an automatic RPS scram signal. This scram signal is generated to ensure that control rods are inserted prior to the SDV filling up to the point at which it would have insufficient volume to accept the over-piston fluid.

3.2.1.1 RPS System Design Functions

The RPS has two functions: scram initiation, and uninterruptible 120 VAC power sourcing. The alignments that support each function are discussed below. The RPS provides a scram initiation signal to the CRD System through the CRD HCUs when the system is manually or automatically initiated. The RPS also provides uninterruptible 120 VAC power for specific instrumentation in various systems, whose signal outputs go to the RPS and to certain N4S isolation logic or whose functions must be immune to short power losses.

The RPS is required to be operable during all plant operating conditions (OPCON) when fuel is in the RPV (OPCON 1 through 5). These include Power Operation (OPCON 1), Startup (OPCON 2), Hot Shutdown (OPCON 3), Cold Shutdown (OPCON 4), and Refueling (OPCON 5).

The existing logic associated with the automatic scram function from the RPS relies on a 1oo2 taken-twice arrangement. In general, there are four channels associated with each of the plant parameters above which are consolidated further into two divisions, each having two channels. A full scram and reactor shutdown occurs if one of the channels in each division exceeds the preestablished setpoint required for a shutdown. This logic is slightly different for the MSIV and TSV scram functions, which rely on limit switch inputs to the system and not a process parameter (e.g., pressure, level). Manual interfaces with RPS are provided for operators to initiate a reactor shutdown, if required.

Figure 3-10 below shows the existing RPS as a signal flow. In this figure, the outputs of the existing RPS analog trip modules are shown as inputs to the two divisions. Each of the individual trips from the channels is provided to a "voter," which implements a logical OR of the input signals. Any trip from Channels A1 or A2 (Division A) along with any trip from Channels B1 or B2 (Division B) initiates a plant scram. There is no requirement for the two votes to trip to be the same plant parameters; this can (and has) resulted in full reactor scrams caused by noncoincident trip signals occurring in both divisions. Trips 4–9 are the same

as Trips 1 through 3 but not shown to simplify the diagram. The NUMAC 2oo4 voters for each channel provide dual nuclear instrumentation trips to the channels as discrete inputs.

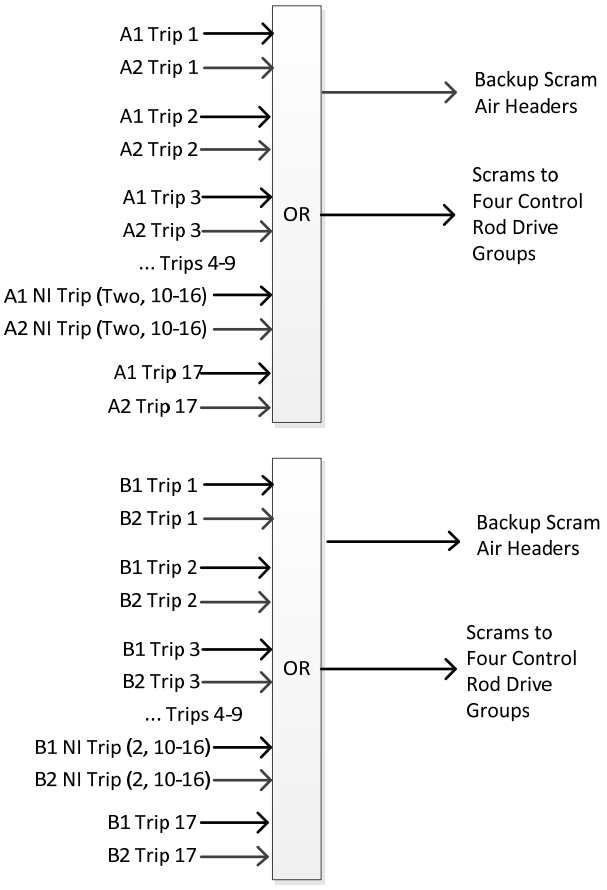

Figure 3-10. Existing RPS Plant Scram Logic

To provide additional granularity regarding the architecture described above, the four divisions are represented in Figure 3-11 below according to their standard logical arrangement. The "Scram Parameter Contacts" pointer indicates where receipt of a scram signal would result in the de-energization of the associated channel (A1, A2, B1, or B2). The relationship between the K14 contactors and CRDMs was shown previously in Figure 3-9 above, where de-energizing the appropriate pair of K14 contactors results in control rod insertion.

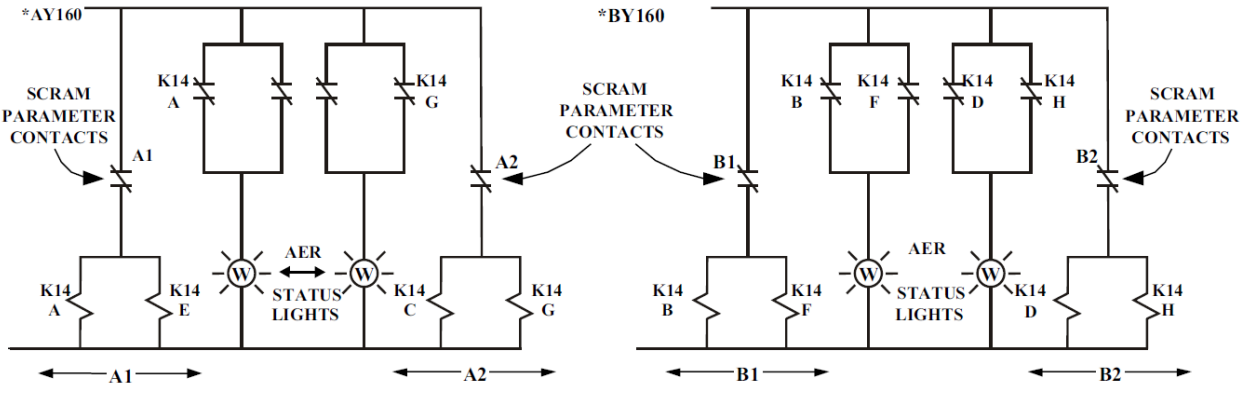

Figure 3-11. General Overview of LGS RPS Circuitry (Reference 47)

An example of one channel of automatic scram logic is provided Figure 3-12 below. As shown in the figure, the various automatic scram signals (and manual scram interface) are primarily arranged in series. Receipt of a scram signal in the associated channel's logic ultimately de-energizes the K14 contactors to insert the associated control rod group, provided that the logic on the opposite division is also satisfied. The figure below also illustrates the current method uses to reset a scram signal, which is reliant on a 10-second-reset lockout delay and ensuring that the initiating scram signal is clear (i.e., the scram cannot be reset until the initiating condition no longer exists).

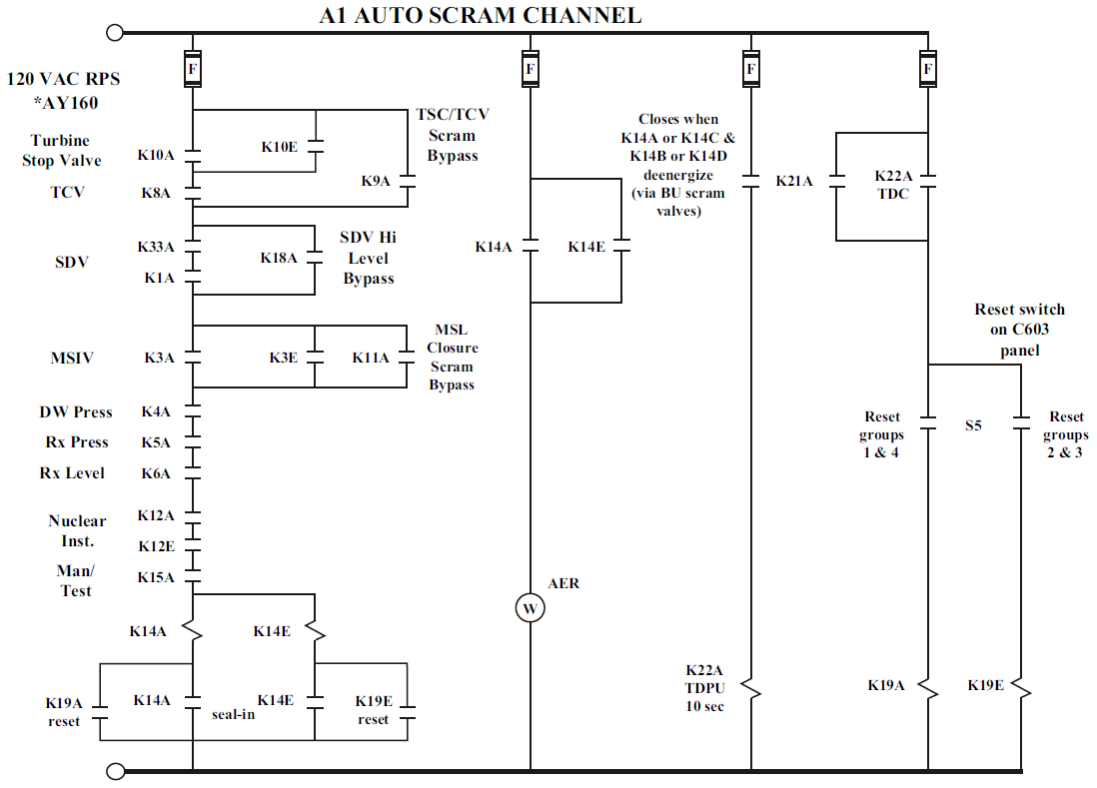

Figure 3-12. Current LGS RPS Automatic Scram Logic (Channel A1) (Reference 48)

The proposed modifications to the existing RPS will not modify any aspect of the system as it relates to the CRD System interface. However, the K14 contactors will be replaced with alternative drivers capable of de-energizing the 185 pairs of SSPVs. Analog logic upstream of the K14 contactors will be replaced in its entirety by application software capable of executing the logic previously described.

Scram Initiation

The RPS provides the scram initiation signal to the CRD System, either automatically when any of the monitored parameters exceed a preestablished value or by manual initiation. Table 3-3 below defines the parameters monitored by the RPS to determine whether automatic system initiation and a subsequent reactor scram are warranted. If a scram is generated in the RPS based on a setpoint value configured in the RPS, that setpoint value is shown as "[setpoint]" in the table to avoid duplicating setpoint values in multiple parts of this LAR Framework Document. If the setpoint is generated externally, then the current external value is provided in the table.

Table 3-3. RPS Reactor Scram Conditions

Trip	Signal and Condition	Condition	Bypass
1.	Manual Scram switches pressed	Operator decision, 1oo2 taken twice, one switch for each channel	No Bypass. Internal timed reset inhibit for 10 seconds after scram
2.	Reactor Mode Switch in Shutdown	Operation decision	No Bypass. Internal timed reset inhibit for 10 seconds after scram
3.	TSV Closure	3oo4, TSVs <95% open A1=TSV3&TSV4; A2=TSV1&TSV2; B1=TSV1&TSV3; B2=TSV2&TSV4 Scram function is accomplished by limit switches on each valve	Operational bypass if reactor power <[setpoint], based on turbine first stage pressure <[setpoint]
4.	TCV Fast Closure	1oo2 taken twice	Same as TSV Closure Trip
5.	SDV High Water Level	1oo2 taken twice for four float switches; 1oo2 taken twice for four level transmitters, >[setpoint] gallons	Valve lockout bypassed with Reactor Mode Switch in (Shutdown OR Refuel) AND SDV High Level Bypass Keylock Switch in Bypass (Bypass allows post-scram draining of SDV)

Table 3-3. RPS Reactor Scram Conditions

Trip	Signal and Condition	Condition	Bypass
6.	MSIV Closure	Inboard or outboard valve closure in 3oo4 Main Steam Lines, detected by not full open (<8% closed) limit switches. Trip only if inboard or outboard valve is not full open on three or more Main Steam Lines. All logically OR the inboard and outboard valve conditions. A1=MSIV A and MSIV B; A2=MSIV C and MSIV D; B1=MSIV A and MSIV C; B2=MSIV B and MSIV D;	Bypassed with Reactor Mode Switch not in Run
7.	Drywell High Pressure	>[setpoint] psig	None
8.	RPV High Pressure	>[setpoint] psig	None
9.	RPV Low Water Level	<[setpoint] inches	None
10.	Average Power Range Neutron Monitor (APRM) Upscale, Flow Biased, Simulated Thermal Power	Scram occurs if any two APRM channels exceed the following: High power, clamped at 116.6% Two loop: 0.65*(% Recirculation total drive flow)+61.7% One loop: 0.65*(% Recirculation total drive flow-7.6%)+61.5% APRM and OPRM trip function is accomplished by four APRM 2oo4 Logic Modules (“Voters”), which each use all four APRM inputs. Each pair (single-failure tolerant) of voter outputs is sent to one of four RPS channels	No bypass in RPS APRM/OPRM and voter logic unchanged: Bypassed with Reactor Mode Switch not in Run
11.	APRM Upscale, Setdown	Scram occurs if any two APRM channels exceed 15% reactor power with Reactor Mode Switch not in RUN	No bypass in RPS APRM/OPRM and voter logic unchanged: Bypassed with Reactor Mode Switch in Run
12.	APRM Neutron Flux Scram	Scram occurs if any two APRM channels >118.3% reactor power with Reactor Mode Switch in RUN OR >15% with Reactor Mode Switch not in RUN	APRM voter logic unchanged
13.	APRM INOP	Scram occurs if any two APRM are inoperative	No bypass in RPS APRM/OPRM and voter logic unchanged: A single inoperative APRM can be bypassed

Table 3-3. RPS Reactor Scram Conditions

Trip	Signal and Condition	Condition	Bypass
14.	Oscillation Power Range Monitor (OPRM) Upscale	Channel in enabled region (≥29.5% APRM STP, AND <60% recirculation drive flow) AND any two OPRMs reach or exceed the Upscale Trip setpoint values	No bypass in RPS APRM/OPRM and voter logic unchanged: • Bypassed with Reactor Mode Switch not in Run • Bypassed outside of the enabled region
15.	Intermediate Range Neutron Monitor (IRM) Upscale	1oo2 taken twice, >120/125 of scale	Bypassed with Reactor Mode Switch in Run
16.	IRM Inoperative (INOP)	1oo2 taken twice	Bypassed with Reactor Mode Switch in Run
17.	Noncoincident Neutron Monitoring	Any single Source Range Neutron Monitor (SRM), IRM, or APRM channel trip causes scram	Bypassed by jumper if not in startup testing

Trip 17 above is no longer used in the existing plant and has been removed from all procedures. The unused function will be removed as part of this modernization, to simplify the application software. The strongest-rod out determinations are made analytically, eliminating the need for the function for empirical strongest rod-out testing, which is disabled by the normally inserted shorting links.

For all scrams, a 10-second-reset inhibit timer ensures that the control rod insertion completes, requiring the timer to timeout before the RO can reset the scram.

Scrams are inhibited when volume inputs from the SDV to the RPS indicate that insufficient volume remains to hold the water from the reactor coolant system that results when the control rods are inserted.

When a scram occurs, power is removed from the four groups of SSPVs in each division, power is removed from the SDV Vent and Drain Pilot Valves, and power is applied to the Backup scram SOVs. After the scram is reset, power is applied to the four groups of SSPVs in each division, power is applied to the SDV Vent and Drain Pilot Valves, and power is removed from the Backup scram SOVs. The SDV Vent and Drain Pilot Valves have a manual bypass to allow draining the SDV after a scram, while the reactor is in the Shutdown or Refuel mode.

Trips 10 through 14, inclusive, are provided to the RPS through a pair of nuclear instrumentation voters for each of the four channels, shown in Figure 3-13 below. Each voter is assigned to one of four RPS channels and receives inputs from all four APRM channels to determine whether or not a scram is warranted. The APRM modules also perform OPRM monitoring functions to ensure that the reactor is safely shut down upon indications of excessive thermal-

hydraulic instability. OPRM trip signals, generated by the APRM modules, are also sent to the voting modules. If 2oo4 APRMs or 2oo4 OPRMs exceed their established scram setpoint values, all four voters will generate a scram signal to de-energize the associated RPS logic channels. The necessity for each voter to receive at least two APRM or OPRM scram signals prevents the possibility of receiving a half scram (with the exception of when a voter module has a failed power supply). This figure also shows the APRM interface with Local Power Range Monitors (LPRMs), the Rod Block Monitors (RBMs), and the Operator Display Assemblies (ODAs).

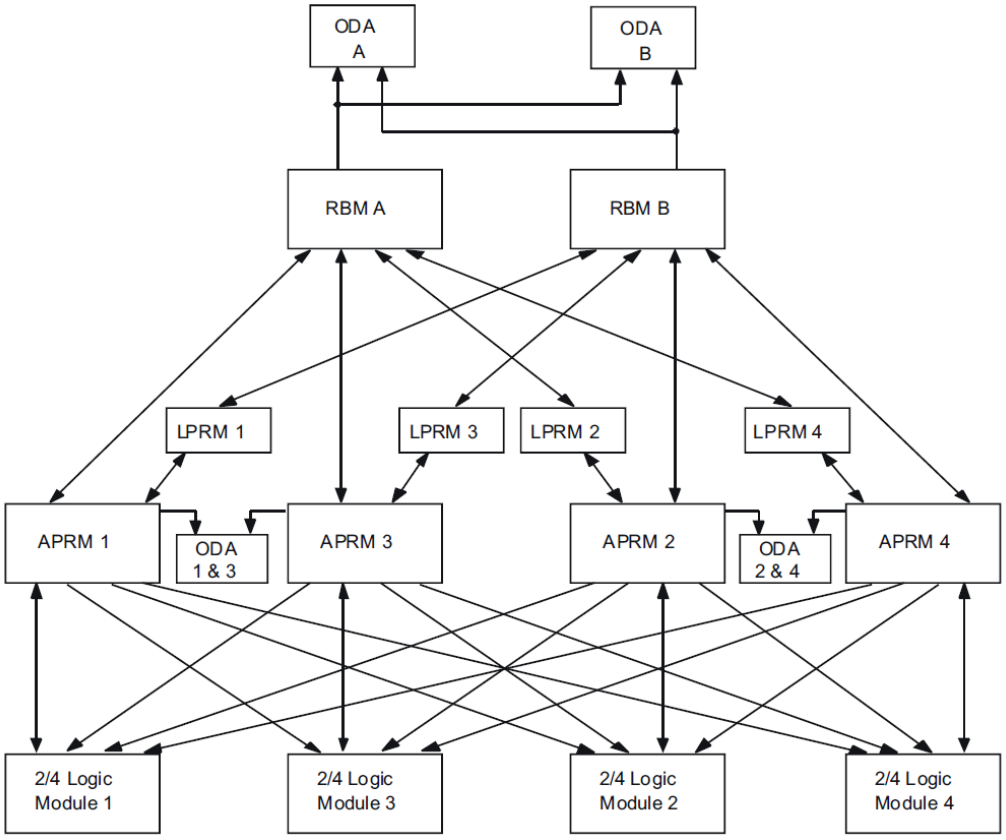

Figure 3-13. Neutron Monitoring Voter Structure (Reference 49)

When the RPS detects a condition requiring a scram, the RPS removes power from the SSPVs and from the SDV Vent and Drain Pilot Valve solenoids. This action causes the rapid insertion of the control rods by the CRD System and closure of the SDV Vent and Drain Valves. The RPS scram signal also energizes the Backup Scram Valves. The use of Backup Scram Valves provides an independent means of control rod insertion but at a much slower rate than control rod insertion normally occurs using the Scram Pilot Valves. Backup Scram Valve operation is not assumed in any of the analyses utilizing the scram function.

Uninterruptible 120 VAC Power Source

The RPS power, which is normally supplied from uninterruptible power supplies (UPS), is used as a source of power for the instrumentation, whose trip outputs go to normally energized logic

such as the RPS and certain functions of the N4S. The UPS preferred power source is the station's 250 VDC Class 1E battery system. An alternate source is available from the station auxiliary AC power distribution system. Use of the UPS is necessary to prevent inadvertent scrams and isolations. RPS power is also used to power ODAs and recorders for the Power Range Neutron Monitoring (PRNM) and Reactor Recirculation Systems in order to increase the availability of these readout devices.

RPS power also provides an alternate source of power for the following equipment:

- PRNM cabinet buses
- Control Rod Position Information cabinet
- SRV position indication system
- Reactor control and feedwater console.

Alternate power for these features is provided through manual transfer switches.

3.2.1.2 RPS Technical Specification Surveillance Requirements

Testing of the existing RPS is performed through a series of manually-executed evolutions. Many of these evolutions are driven by existing TS Surveillance Requirements (SRs) to verify that the RPS remains operable in all applicable modes of operation. The independence associated with the existing system architecture permits testing of individual system components (e.g., sensing instruments) as well as individual channels. The following service and test functions are applicable to the RPS:

- Sensor Calibration: Each sensing instrument and input to the RPS scram logic channels can be tested and calibrated. Certain inputs necessitating the use of sensing instrument transmitters may be valved out of service to support calibration and functional checks of the associated scram logic. However, the calibration of other functions (e.g., those requiring MSIV and TSV limit switches, TCV pressure switches, and neutron monitoring instrumentation) may also be calibrated and exercised but through different means.

- Response Time Testing: This test verifies that the maximum operating time from the change of state of a sensor input contact or an analog signal for a monitored parameter exceeding a setpoint, to and including opening of the contacts on the main trip actuators (scram contactors), meets the timing provided in the RPS portion of the PPS Functional Requirements (Reference 9). This satisfies the existing TS SRs associated with system response time to ensure that assumptions in the accident analyses remain satisfied.

- Logic System Functional Tests: Verification that the appropriate channel trips in response to abnormal conditions is performed by applying test signals directly to sensing instruments or by applying a calibration input to existing analog trip units (which have a built-in calibrator).

- Channel Check: Operability of individual process inputs to RPS is verified by cross-checking readings from one channel to the other channels to verify that each input is within a certain tolerance of the other inputs. Channel checks can be performed for the Reactor Vessel Water Level, Reactor Pressure, and Drywell Pressure scram functions. These channel checks satisfy current TS SRs for the system.

- Manual Scram Test: This test verifies the scram contactors in the RPS logic channels properly open in response to a manual scram signal.

- Automatic Scram Test: This test verifies the scram contactors in the RPS logic channels properly open in response to an automatic scram signal.

- Single Rod Scram Test: TS SRs dictate that each control rod must be individually inserted using a scram signal at certain frequencies. This test is executed using toggle switches at the HCU for a particular control rod. The control rod is timed ("scram time testing") to verify that accident analysis assumptions regarding reactor scram times remain satisfied. These tests are preceded by reactor engineering evaluations to ensure that these tests do not result in rod patterns that could potentially challenge thermal limits.

3.2.1.3 RPS Separation and Independence

The existing RPS design satisfies the IEEE Std. 384-1977 (Reference 26) requirement that redundant sensors and their connections to the process system be sufficiently separated to ensure that the functional capability of the protection system is maintained despite any single design basis event or resulting effect, with the exception of those inputs provided by the Main Turbine System components for anticipatory trips. Specifically, the RPS interface with the TSV limit switches and TCV pressure switches, which provide inputs to RPS, does not satisfy this requirement, since the turbine building is non-seismic. Therefore, these trip signals may not be generated following a Safe Shutdown Earthquake (SSE) event. However, sufficient diversity for these signals is provided by the high Reactor Vessel Pressure and high neutron flux scram signals, as discussed in LGS UFSAR Section 7.2.1.2.8 (Reference 41).

The existing design of the RPS satisfies the requirements of IEEE Std. 279-1971 (Reference 10) for channel independence. In general, each RPS scram function requires four redundant process parameter inputs (e.g., pressure, level, valve position) to actuate the system and initiate a scram. The redundant sensor devices are physically separated to ensure that no single failure can impact the ability of RPS to carry out its specified safety function. All RPS wiring outside the equipment cabinets retains the existing separation and protection. The existing divisional equipment cabinet locations in the AER are separated, and the new equipment will maintain the divisional separation. Each divisional cabinet contains two separate bays to contain each of the two channels in the division.

3.2.1.4 RPS Connections and Internal Interfaces

The RPS is electrically isolated from the plant control systems to ensure compliance with IEEE Std. 279 (Reference 10) design requirements associated with control and protection system

interactions. Physical connections to the RPS are currently terminated at the respective AER cabinets identified in Section 3.2.1.10. Field terminations associated with the existing RPS cabinets will be maintained as part of the modernization, and new terminations will be made, as required.

There are no internal communications between divisions and channels of the RPS. Inputs to the various RPS channels are routed and processed independently in the existing analog I&C architecture, with the exception of the neutron monitoring voter modules, which accept inputs from multiple APRM modules. While the output of each voter is provided to its respective RPS channels, the voters are considered to be part of the neutron monitoring system and are outside the scope of the modernization. Interfaces with RPS control features are addressed below in Section 3.2.1.5. Interfaces with other safety-related and non-safety related systems are discussed in Sections 3.2.1.6 and 3.2.1.7, respectively.

3.2.1.5 RPS Human-System Interface

Table 3-4 below identifies the existing HSI interfaces and functions and denotes whether these will be impacted by the modernization.

Table 3-4. Existing RPS Human-System Interfaces

Interface	Function	Modernization Impact
Analog Trip Units	Analog trip units located in the AER are used to support testing activities (e.g., trip and calibration activities) and TS-required channel checks using the analog indicators.	The analog trip units will be removed entirely. The bi-stable function currently executed by the trip units, where the input value is compared to the established set point, will be replaced by application software on the new digital platform. Data will be provided in the CR on video displays.
Reactor Mode Switch	The reactor system mode switch selects appropriate operating bypasses for various RPS variables in the shutdown, refuel, startup, and run modes of operation.	The Reactor Mode Switch will be sampled once and used by the PPS.
SDV High Water Level Bypass	The SDV high-level scram signal can be bypassed through the use of two key-locked switches, a bypass switch, and the reactor mode switch. This allows a scram to be reset and the SDV to be drained.	This interface will be executed using soft controls. The existing physical switches will be removed from the main CR control panel.
Manual scram Pushbuttons	Four manual scram pushbuttons (one per channel) are provided to allow operators to manually initiate the RPS.	The scram function of these interfaces will not be impacted by the proposed modification, although individual switch functions are changed.

Table 3-4. Existing RPS Human-System Interfaces

Interface	Function	Modernization Impact
RPS Reset Switch	A three-position reset switch is provided for the RPS in the main CR. This switch can be used to reset RPS logic provided that the requisite time delay has passed and the initiating condition is clear.	This RPS reset interface will be replaced using soft controls as part of this modification.
RPS Annunciators	Manual and/or automatic RPS inputs are annunciated in the main CR through the use of isolated relay contacts. Tripping of the associated RPS logic strings is also annunciated.	Some existing annunciation tiles will be migrated to soft control displays as part of this modification. These tiles are non-safety related and may co-exist with the new displays for a period of time.
Control Rod Group Indicators	The main CR has eight lights in the RPS-related controls area, providing one lamp for each Division 1 rod group and one lamp for each Division 2 rod group. The lamps are illuminated when power is applied to the solenoid valve groups and extinguished when power is removed (i.e., when a scram is requested for the group).	These indicators will be moved to the video displays.
Plant Process Computer	Computer alarms are generated when an RPS channel is tripped. This provides the capability for operators to analyze an event which could have occurred too quickly to analyze in real time.	The PPC interface will not be impacted by the proposed modification.

3.2.1.6 RPS Connections between Safety Systems

The RPS interfaces with a number of safety systems to execute its specified safety functions. These safety systems include the following:

- Class 1E Power System: The Class 1E power system supports the RPS by providing a UPS for the various system functions and supporting interfaces (e.g., instrumentation). The UPS itself is supported by preferred 250 VDC power supplies from the station batteries and auxiliary AC power supplies. There is one UPS per RPS division. Two Class 1E circuit breakers are located between the UPS static transfer switch and its respective RPS distribution panel to protect the RPS power buses from an overvoltage, undervoltage, and under-frequency conditions.

- Nuclear Boiler System: Numerous inputs are provided from Nuclear Boiler System instrumentation to the RPS. These inputs include Reactor Vessel Water Level, Reactor Vessel Pressure, and Drywell Pressure. These signals are generally sent directly to the RPS as 4 to 20 mA signals.

- Neutron Monitoring System: The RPS interfaces with the IRMs and PRNM systems to provide discrete inputs to the RPS scram logic through interposing relays.

- CRD System: The RPS interfaces with the CRD System to insert control rods using HCUs and CRDMs. The HCU SSPVs serve as the boundary components between the RPS and CRD System. Additionally, the CRD SDV provides inputs to the RPS using level transmitters and level switches to support RPS scram logic.

- N4S: RPS and the N4S share a number of sensor inputs and analog trip units in the existing I&C architecture. Specifically, the RPS provides signals to the N4S under the following conditions:

  – Reactor Vessel Water Level Low (Low Level 3)

  – High Drywell Pressure

  – Reactor Mode Switch not in "RUN" position

  – Turbine Stop Valve <90% open.

3.2.1.7 RPS Connections to Non-Safety Related Systems

The existing RPS interfaces with the following non-safety related systems:

- Reactor Recirculation System: The RPS sends an EOC-RPT signal to the safety-related breakers for the Recirculation System pumps when a scram is caused by TSV closure or TCV fast closure RPS functions. To counteract this potential power increase, the EOC-RPT inserts negative reactivity by tripping the reactor recirculation pumps upon receipt of a TSV or TCV scram signal[3]. Interposing relays are used to support the interface between the TSV and TCV inputs and the RPS.

- Main Turbine: The RPS receives inputs from TSV limit switches and the main turbine Electrohydraulic Controller (EHC) pressure switches at the TCVs. The main turbine first stage pressure also is used as an input to the RPS to determine when to bypass the RPS scram signals associated with TSV closure or TCV fast closure. Specifically, the first stage pressure is used as a proxy for reactor power and below certain power levels (i.e., first stage pressures), the reactor will not scram upon receipt of these scram signals. Interposing relays are used to interface between the TSV and TCV inputs and the RPS.

[3] The EOC-RPT logic is different from the RPS 1oo2, taken twice logic. This difference means that, for the TSV closure function, which causes a scram when any three or more of the turbine stop valves are closed, a scram will also always result in an RPT. For the TCV fast closure function, the logic difference means that if a scram were to occur because of the fast closure of only two specific control valves [(1 and 4) or (2 and 3)] an associated RPT would not occur. However, the chance of this occurring is extremely small, since the events which cause the TSVs to close or the TCVs to fast close should cause all four of the specific type valve to close, thereby making the logic difference inconsequential.

- Process Radiation Monitoring: The RPS interfaces with this system to support tripping of mechanical vacuum pumps upon receipt of a high radiation condition in the main steam lines. This is currently an N4S Group I isolation signal. (While currently listed as an RPS signal, this function will be moved to the N4S in the modernized system.)

- Annunciator System: The non-safety related annunciators provided audible and visual indication to operators regarding critical and noncritical events associated with the RPS. Outputs from the RPS are provided through the network to the DCS, which then provides contact closure outputs to the annunciator system.

- PPC: The RPS interfaces with the PPC to support event logging of RPS channel trips to aid in operator analysis of plant events that resulted in actuation of the RPS. Communicated data from the RPS are electrically isolated from the PPC.

3.2.1.8 RPS Temporary Connections

Temporary connections associated with the RPS are made on an as-needed basis. These connections are typically utilized to support performance of the testing activities (e.g., control rod scram time testing).

3.2.1.9 RPS Interface with Supporting Systems

The RPS is supported by the Control Structure Chilled Water System and the UPS previously discussed in Section 3.2.1.1. The Control Structure Chilled Water System and Control Enclosure Heating, Ventilation, and Air Conditioning (HVAC) are required to ensure operation of the RPS components within their environmental design requirements. As previously discussed, the UPS works to prevent inadvertent scrams and isolations, which decrease plant availability and place added stresses on the plant.

3.2.1.10 RPS Equipment Locations

The existing RPS equipment is installed in cabinets in the AER. Specifically, cabinets C609 and C611 contain the Division A and Division B RPS equipment, respectively, with the exception of the reactor mode switch, reactor manual scram pushbuttons, RPS reset switch, indicating lamps, and annunciators which are located in the CR. The modernized digital equipment will be installed in the AER in the same cabinets as the original equipment. The modernized equipment provides the software-based data acquisition, bi-stable, timing, logic solving, and output drive to replace the analog trip modules, pneumatic time delay relays, relay logic, and contactors in the existing architecture.

3.2.1.11 RPS Existing Use in Post-Accident Monitoring

The RPS is not used to support Post-Accident Monitoring (PAM) functions.

3.2.1.12 RPS Existing Bypass and Status Indication in Control Room

The existing RPS provides annunciation when essential portions of the system are bypassed. Indicator lamps and annunciators are automatically illuminated to inform CR operators that portions of the RPS are out of service and inoperable.

System out-of-service annunciators energize when one or more of the following conditions occur:

1. Trip units are being tested or a gross failure of a transmitter is detected.

2. Trip units are out of their card file, or there is a loss of power to the transmitters, or trip units.

In addition to the automatic bypassed indications, operators are provided with a switch in the CR to manually bring up the system out-of-service annunciator. Instruments that form part of a 1oo2 taken-twice logic system can be removed from service for calibration. Removal of the instrument from service is indicated in the CR by manual actuation of the system out-of-service annunciator by the system out-of-service switch. These design features satisfy the design requirements of IEEE Std. 279 (Reference 10) to ensure that bypassed indications are appropriately indicated in the CR.

3.2.2 N4S Existing Architecture (DI&C-ISG-06 D.2.1.1)

The N4S uses the same equipment as the RPS in a similar architecture. As shown in Figure 3-14 below, an isolation signal generated by the N4S actuates field equipment to implement the required safety function or functions. The N4S uses analog trip units, relay logic, and other I&C components to execute isolation functions. The system architecture is different in that each N4S function and the corresponding function channels are not supplied with every parameter. Thus, the relay logic associated with each function is different. Voting architectures vary depending on the number of input parameters and the voting required to implement the N4S isolation functions. The outputs from the N4S interface with the control wiring associated with valve motors, solenoids, and other hardware to execute isolation functions in interfacing systems.

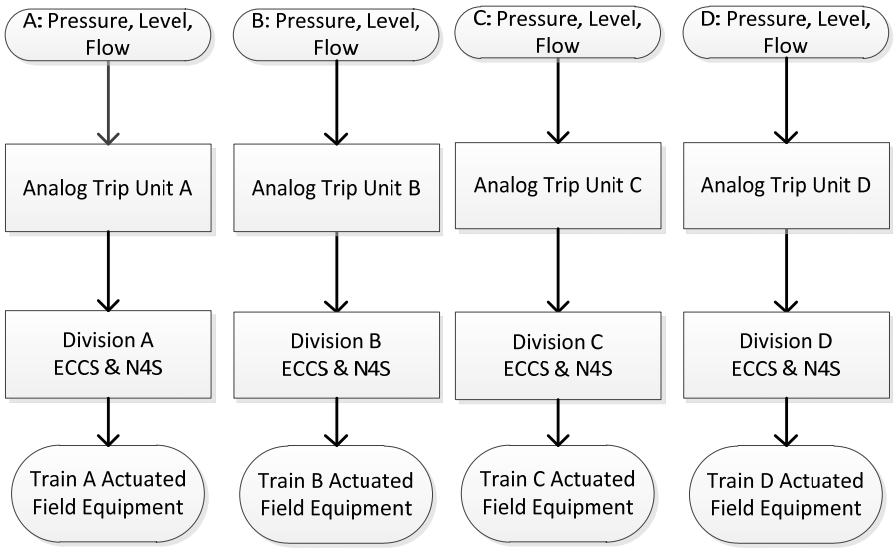

Figure 3-14. Existing ECCS and N4S Data Flow

3.2.2.1 N4S System Design Functions

The general logic associated with N4S is illustrated in Figure 3-15 below, which shows a generic process piping arrangement. It is assumed that the associated process pipe interfaces directly with the reactor vessel, which necessitates one isolation valve inside containment and one isolation valve outside containment. The sensor inputs to the example logic string in Figure 3-15 are representative of the various pressure transmitters, flow elements, radiation detectors, temperature elements, or limit switches that are converted into electrical signals for use in the circuit. As shown in Figure 3-15, the N4S logic is generally arranged in a 2oo2 taken once arrangement, except as noted in subsequent sections.

Many of the isolation functions are "de-energize-to-actuate," where the initiation relay is normally energized by maintaining closed contacts along the length of the circuit. Drop out of contacts on both sides of the circuit, resulting from some sensor input(s), will de-energize the relay and isolate the valve. Note that this arrangement can result in "half isolation" situations if the logic power supplies are lost and the initiation relay becomes de-energized. In this instance, either the inboard or outboard valve isolates, due to the logic power supply loss. These half-isolations do isolate the entire process pathway, as long as the energized valve operates correctly. To ensure isolation, the modernized voting will be changed to ensure that both valves actuate, which will result in the isolation even if one valve fails. The isolation signals associated with Group IV (HPCI) and Group V (RCIC) are "energize-to-actuate" and, therefore, are not susceptible to spurious isolations due to logic power supply loss. Note that manual isolation functions are also possible, where a switch or other device can be used to execute the N4S isolation function and close the associated valve.

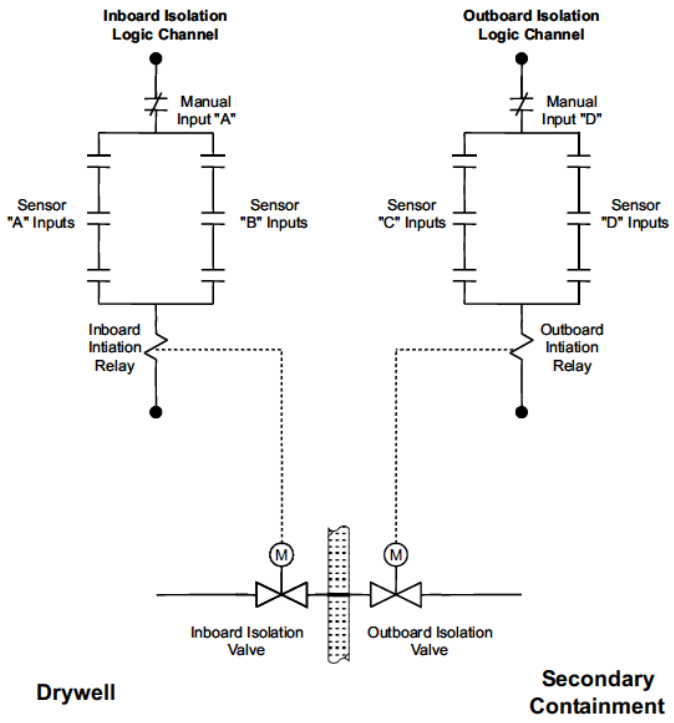

Figure 3-15. Typical N4S Inboard and Outboard Configuration (Reference 50)

The example illustrated in Figure 3-15 above is representative of most of the existing N4S isolation logic. However, there are some important exceptions to the logic described above. These include valves in the Containment Atmospheric Sampling System (CASS), various isolation dampers associated with the secondary containment isolation, and others shown in Table 3-5 below. Additionally, inputs to the N4S from the Steam LDSs operating on the NUMAC platform require only one detector to trip for valve isolation. The Steam LDS is divided into four channels that each receive a number of temperature inputs from various plant areas to determine whether a steam leak is present and, subsequently, that isolation of the associated pathway is warranted.

The most significant difference between the generic logic described above and the exceptions is found in the MSIV isolation logic. As shown in Figure 3-16 below, MSIV isolation logic can be classified as 1oo2, taken twice. Both pilot solenoids used to control valve pneumatics must be de-energized to close the associated MSIV. This arrangement has been structured to prevent inadvertent isolation of the MSIVs which results in a significant plant transient.

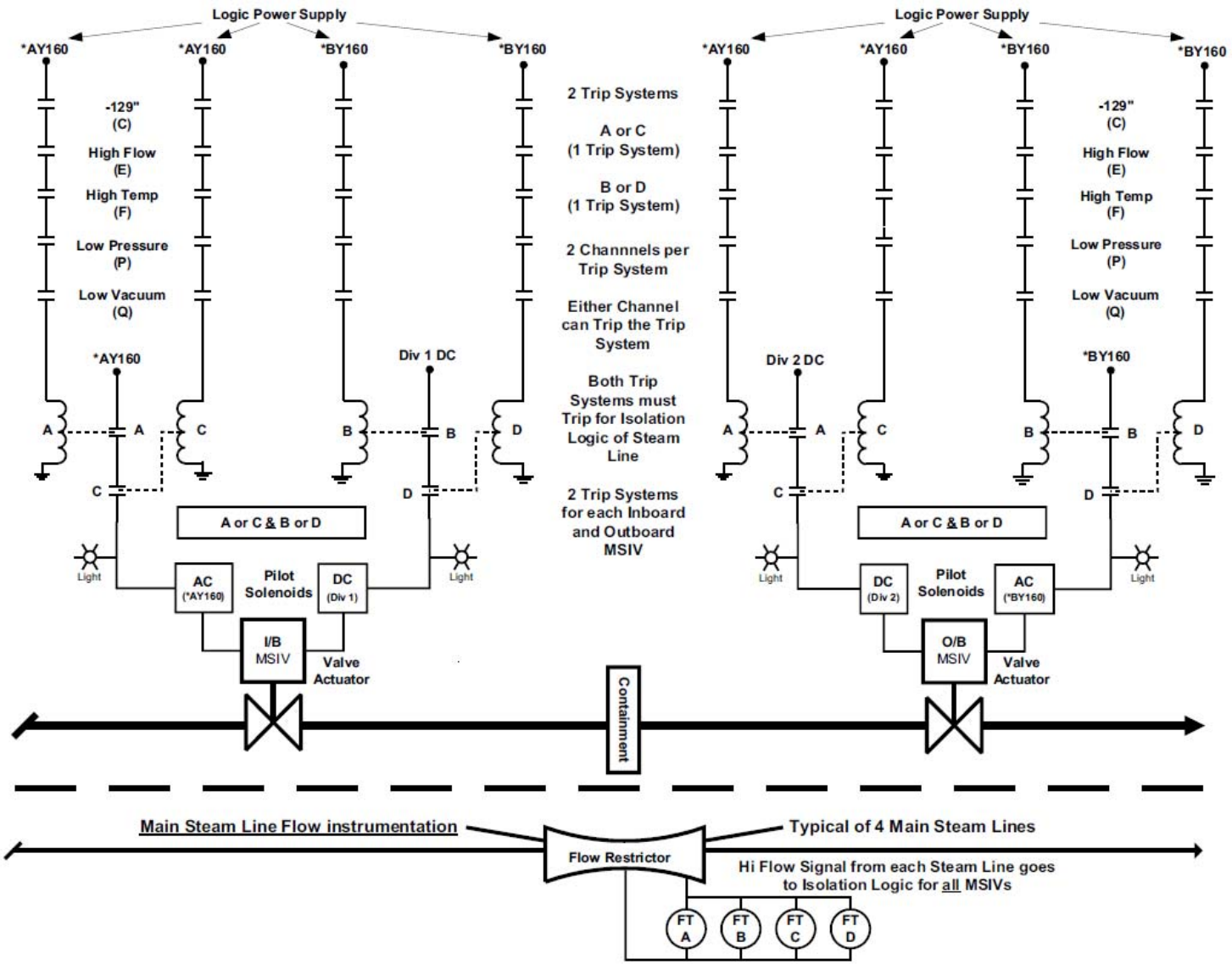

Figure 3-16. Current MSIV Isolation Logic (Reference 51)

The MSIV logic in Figure 3-16 above also illustrates a problem similar to the RPS logic: noncoincident trips. The MSIVs will isolate upon receipt of a number of abnormal conditions, including, but not limited to, low Main Steam Line Pressure, high Main Steam Line Flow, and high temperature, which are conditions indicative of a steam line break. However, the current logic arrangement can result in a situation where receipt of one abnormal condition in one logic string can combine with a completely different adverse condition in another logic string to cause a noncoincident isolation signal. This raises the potential for instrument failures to cause significant plant transients.

Isolation Signals

The N4S initiates closure of various automatic isolation valves when monitored system variables exceed preestablished limits. This action limits the loss of coolant from the RCPB and the release of radioactive materials from the RCPB, the primary containment, and the reactor enclosure. To satisfy this design function, the N4S performs the isolation functions defined in Table 3-5 below. These isolation functions are initiated based on inputs from different channels for the listed conditions. Logic may be shared between isolations, but there is not a common logic scheme that applies to all isolations of the N4S. Table 3-5 also denotes whether an available operational bypass exists for the isolation signal, whether any (or all) of the isolation conditions for a particular group can be bypassed and whether the bypass is applicable to all or part of the interfacing systems. Operational bypasses include those which are automatically implemented and those which are enabled manually through operator action.

Table 3-5. N4S Isolation Functions

Group	Isolated Equipment	Conditions for Isolation	Logic[1]	Bypass
IA	MSIVs		1oo2 Taken Twice (see Figure 3-16)	No (except that Condenser Vacuum – Low and Main Steam Line – Low Pressure condition only applies when the Reactor Mode Switch is not in Run)
	Main Steam Line Drains	a. Reactor Vessel Water Level 1 – Low, Low, Low	a. 2oo2	
		b. Main Steam Line – Low Pressure	b. 2oo2	
		c. Main Steam Line – High Flow	c. 2oo2	
		d. Condenser Vacuum – Low	d. 2oo2	
		e. Outboard MSIV Room Temperature High	e. 2oo2[2]	
		f. Turbine Enclosure – Main Steam Tunnel – High Temperature	f. 2oo2[2]	
		g. Manual Initiation	g. 1oo1	
IB	Main Steam and Reactor Sample	a. Reactor Vessel Water Level 2 – Low, Low	a. 2oo2	No
		b. Manual Initiation	b. 1oo1	

Table 3-5. N4S Isolation Functions

Group	Isolated Equipment	Conditions for Isolation	Logic[1]	Bypass
IIA	RHR Shutdown Cooling	a. Reactor Vessel Water Level 3 – Low b. Reactor Vessel Pressure – High (RHR Valve Permissive) c. Manual Initiation	a. 2oo2 b. 1oo2 c. 1oo1	No
IIB	RHR Heat Exchanger Sample and Drain to Radwaste	a. Reactor Vessel Water Level 3 – Low b. Drywell High Pressure c. Manual Initiation	a. 2oo2 b. 2oo2 c. 1oo1	Yes (except for RHR Drain to Radwaste Valves)
III	Reactor Water Cleanup	a. RWCU – Differential Flow High b. RWCU – Area High Temperature c. RWCU – Area Delta Temperature High d. SLCS Initiation (Initiated by RRCS) e. Reactor Vessel Water Level 2 – Low, Low f. Manual Initiation	a. 1oo1 b. 1oo1[2] c. 1oo1[2] d. 1oo2 (Inboard Valve, 1oo1 Outboard Valve) e. 2oo2 f. 1oo1	No (Except for RWCU – Differential Flow High is bypassed 45 seconds once setpoint is exceeded)
IVA	HPCI Process	a. HPCI – Reactor Steam flow high b. HPCI – Steam Supply Pressure Low c. HPCI – Turbine Exhaust Diaphragm High Pressure d. HPCI – Room Temperature High e. HPCI – Pump Room Delta Temperature High f. Manual Initiation (Division 2 only, requires HPCI initiation condition present)	a. 1oo1 b. 2oo2 c. 2oo2 d. 1oo1[2] e. 1oo1[2] f. 1oo1	No (Except for HPCI – Reactor Steam Flow High is bypassed 3 seconds once setpoint is exceeded)
IVB	HPCI Vacuum Breaker	a. Drywell Pressure High AND b. HPCI – Steam Supply Low Pressure	a. 2oo2 b. 2oo2	No

Table 3-5. N4S Isolation Functions

Group	Isolated Equipment	Conditions for Isolation	Logic[1]	Bypass
VA	RCIC Process	a. RCIC – Steam Flow High b. RCIC – Steam Supply Low Pressure c. RCIC – Exhaust Diaphragm High Pressure d. RCIC – Room High Temperature e. RCIC – Pump Delta High Temperature f. Manual initiation (Division 1 only, requires RCIC initiation signal not reset)	a. 1oo2 b. 2oo2 c. 2oo2 d. 1oo1[2] e. 1oo1[2] f. 1oo1	No (Except for RCIC – Reactor Steam Flow High is bypassed 3 seconds after setpoint is exceeded)
VB	RCIC Vacuum Breaker	a. Drywell High Pressure AND b. RCIC – Steam Supply Low Pressure	a. 2oo2 b. 2oo2	No
VIA	Primary Containment Purge Supply and Exhaust	a. Reactor Vessel Water Level 2 – Low, Low b. Drywell High Pressure c. North Stack Effluent – High Radiation d. Reactor Enclosure Ventilation Exhaust Duct High Radiation e. Refueling Area Ventilation Exhaust Duct – High Radiation f. Outside Atmosphere to Refueling Area – Low Differential Pressure g. Outside Atmosphere to Reactor Enclosure – Low Differential Pressure h. Refuel Floor/ Standby Gas Treatment System (SGTS) Connecting Valves Failed Open i. Reactor Enclosure/SGTS Connecting Valves Failed Open j. Manual initiation	a. 2oo2 b. 2oo2 c. 1oo1 d. 2oo2 e. 2oo2 f. 1oo1 g. 1oo1 h. 1oo1 i. 1oo1 j. 1oo3	Yes (except for North Stack Effluent High Radiation)

Table 3-5. N4S Isolation Functions

Group	Isolated Equipment	Conditions for Isolation	Logic[1]	Bypass
VIB	Primary Containment Exhaust to Reactor Enclosure Equipment Compartment Exhaust (REECE) and Nitrogen (N_2) Block Valves	a. Reactor Vessel Water Level 2 – Low, Low b. Drywell High Pressure c. Reactor Enclosure Ventilation Exhaust Duct High Radiation d. Refueling Area Ventilation Exhaust Duct - High Radiation e. Outside Atmosphere to Refueling Area - Low Differential Pressure f. Outside Atmosphere to Reactor Enclosure - Low Differential Pressure g. Refuel Floor/ SGTS Connecting Valves Failed Open h. Reactor Enclosure/SGTS Connecting Valves Failed Open i. Manual initiation	a. 2oo2 b. 2oo2 c. 2oo2 d. 2oo2 e. 1oo1 f. 1oo1 g. 1oo1 h. 1oo1 i. 1oo3	Yes
VIC	Primary Containment Hydrogen/Oxygen (H_2/O_2) Sampling and Recombiner Lines	a. Reactor Vessel Water Level 2 – Low, Low b. Drywell High Pressure c. Refueling Area Ventilation Exhaust Duct - High Radiation d. Reactor Enclosure Ventilation Exhaust Duct High Radiation e. Manual Initiation	a. 1oo1 b. 1oo1 c. 1oo1 d. 1oo1 e. 1oo1	Yes (All valves except for Drywell Rad Sample Supply and Return Lines valves)
VIIA	Primary Containment Instrument Gas (PCIG)	a. Reactor Vessel Water Level 1 - Low, Low, Low b. Drywell High Pressure c. Reactor Enclosure Ventilation Exhaust Duct High Radiation d. Manual	a. 2oo2 b. 2oo2 c. 2oo2 d. 1oo2	Yes (Except for Primary Containment Vacuum Relief Valve Supply Line for conditions a and b)
VIIB	PCIG Traversing In-core Probes (TIP) Purge Supply	a. Reactor Vessel Water Level 2 – Low, Low b. Drywell High Pressure c. Reactor Enclosure Ventilation Exhaust Duct High Radiation d. Manual	a. 2oo2 b. 2oo2 c. 2oo2 d. 1oo2	No
VIIC	PCIG to ADS	a. PCIG to Drywell – Low Differential Pressure	a. 1oo1	No

Table 3-5. N4S Isolation Functions

Group	Isolated Equipment	Conditions for Isolation	Logic[1]	Bypass
VIIIA	Drywell Chilled Water and Reactor Enclosure Cooling Water (RECW)	a. Reactor Vessel Water Level 1 – Low, Low, Low b. Drywell High Pressure c. Manual	a. 2oo2 b. 2oo2 c. 1oo1	Yes
VIIIB	Drywell Sump, Suppression Pool Cleanup, TIPs	a. Reactor Vessel Water Level 2 – Low, Low b. Drywell High Pressure c. Manual	a. 2oo2 b. 2oo2 c. 1oo1	No
VIIIB	ECCS Process Lines	a. Reactor Vessel Water Level 1 – Low, Low, Low b. Drywell High Pressure AND c. Low Reactor Vessel Pressure	a. 1oo1 b. 1oo1 c. 1oo1	No
VIIIB	Bypass Barrier Block and Vents	a. Reactor Vessel Water Level 1 – Low, Low, Low b. Drywell High Pressure c. Refueling Area Ventilation Exhaust Duct – High Radiation d. Reactor Enclosure Ventilation Exhaust Duct High Radiation e. Manual	a. 1oo1 b. 1oo1 c. 1oo1 d. 1oo1 e. 1oo1	No (Except for N_2 Supply Vent Valves)
VIIIB	PCIG Block and Vents	a. Reactor Vessel Water Level at or below Level 1 b. Drywell High Pressure c. Reactor Enclosure Ventilation Exhaust Duct High Radiation d. Manual	a. 1oo1 b. 1oo1 c. 1oo1 d. 1oo1	Yes
VIIIB	Refuel Floor HVAC	a. Refueling Area Ventilation Exhaust Duct – High Radiation b. Outside Atmosphere to Refueling Area – Low Differential Pressure c. Refuel Floor/ SGTS Connecting Valves Failed Open d. Manual	a. 2oo2 b. 1oo1 c. 1oo1 d. 1oo6	Yes

Table 3-5. N4S Isolation Functions

Group	Isolated Equipment	Conditions for Isolation	Logic[1]	Bypass
VIIIB	Reactor Enclosure HVAC	a. Reactor Vessel Water Level 2 – Low, Low	a. 2oo2	Yes
		b. Drywell High Pressure	b. 2oo2	
		c. Reactor Enclosure Ventilation Exhaust Duct High Radiation	c. 2oo2	
		d. Outside Atmosphere to Reactor Enclosure - Low Differential Pressure	d. 1oo1	
		e. Reactor Enclosure/SGTS Connecting Valves Failed Open	e. 1oo1	
		f. Manual	f. 1oo6	

Note:

(1) The logic in this table refers to the logic required for isolation in each division, where divisions typically refer to either inboard or outboard divisions.

(2) Each channel of steam leak detection monitoring contains inputs from multiple areas.

3.2.2.2 N4S Technical Specification Surveillance Requirements

Testing of the existing N4S is performed through a series of manually-executed evolutions. Many of these evolutions are driven by existing TS SRs to verify that the N4S remains Operable in all applicable modes of operation. The independence associated with the existing system architecture permits the testing of individual system components (e.g., sensing instruments) as well as individual channels. The N4S also permits the testing of individual isolation valves, although the valves themselves are classified as part of the process system (e.g., main steam) and do not belong to the N4S.

The following service and test functions are applicable to the N4S:

- Logic and Actuation Functional Testing: These tests verify that the isolation valves actuated by the N4S will operate properly when required. Testing incorporates all elements of the system and tests the system from sensor to the actuator during plant operation, with the exception of the MSIVs. The MSIVs can only be tested from a particular sensor to one of the two solenoids required for valve closure. Actuation function testing verifies that all components from the sensor to the actuator, including the logic, function correctly.

- Slow-Acting Test: This test verifies actuation of the MSIVs. The MSIVs are exercised closed with the slow-acting test solenoid to verify that there are no obstructions to the valve stem at full power. Valve closure, using the two fast-acting main solenoids, requires a reduction in power to avoid reactor scram, due to high pressure and/or high neutron flux.

- Channel Check: Operability of individual process inputs to N4S is verified by cross-checking readings from one channel to the other channels to verify that each input is within a certain tolerance of the other inputs. These channel checks satisfy current TS SRs for the system.

- Calibration: Channel trip units and trip relays and instrument channels are calibrated and tested by injecting a calibration signal. This test verifies that the operating range of the component has not drifted out of the acceptable region.

3.2.2.3 N4S Separation and Independence

The existing design of the N4S satisfies the requirements of IEEE Std. 279-1971 (Reference 10) for channel independence. In general, each N4S isolation trip function requires four redundant process parameter inputs (e.g., pressure, level) to actuate the system and initiate isolation. Redundant sensor devices are physically separated to ensure that no single failure can impact the ability of N4S to carry out its specified safety function. However, as previously discussed, the N4S does support isolation functions with varying types and numbers of inputs (e.g., sixteen main steam flow inputs). Therefore, independence is not applicable to all N4S isolation functions. All N4S wiring outside the associated equipment cabinets is run in completely enclosed metallic raceways or in embedded PVC conduits. The equipment cabinets are located such that each division is located in separate areas of the AER. Each divisional cabinet contains two separate bays to contain each of the two channels in the division.

The existing N4S design satisfies the IEEE Std. 384 (Reference 25) requirement that redundant sensors and their connections to the process system be sufficiently separated to ensure that functional capability of the protection system is maintained despite any single design basis event or resulting effect.

3.2.2.4 N4S Connections and Internal Interfaces

Physical connections to the N4S are currently terminated at the respective cabinets identified in Section 3.2.2.10. Field terminations associated with the existing N4S cabinets will be maintained as part of this modification and new terminations will be made, as required. Non-safety related connections that interface with the N4S are provided with sufficient isolation to ensure that a fault associated with the interfacing system will not prevent the N4S from performing its specified safety functions. This includes the use of isolation between the N4S, the annunciator system, and the PPC.

There are no internal communications between divisions and channels of the N4S. Inputs to the various N4S channels are routed and processed independently in the existing analog I&C architecture, with the exception of the temperature inputs into the NUMAC steam LDS modules. Each NUMAC module receives numerous (greater than ten) temperature inputs that are processed independently to generate trip signals for the respective isolation group. However, each NUMAC module only provides a discrete output to the existing N4S architecture.

3.2.2.5 N4S Human-System Interface

Table 3-6 below identifies the existing HSI interfaces and functions and denotes whether these will be impacted by the modernization.

Table 3-6. Existing N4S Human-System Interfaces

Interface	Function	Modernization Impact
Analog Trip Units	Analog trip units located in the AER are used to support testing activities (e.g., trip and calibration activities) and TS-required channel checks using the analog indicators.	The analog trip units will be removed entirely. The bi-stable function currently executed by the trip units, where the input value is compared to the established set point, will be replaced by application software on the new digital platform. Data will be provided in the CR on video displays.
Manual Isolation Push Button Switches	Manual isolation of the various N4S functions described in Table 3-5 above is accomplished through the use of ten manual pushbuttons. Operation of these pushbuttons accomplishes initiation of all functions performed by automatic initiation circuitry.	The N4S manual isolation pushbuttons will be replaced using soft controls as part of this modification.
Key-Locked Bypass Switches	Sixteen bypass switches are provided to support testing and reopening various valves with isolation signals present. Bypass capabilities are listed in Table 3-5 above.	The N4S bypass switches will be replaced using soft controls as part of this modification.
N4S Reset Switches	Eight reset switches are available for resetting N4S isolation signals. Two switches support many of the N4S isolations. Six switches, including four key-locked switches, are used to support HVAC restoration.	The N4S reset interface will be replaced using soft controls as part of this modification.
N4S NUMAC Modules	Four NUMAC modules provide real-time data readouts related to steam leak detection in the form of area temperatures and differential temperatures. Modules are located in the AER and generate annunciator alarms and, potentially, isolations when various setpoints are exceeded.	Thermocouple inputs will be transmitted directly to the new digital platform. This will eliminate the need for the NUMAC modules. Application software will be used to generate protective trip signals when established temperature (or flow) values reach established set points. Data will be made available to CR operators using video displays.
N4S Indicating Lamps	Indicating lamps are illuminated based on the position of individual valves.	The N4S indicator lamps will be replaced with soft controls (i.e., digital indications) as part of this modification.

Table 3-6. Existing N4S Human-System Interfaces

Interface	Function	Modernization Impact
N4S Annunciators	Manual and/or automatic N4S inputs are annunciated in the main CR through the use of isolated relay contacts. Tripping of the associated N4S logic strings are also annunciated.	Existing annunciation tiles will remain. The data will be presented on video displays as part of this modification.
PPC	The PPC provides isolation status in the CR. This provides the operators real-time information on the progress and state of isolations.	The DKTs will provide the primary indication of isolation status to the operator. The PPS will provide electronic data directly to the DCS for monitoring. Direct PPC monitoring of isolated contact outputs from the N4S is no longer required. The PPC can still provide backup display, if desired.

3.2.2.6 N4S Connections Between Safety Systems

The N4S interfaces with a number of safety systems to execute its specified safety functions. These safety systems include the following:

- Class 1E Power System: The Class 1E power system supports the N4S by providing a UPS for the various system functions and supporting interfaces (e.g., instrumentation). The UPS itself is supported by preferred 250 VDC power supplies from the station batteries and auxiliary AC power supplies. N4S power comes from two nonessential RPS buses.

- RPS: RPS and the N4S share a number of sensor inputs and analog trip units in the existing I&C architecture. Specifically, the RPS provides signals to the N4S under the following conditions:

  – Reactor Vessel Water Level Low (Low Level 3)

  – High Drywell Pressure

  – Reactor Mode Switch not in “Run” position

  – Turbine Stop Valve <90% open.

- RHR: N4S initiates the closure of the following RHR components when the set conditions for isolation are met:

  – Discharge to Radwaste isolation valves

  – Process sampling isolation valves

  – Shutdown Cooling suction valves

  - Shutdown Cooling injection-testable check valves and bypass valves
  - Suppression Pool Spray line
  - Heat exchanger vent valve discharge lines

- RCIC: N4S provides constant leak monitoring for the RCIC system. Area ambient and differential temperatures, RCIC steam flow rate, RCIC steam line pressure, and RCIC turbine exhaust diaphragm pressure are all monitored. N4S initiates auto-isolation signals when the set conditions for isolation are met.

- HPCI: N4S provides constant leak monitoring for the HPCI system. Area ambient and differential temperatures, HPCI steam flow rate, and HPCI turbine exhaust diaphragm pressure are all monitored. N4S initiates auto-isolation signals when the set conditions for isolation are met.

- SGTS: N4S initiates the standby gas treatment upon receipt of a reactor enclosure or refueling floor isolation signal.

- N4S initiates isolation of process lines in the following safety-related systems when the respective conditions for isolation are met:
  - Chilled Water System
  - Main Steam
  - Containment Atmospheric Control
  - Process Radiation Monitoring System
  - Reactor Enclosure Recirculation System
  - Reactor Enclosure Isolation System
  - Primary Containment Instrument Gas System (ADS)
  - Core Spray

3.2.2.7 N4S Connections to Non-Safety Related Systems

The existing N4S interfaces with the following non-safety related systems:

- Annunciator System: The non-safety related annunciators provide audible and visual indications to operators regarding critical and noncritical events associated with the N4S. Outputs from the N4S are provided as contact closure outputs to the annunciator system.

- PPC: The PPC provides an interface for operators to view N4S isolation statuses, progress of isolations, and individual valve statuses. Communicated data from the ECCS are electrically isolated from the PPC.

- N4S initiates the isolation of lines in the following non-safety related systems when the respective conditions for isolation are met:

  - Reactor Recirculation System

  - Reactor Water Cleanup System

  - Suppression Pool Cleanup System

  - Reactor Enclosure Cooling Water System

  - TIP System

  - Primary Containment Instrument Gas System (non-ADS)

  - Primary Containment Purge

3.2.2.8 N4S Temporary Connections

Temporary connections associated with the N4S are made on an as-needed basis. These connections are typically used to support performance of the testing activities (e.g., trip unit calibration).

3.2.2.9 N4S Interface with Supporting Systems

Power for the N4S isolation logic is provided primarily by the RPS UPS power supplies previously described in Section 3.2.1.1. This includes power supplies for one of two solenoids on each MSIV actuator. The 125 VDC station batteries provide power supplies for N4S isolation functions associated with the HPCI and RCIC systems and the second of two MSIV actuator solenoids. The N4S equipment is located almost entirely in the AER, with the exception of the HSI located in the main CR. This equipment is supported by the Control Enclosure Chilled Water System. The Control Enclosure Chilled Water System and associated unit coolers are required to ensure operation of the N4S components within their environmental design requirements.

3.2.2.10 N4S Physical Location of System Equipment

Most of the existing N4S equipment is installed with the RPS equipment in AER cabinets. Specifically, cabinets C609 and C611 contain the Division 1 and Division 2 N4S equipment, respectively. The manual isolation pushbuttons, reset pushbuttons, key-locked bypass switches, indicating lamps, and annunciators are located in the CR. N4S equipment associated with the HPCI and RCIC systems is located in separate, divisionalized cabinets in the AER. Panels C620 and C641 contain equipment that supports HPCI Isolation functions. Panels C621 and C640 contain equipment that supports RCIC isolation functions. The HPCI and RCIC panels also contain equipment that supports other design functions associated with these systems.

The modernized digital equipment will be installed in the AER in the same cabinets as the original equipment. The modernized equipment will provide the software-based data acquisition, bi-stable, timing, logic solving, and output drive to replace the analog trip modules, pneumatic time delay relays, relay logic, and contactors in the existing architecture.

3.2.2.11 N4S Use in Post-Accident Monitoring

The N4S supports PAM by providing valve indication status for various isolation valves.

3.2.2.12 N4S Bypass and Status Indication in Control Room

System status is automatically indicated in the CR to alert operators that a system is inoperable. Annunciation occurs whenever a system or part of a system becomes inoperable. Any time a bypass switch is moved to a position that would cause a bypass of an isolation signal; this condition is annunciated. Control switches are also provided to manually actuate the out-of-service annunciator. Manual actuation is also provided for the out-of-service annunciators for instruments that are removed from service for calibration. This applies to instruments that are part of a 1oo2 logic system.

3.2.3 ECCS Existing Architecture (DI&C-ISG-06 D.2.1.1)

The ECCS I&C provides automatic initiation and manual control capabilities for the in-scope systems to ensure that each system is capable of performing its specified safety function. The existing ECCS I&C architecture uses the same trip units, time delay relays, and relay logic as the N4S and RPS. The ECCS uses the same equipment as the RPS and N4S and is built in a similar architecture. As shown Figure 3-14 above (common to both ECCS and N4S), an isolation signal generated by the ECCS actuates field equipment to implement the required safety function or functions. The existing system architecture is safety-related and composed of four channels and two or four voters. Each of the four channels is independent of the other channels and relies on an “energize-to-actuate” principle, where the logic is normally de-energized and uses 125 VDC power supplies.

3.2.3.1 ECCS System Design Functions

The primary design function of the ECCS I&C is to initiate appropriate system responses to ensure that the fuel is adequately cooled in the event of a design basis accident. Initiation of the ECCS subsystems and RCIC occurs in response to the signals documented in Table 3-7 below.

This table also includes the initiation logic associated with each subsystem. Initiation in this context refers to CS and RHR pump starts, steam admission valves opening for HPCI and RCIC, injection valves opening for all subsystems, ADS SRVs opening, and other required equipment actuations (e.g., preferred suction pathway valves opening).

Logic

A simplified version of the LOCA initiation logic is presented Figure 3-17 below. This logic is representative of most ECCS logic arrangements which are 2oo2. As shown in Figure 3-17, a LOCA initiation in a single division can be generated by the receipt of two channels of low Reactor Vessel Water Level[4] (A1 and A2) or two channels of low Reactor Vessel Pressure (A1 and A2) and high Drywell Pressure (A1 and A2).

The following combinations of low Reactor Vessel Water Level, low Reactor Vessel Pressure, and high Drywell Pressure will also result in a LOCA signal:

1. One channel of low Reactor Vessel Water Level (A1) with one channel of low Reactor Vessel Pressure (A2) and high Drywell Pressure (A2); or

2. One channel of low Reactor Vessel Water Level (A2) with one channel of low Reactor Vessel Pressure (A1) and high Drywell Pressure (A1).

Receipt of these combinations of input signals closes contacts in the associated logic string and energizes contactors and relays to actuate equipment in respective safety systems (e.g., starting pump motors, opening injection valves). Manual initiation of each division can also be used to actuate the associated ECCS subsystems.

[4] LOCA initiation occurs upon the receipt of Level 1 – Low, Low, Low Reactor Vessel Water Level.

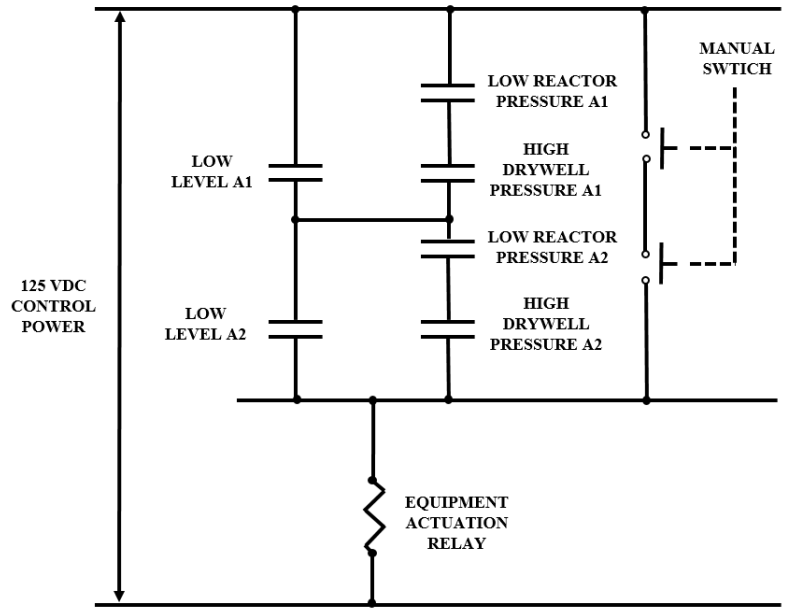

Figure 3-17. Simplified LOCA Initiation Logic for ECCS (based on Reference 52)

Figure 3-17 above is representative of the ECCS logic associated with RHR and CS. HPCI and RCIC initiation logic operates in a similar manner. A simplified version of the HPCI initiation logic is presented in Figure 3-18 below. As shown in Figure 3-18, the HPCI initiation logic also works on a 1oo2 taken-twice arrangement for both the low Reactor Vessel Water Level (Level 2) and high Drywell Pressure initiation signals. RCIC initiation logic is identical to that associated with the HPCI system, except that RCIC only initiates in response to low Reactor Vessel Water Level (Level 2 – Low, Low) and does not initiate in response to high Drywell Pressure.

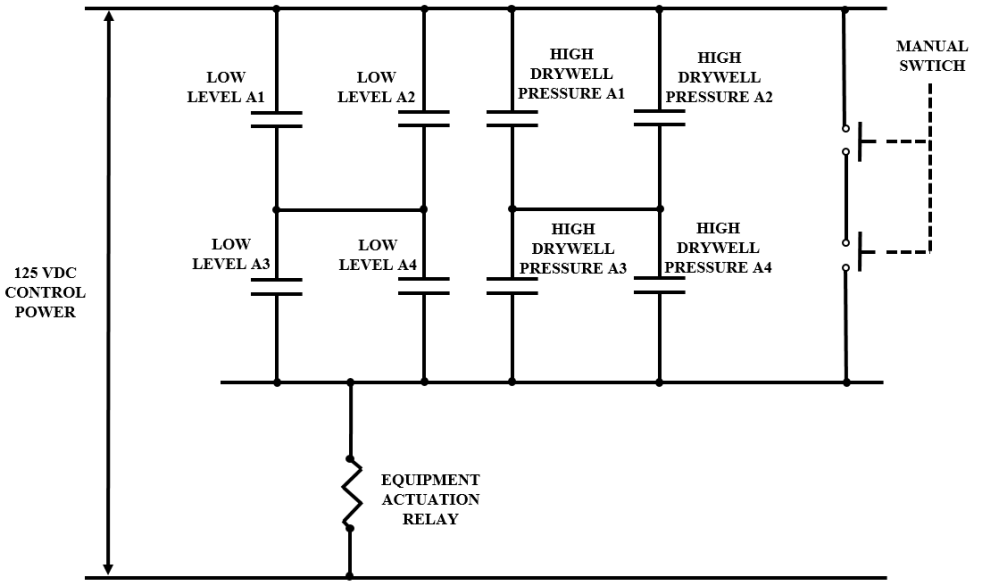

Figure 3-18. Simplified HPCI Initiation Logic for ECCS (based on Reference 53)

ADS initiation logic is significantly hardened to prevent against inadvertent and spurious SRV operation, which can induce severe transients on the RPV and other plant Structures, Systems, and Components (SSC). This logic is depicted in Figure 3-19 below. Figure 3-19 represents one of two ADS divisions (Division III not shown). As depicted, two channels of logic (Channels A and E of Division I) are required to actuate in order for ADS to automatically initiate and open the corresponding SRVs. Alternatively, the ADS valve switch may be placed in the Open position to manually open the SRV.

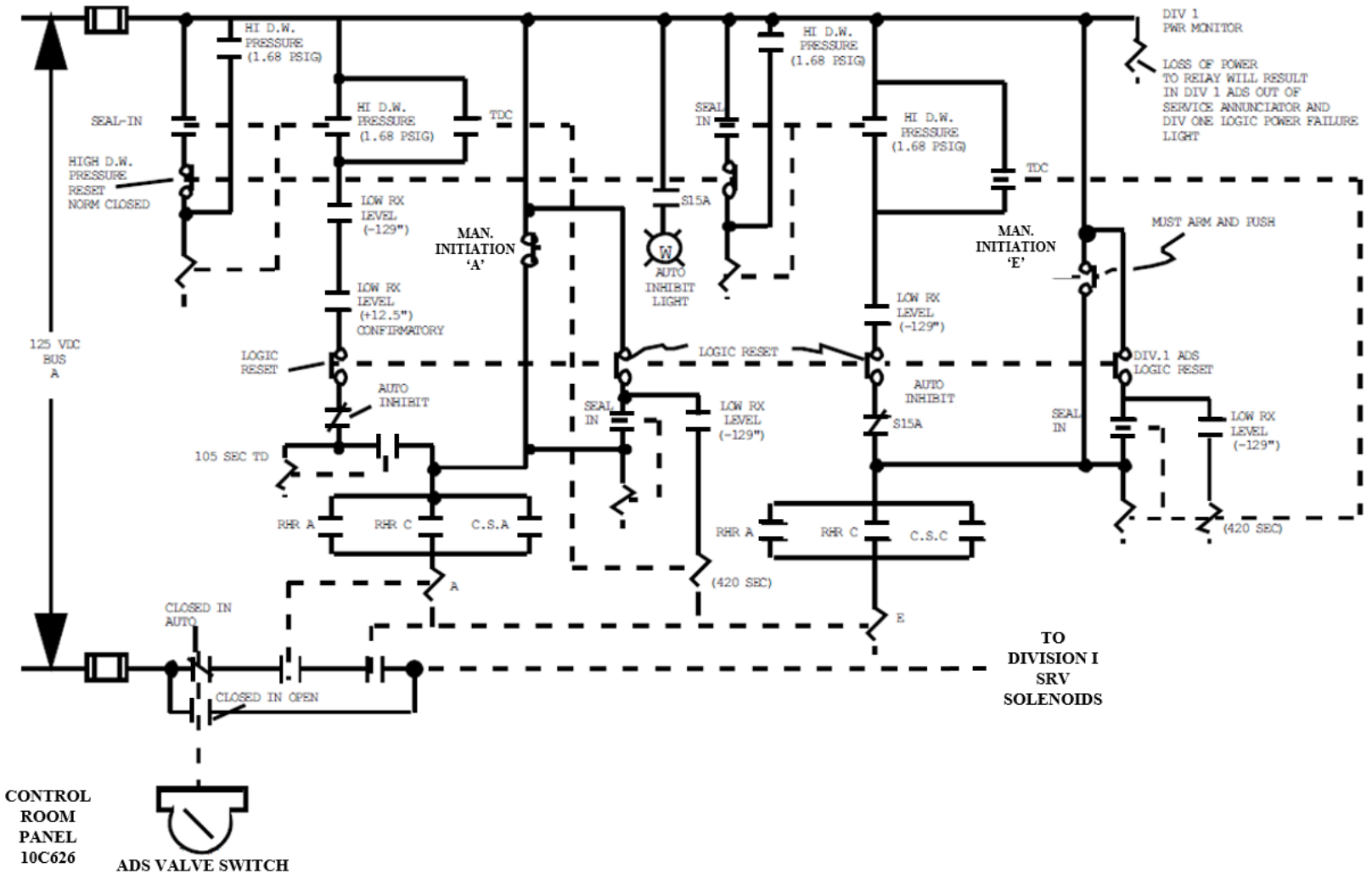

Figure 3-19. Division I ADS Initiation Logic (Reference 54)

Key features associated with the existing ADS logic include the following:

- The logic is powered by 125 VDC and is energize-to-actuate, consistent with other ECCS logic.
- Initiation of ADS logic requires both channels within an electrical division to actuate, using the following inputs:
  - Low Reactor Vessel Water Level 1 (both channels)
  - Low Reactor Vessel Water Level 3 (confirmatory low level, Channel A only)
  - High Drywell Pressure[5] (both channels)
  - 105-second delay relay timeout (Channel A, relies on both Reactor Vessel Water Level and Drywell Pressure permissives)
  - ECCS pumps running (RHR A or RHR C or both CS A and CS C)
  - ADS not inhibited.
- Operators are provided with the option of manually initiating ADS, provided that the required ECCS pump(s) are operating (buttons for both channels in one division must be depressed).
- ADS can be inhibited using one switch per division (both must be inhibited to ensure no initiation).
- ADS logic can be reset at any time by depressing the reset pushbuttons.

[5] The high Drywell Pressure permissive is bypassed if 420 seconds have elapsed since Reactor Vessel Water Level was ≤ Low Level 1. As a result, ADS will initiate regardless of drywell pressure after 420 seconds, provided that all other permissives are met. This timer protects against breaks outside the drywell. In these cases, the Drywell Pressure permissive may not be established, even though the Reactor Vessel Water Level was low enough to indicate that a primary break had occurred.

Table 3-7. ECCS Initiation Signals and Logic

System	Initiation Signals	Logic
CS	Reactor Vessel Water Level at or below Level 1 Low Reactor Vessel Pressure AND High Drywell Pressure Manual initiation	2oo2 (per division) (see Figure 3-17) 1oo1 (manual initiation only, per division)
RHR – LPCI Mode	Reactor Vessel Water Level at or below Level 1 Low Reactor Vessel Pressure AND High Drywell Pressure Manual Initiation	2oo2 (per division) (see Figure 3-17) 1oo1 (manual initiation only, per division)
HPCI	Reactor Vessel Water Level at or below Level 2 High Drywell Pressure Manual initiation	1oo2 (taken twice) (see Figure 3-18) 1oo1 (manual initiation only)
ADS	Reactor Vessel Water Level at or below Level 1 AND High Drywell Pressure AND Reactor Vessel Water Level at or below Level 3 Manual initiation	See Section 3.2.3.1 for full description of ADS logic
RCIC	Reactor Vessel Water Level at or below Level 2 Manual initiation	1oo2 (taken twice) 1oo1 (manual initiation only)

While only ECCS functions are described in the table above, the modernized system will automate additional manual RHR system functions in the PPS platform.

The RHR system executes a number of functions beyond its ECCS LPCI mode including the following:

- Suppression Pool Cooling: The RHR system limits the Suppression Pool temperature through the use of RHR heat exchangers and recirculating the Suppression Pool contents.

- Containment Spray: The RHR system can be used to spray the drywell or Suppression Pool when emergency conditions (e.g., high Drywell Pressure) dictate that these functions are required.

- Shutdown Cooling: The RHR system supports decay and sensible heat removal during shutdown conditions by recirculating the reactor coolant system through the RHR heat exchangers.

- Fuel Pool Cooling Assist: The RHR system can be used to supplement the Fuel Pool Cooling System by aligning the valves and sending the Spent Fuel Pool inventory through the RHR heat exchangers.

- RHR Drain to Radwaste: This mode of RHR supports Reactor Vessel Water Level drain down or Suppression Pool level control by providing a path for these volumes to Radwaste for collection and processing.

The functions above are controlled using a number of interlocks that ensure the LPCI mode is prioritized. Entry into these modes is done deliberately with consideration for any isolation or injection signals that may be present.

3.2.3.2 ECCS Technical Specification Surveillance Requirements

Testing the existing ECCS is performed through a series of manually-executed evolutions. Many of these evolutions are driven by existing TS SRs to verify that the ECCS remains operable in all applicable modes of operation. The independence associated with the existing system architecture permits the testing of individual system components (e.g., sensing instruments) as well as individual channels. The existing ECCS I&C architecture provides sufficient flexibility such that the removal of one input from each subsystem's initiation logic will not result in inadvertent actuation and will not prevent system actuation, if required during service or test activities.

The following service and test functions are applicable to the ECCS:

- Logic Functional Testing: These tests verify that the initiation logic associated with each ECCS subsystem operates satisfactorily by exercising the various elements of the individual logic strings. Logic relays can be exercised by means of plug-in test switches or in conjunction with sensor calibration activities (see below). Logic functional testing verifies that all components from the sensor to the actuator, including the logic, function correctly.

- System Functional Testing: The ECCS subsystems and RCIC can be functionally tested during normal plant operation (with the exception of ADS) to exercise pump starting and

valve stroke capabilities. Full-flow testing is performed using dedicated test lines to prevent the introduction of water into the reactor vessel under operating or shutdown conditions. While these tests are largely focused on the mechanical aspects of system operation (and not I&C), they are mentioned here for completeness. ADS must be tested during outage conditions (individual SRVs may be tested at low power during startup).

- Channel Check: Operability of individual process inputs to the ECCS I&C architecture are verified by cross-checking readings from one channel to the other channels to verify that each input is within a certain tolerance of the other inputs. These channel checks satisfy current TS SRs for the system.

- Calibration: Channel trip units and trip relays and instrument channels can be calibrated and tested by injecting a calibration signal. Calibration may also be performed on the sensing instruments that provide inputs to the ECCS I&C architecture by applying test pressures to the individual instruments. Calibration is used to verify that the operating range of the component has not drifted out of the acceptable region.

3.2.3.3 ECCS Separation and Independence

Separation associated with the various ECCS subsystems is generally structured to ensure that no single failure can prevent core cooling when required. This is illustrated in Table 3-8 below, which shows that the loss of one division of ECCS does not result in the loss of functional capabilities provided by redundant divisions of the same system (i.e., RHR and CS). For HPCI, functional redundancy is provided by the ADS, which actuates in the event that HPCI has failed to control Reactor Vessel Water Level following a small break LOCA. The HPCI system itself is not required to meet single-failure criteria as a result of this functional redundancy. Mechanical and electrical separation between the ADS and HPCI systems provides assurance that this functional redundancy is not challenged. Although not credited as part of ECCS, the RCIC system provides additional functional redundancy for the HPCI system, due to the fact that it is also a steam-driven, high-pressure injection system used for reactor isolation conditions (i.e., MSIVs closed with loss of normal feedwater).

Table 3-8. ECCS Separation

Division 1	Division 2	Division 3	Division 4
CS Train A	CS Train B	CS Train C	CS Train D
RHR Train A	RHR Train B	RHR Train C	RHR Train D
ADS Train A	HPCI (including outboard isolation valve)	ADS Train C	HPCI (including inboard isolation valves)
RCIC[1] (including outboard isolation valve)		RCIC[1] (including inboard isolation valve)	

Notes:

(1) RCIC is not part of the ECCS but is included here for illustrative purposes and to support discussions regarding redundancy, separation, and independence.

Channel independence associated with the various ECCS subsystems is provided through mechanical and electrical separation. Sensing instruments that support the initiation signals described above are located on instrument panels widely separated from each other and are identified as belonging to one of four divisions. For CS and RHR sensing instruments, the various instruments used to support each system are divided amongst four instrument panels. For HPCI and ADS, each system makes use of instruments in two separate divisions, as shown in Table 3-8 above. Separation for RCIC sensing instrumentation follows the same principles associated with HPCI and ADS with respect to the mechanical and electrical separation for the two divisions used to support RCIC operation.

In addition to the sensing instrumentation separation described above, the relay cabinets associated with ECCS subsystems and RCIC also satisfy governing design requirements for channel separation and independence. Relay cabinets for each CS and RHR division are located in separate areas. These cabinets are supported by separate 125 VDC Class 1E power supplies. Divisional splits exist all the way from the process parameter taps associated with sensing instruments to the final control element, including control and motive power supplies.

3.2.3.4 ECCS Connections and Internal Interfaces

Physical connections to the ECCS I&C architecture are currently terminated at the respective cabinets identified in Section 3.2.3.10 below. In the modernization, field terminations associated with the existing ECCS cabinets will be maintained, and new connections between the existing field terminations and the logic solvers will be made. Non-safety related connections that interface with the ECCS are provided with sufficient isolation to ensure that a fault associated with the interfacing system will not prevent the ECCS from performing its specified safety functions. This includes the use of isolation between the ECCS, the annunciator system, and the PPC. Detailed discussions regarding these interfaces are provided in subsequent sections.

There are no internal communications between divisions and channels of the ECCS I&C architecture, as described above in the separation and independence discussion. However, there are a number of sensing instruments that are shared between the various ECCS subsystems and RCIC. These include Reactor Vessel Water Level transmitters, Reactor Vessel Pressure transmitters, and Drywell Pressure transmitters. In general, the CS system is responsible for providing the LOCA signal to other plant systems, including RHR. Existing relays associated with LOCA signal generation are part of the CS system.

3.2.3.5 ECCS Human-System Interface

The ECCS contains a significant number of HSIs, due to its extensive use in responding to abnormal plant conditions. Certain system functions (e.g., RHR Suppression Pool cooling, drainage to Radwaste) are also used during normal plant operation to support testing and other activities. This necessitates an appropriate suite of HSIs for operators to carry out these functions. Table 3-9 below identifies the existing HSI interfaces and functions and denotes whether these will be impacted by the modernization.

Table 3-9. Existing ECCS Human-System Interfaces

Interface	Function	Modernization Impacts
Analog Trip Units	Analog trip units located in the AER are used to support testing activities (e.g., trip and calibration activities) and TS-required channel checks using the analog indicators.	The analog trip units will be removed entirely. The bi-stable function currently executed by the trip units, where the input value is compared to the established set point, will be replaced by application software on the new digital platform. The data currently displayed on the trip units will be provided on CR video displays.
Manual Initiation Push Button Switches	Manual initiation of the various ECCS subsystems is accomplished through the use of 13 pushbutton switches. One pushbutton switch is provided for manual initiation of the RCIC system. Operation of these switches accomplishes initiation of all functions performed by automatic initiation circuitry.	The ECCS manual initiation pushbutton switches will be replaced using soft controls as part of this modification.
ADS Inhibit Switches	Two inhibit switches (one per division) are provided to inhibit operation of ADS if required during an emergency condition. Automatic initiation of ADS is not desired during emergency response.	The inhibit function currently provided by the tactile switches will be transitioned to soft controls as part of this modification.
Manual Equipment Operation Switches	Numerous tactile control switches are provided to manually operate the ECCS equipment described above, including pumps and valves.	All tactile control switches will be replaced with soft controls as part of this modification.
Flow Indicating Controllers	The HPCI and RCIC systems each use a FIC to provide operators with a method for controlling pump speed based on an automatic flow set point or a manually-set controller output. The FIC output controls the speed governor for each systems steam-driven turbine. The FIC supports operation in flow, level, or pressure control mode, depending on the nature of the transient.	The FICs will be removed. Their function will be incorporated into the PPS, providing the existing flow control and adding Reactor Water Level and Reactor Pressure control capabilities. The RO HSI is driven by DKT soft controls as part of this modification.
ECCS Reset Switches	Each ECCS subsystem contains one or more reset switches to support resetting the initiation logic once the initiating conditions have cleared. This provides a mechanism for returning equipment to their normal standby lineup or alternative lineup required for transient mitigation.	The ECCS reset switches will be replaced with soft controls as part of this modification.

Table 3-9. Existing ECCS Human-System Interfaces

Interface	Function	Modernization Impacts
ECCS Indicating Lamps	Indicating lamps are used to denote the position of system valves, pump motors, and system initiation status.	The ECCS indicator lamps will be provided on CR video displays.
Process Parameter Indicators	Various analog indicators are employed in the main CR to provide operators with the following indications: Flow rates Pressures Temperatures Running currents Turbine speeds (HPCI/RCIC) Vibration monitoring	Analog indicators in the CR will be replaced with CR video displays as part of this modification. Vibration monitoring will not be affected.
ECCS Annunciators	Manual and/or automatic ECCS inputs are annunciated in the main CR through the use of isolated relay contacts. Tripping of the associated ECCS logic strings is also annunciated.	Existing annunciation tiles will be retained. Data will be displayed on CR video displays as part of this modification. These tiles are non-safety related and may coexist with the new displays.
PPC	The PPC provides indications of ECCS trips.	The functionality of the PPC interface will not be impacted by the proposed modification.

3.2.3.6 ECCS Connections between Safety Systems

The ECCS interfaces with a number of safety systems to execute its specified safety functions. These safety systems include the following:

- Class 1E Power System: The Class 1E power system provides support for the ECCS I&C architecture. Specifically, 125 VDC is provided from the station batteries to energize the various control logic arrangements described above. The station batteries also provide power for the HPCI and RCIC equipment that is actuated by the initiation logic (e.g., valves, auxiliary oil pump, vacuum pumps, etc.). Broadly, the Class 1E power system provides motive power for the various pieces of actuated equipment associated with each ECCS subsystem.

- Diesel Generator and Auxiliary Systems: The ECCS interfaces with the EDGs through the CS initiation logic. Receipt of a LOCA signal in any one of four CS divisions results in an automatic start of the division's respective EDG.

- N4S: HPCI and RCIC valves are isolated in response to signals generated by the N4S. Additionally, the N4S also supports other ECCS process pathways by closing the CS test return valves and RHR containment spray valves in response to LOCA conditions.

- Nuclear Boiler System: Numerous inputs are provided from Nuclear Boiler System instrumentation to the ECCS. These inputs include Reactor Vessel Water Level, Reactor Vessel Pressure, and Drywell Pressure. These signals are generally sent directly to the ECCS in the form of a 4–20 mA signal.

3.2.3.7 ECCS Connections to Non-Safety Related Systems

The existing ECCS interfaces with the following non-safety related systems:

- Remote Shutdown System (RSS): The RSS does not interface directly with the ECCS subsystems. However, the RSS does interface with RCIC and the RHR shutdown cooling and Suppression Pool cooling modes. RCIC and non-LPCI RHR modes are within the scope of this LAR. However, the PPS modernization will be designed to not affect RSS capabilities or controls.

- Annunciator System: The non-safety related annunciators provide audible and visual indication to operators regarding critical and noncritical events associated with the ECCS. Outputs from the ECCS are provided through the network to the DCS, which then provides contact closure outputs to the annunciator system.

- PPC: The ECCS interfaces with the PPC to support event logging of ECCS channel trips and other events. Communicated data from the ECCS are electrically isolated from the PPC.

3.2.3.8 ECCS Temporary Connections

Temporary connections associated with the ECCS are made on an as-needed basis. These connections are typically used to support the performance of the manual testing activities (e.g., trip unit calibration).

3.2.3.9 ECCS Interface with Supporting Systems

The 125 VDC station batteries provide power supplies for ECCS initiation logic described in previous sections. Power for actuated equipment (e.g., pumps, valves) is provided by additional elements of the Class 1E power system. The ECCS I&C equipment is located almost entirely in the AER, with the exception of the control switches located in the main CR. The Control Enclosure Chilled Water System and associated unit coolers are required to ensure operation of the ECCS components located in these areas to ensure compliance with their environmental design requirements. The mechanical and electrical equipment actuated by the ECCS I&C architecture is located in the unit-specific reactor enclosures and emergency switchgear areas. Continued operability of this equipment is contingent on properly functioning HVAC.

3.2.3.10 ECCS Physical Location of System Equipment

The existing ECCS I&C equipment is located in various cabinets in the AER. As discussed in Section 3.2.3.3, these cabinets are appropriately separated to ensure that ECCS safety functions are not jeopardized due to events within the cabinet vicinities. Mechanical equipment associated with the ECCS (e.g., pumps, valves) is located in the reactor enclosure. Electrical equipment

supporting the ECCS is located in various locations throughout the plant, depending on the associated power supply (e.g., 480 VAC motor control center, 4 KV bus). The main CR contains a significant portion of the HSIs described in Section 3.2.3.5 with the exception of the analog trip units, which are located in the AER.

The modernized digital equipment will be installed in the AER in the same cabinets as the original ECCS I&C equipment. The modernized equipment provides the software-based data acquisition, bi-stable, timing, logic solving, and output drive to replace the analog trip modules, pneumatic time delay relays, relay logic, and contractors in the existing architecture.

3.2.3.11 ECCS Use in Post-Accident Monitoring

The ECCS is used extensively to support post-accident recovery. The following ECCS parameters are required to satisfy the existing licensing basis requirements for PAM:

- HPCI flow indication
- RCIC flow indication
- RHR LPCI flow indication
- RHR-Suppression Pool spray indication
- RHR-Drywell spray indication
- CS flow indication
- RHR heat exchanger outlet temperature.

In addition to the specific parameters above, there are additional PAM requirements associated with ECCS valve position indication. These are largely focused on injection valve and test valve positions to monitor injection pathways.

3.2.3.12 ECCS Bypass and Status Indication in Control Room

System status is automatically indicated in the main CR to alert operators that a system is inoperable. Annunciation occurs whenever a system or part of a system becomes inoperable. Control switches are also provided to manually actuate the out-of-service annunciator. Manual actuation is also provided for the out-of-service annunciators for instruments that are removed from service for calibration.

3.2.4 RRCS Existing Architecture (DI&C-ISG-06 D.2.1.1)

The RRCS, which implements the ATWS mitigation function, provides diverse methods for shutting down the reactor, following a failure of the RPS to accomplish its specified safety function. This LAR Framework Document does not seek approval for modifying the existing RRCS or for replacement within the DAS. Information relative to the RRCS is in UFSAR (Reference 41) Section 7.6.1.8.

3.3 MODERNIZED PPS SYSTEM ARCHITECTURE (DI&C-ISG-06 D.2.2 AND D.2.2.1)

Software for the RPS, N4S, and ECCS functions within the PPS will be built as three separate, segmented applications. There will be no logical connects between the RPS, N4S, or ECCS functions. However, the PPS channels will collect data for the PPS and provide that data, including votes to scram or actuate, to the divisions within the PPS.

The modernized PPS data inputs, logic solvers, field outputs, DKT Interfaces, and automatic DKT Switches will be installed in the AER. The switching function in the DKT Switches is controlled from the DKT keyboards. In the CR, a limited number of indicator lamps will remain, which will be driven by the PPS. In the CR, a limited number of manual switches will be retained, which will be sampled by the PPS. Only those manual switches that are required to operate after the postulated PPS software common cause failure will be hardwired to the field. All other manual switches will be implemented as soft controls in PPS application software. The DKTs will be installed in the CR and AER. Analog inputs will be filtered appropriately to ensure deterministic timing is maintained and to minimize spurious actuations based on noise on the input wiring.

The modernized PPS design will provide redundant fiber optic communication links to send data from each channel to both divisions. The modernized ECCS design also will provide data separation in the channels and divisions for display and data provision to the non-safety related DCS data network, which will provide data to the PPC.

The existing field terminations in the AER cabinets will be maintained. The existing connections between the CR and AER will be maintained, although some wiring will be abandoned in place. Communication for the DKTs between the CR and AER will require the addition of new fiber optic cable. New internal connections between the logic solvers and the existing field connections will be added. The existing connections between safety-related systems will be maintained. The existing supporting systems will continue to be used by the PPS. The existing connections to non-safety related systems will be retained. Any connections to non-safety related systems or equipment will be isolated using qualified isolators.

The modernized design will retain the same logical and functional independence between channels, between divisions, and, with the transition from analog to digital, between data.

Each channel and each division will be implemented in one or more instantiations of the vendor's prequalified platform. The number of vendor's platforms will be based on maintaining the independence as described in the previous paragraph and on the throughput of the vendor's platform and the amount of software logic that each platform can execute, while still maintaining the required maximum delay from channel inputs and logic, through the communication links from channels to divisions and through each division's logic and discrete outputs.

TBD/TBC 16: Change above paragraph to reflect selected platform

Each channel will perform the bi-stable function on each analog input and send the channel's independent votes to scram or actuate to all divisions. All divisions will perform appropriate

voting on the results from all channels and determine whether sufficient channels are voting to initiate a scram or actuation.

The existing RPS, N4S, and ECCS systems use multiple independent, duplicated sets of field transmitters, for each channel for each existing system. There are several identical transmitters mounted to the same instrument tubing with identical calibration, using the same calibration procedures, but hardwired to one analog trip module in one of the existing RPS, NSSS, or ECCS systems. Those identical sets of transmitters will be removed, and all PPS functions will use a single set of redundant field transmitters. This condition also exists for analog trip units, whose functions will be combined when appropriate.

The modernized design will consolidate (eliminate) redundant copies of individual channelized sensors provided in the original design. The PPS channels will sample all data from the remaining sensors and provide the same data to the RPS, N4S, and ECCS functions of the PPS. This functionality will be simple to perform in software, will not compromise system independence, and will enhance PPS reliability through the elimination of components. The automated channel checks, along with more sophisticated analytics in the future, will not require multiple copies of the same sensed variable in one channel. The PPS will operate using consistent data in the RPS, N4S, and ECCS functions.

The CR will maintain a selected subset of the existing manual initiation switches, supplemented with soft controls on the DKTs. The function of the initiation switches is duplicated in soft controls on the DKTs.

The modernized design will eliminate the reset, bypass, test, and other similar switches, which will be soft controls on the DKTs. The eliminated switches will include the RPT Inhibit Switches, MSIV Closure Scram Test Switches, TSV Closure Scram Test Switches, and SDV Isolation Valve Test Switches.

The operator will initiate any of these soft controls that affect protective functions through two disparate actions (e.g., two trackball clicks or two screen touches) on the DKTs. The first operator action will select the requested function, while the second action will be required to initiate the selected function at a different screen location. The DKT will provide the means to cancel a selected function. If the operator does not initiate the selected function and the required second action within a preset timed interval, the selection will be removed.

The remaining manual operator switches will be designed such that PPS software common cause failure will not disable the manual control. Software common cause failure will not prevent the operator from taking any required manual action, based on the manual controls to be provided in the CR.

The PPS will be designed for ease of maintenance. The PPS will identify, to the chassis and module, any faulted or failed field-replaceable unit, along with identifying the failure. The PPS will be designed for hot swap of field-replaceable units, allowing the PPS to continue operation while the module is replaced.

Figure 3-20 below shows the data separation in the channels and divisions for display and data provision to the non-safety related DCS data network to be provided in the modernized PPS.

Each channel and division pair will provide data to the displays and DCS data network. The channels will not provide field input analog and discrete input data to the divisions, to avoid the potential for divisions using the field data inappropriately. The display units will not cross between channels or between divisions to avoid creating the appearance of multi-division displays. The divisions will provide the votes from the channels, status for the channels and division, output states (i.e., scram or not scram, actuate or not actuate), and bypass information, including measured field states.

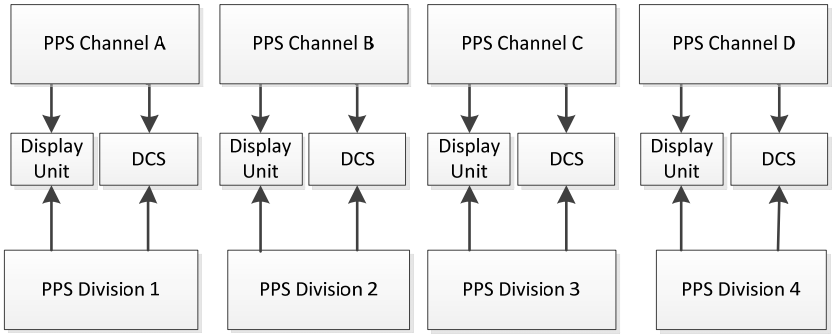

Figure 3-20. Modernized PPS Data Display and Recording

Note that some functions do not use all four divisions, with the same design as is provided in LGS. The RPS uses only Divisions 1 and 2. In the ECCS, HPCI uses only Divisions 2 and 4. In the ECCS, RCIC and ADS use only Divisions 1 and 3, as defined in UFSAR Table 7.1-6 (Reference 41). In the N4S, divisional assignments are provided in UFSAR Table 7.1-6.

The modernized PPS will be designed to detect and mitigate malfunctions in hardware, software, and communication. The modernized PPS and interface to the DCS will be designed to identify faults and failures in field sensing equipment. To the extent practical with the existing field actuated devices, diagnostics will determine the health of the connection to the device. The modernized PPS and interface to the DCS will support the continuous performance of channel checks in the DCS, including checking DAS input data against the PPS input data.

In the existing system, the field analog input values are displayed only in the AER. In the modernized PPS, the field analog engineering unit values will be displayed on the DKTs and made available to the non-safety related DCS for diverse display, for use in the Emergency Plan, and for preservation in a data historian. PPS status information will also be displayed on the DKTs, replacing various indicating lamps and annunciator windows.

Unlike the existing system, the modernized PPS will communicate data to the DCS, which will then provide direct isolated outputs to the annunciator, to ensure alarm notification. Selected PPS events will be annunciated.

The DKTs will also provide BISI for each of the functions within the PPS as well as for the overall PPS.

The PPS will be designed and implemented to avoid adverse interactions with the RSS.

Separation and independence in systems and divisions are evaluated in Section 3.8.2 below.

3.3.1 Modernized PPS Architecture: General Concepts (DI&C-ISG-06 D.2.2.1)

The PPS logic will perform all timing, seal-in, voting, and other logic previously provided in relays. The timing will be a multiple of the scan rate if a microprocessor-based system is used, and any inaccuracy in timing will need to be addressed in a design evaluation. Channels A and B will be powered by Division 1 power. Similarly, Channels C and D will be powered by Division 2 power. The field inputs for each channel and channel power supplies will be isolated and independent from each other.

A general architecture for the PPS is provided in Figure 3-21 below. The modernized design will incorporate cross-divisional connections from all channels to all divisions (i.e., voters or logic solvers). There will be no cross-connects between channels or between divisions, as no channel can communicate with another channel, and no division can communicate with another division, by either discrete I/O or communication links. The channel bypass switch will be common to all divisions but will be electrically isolated. The modernized design will eliminate all the existing design's discrete output to discrete input connections from Channels A and B to Division 1 and from Channels C and D to Division 2.

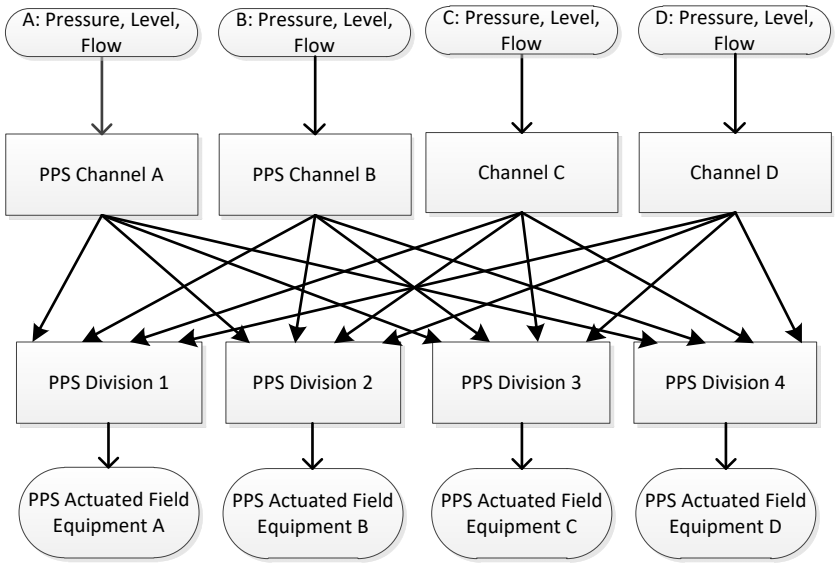

Figure 3-21. Modernized PPS System Signal Flow

All the RPS, N4S, and ECCS logic will be absorbed into independent functions within the PPS divisions. The RPS, N4S, and ECCS will remain as separate functions within the PPS.

Physical separation of inputs to the channels will be maintained, as described in Section 3.1.1.

The existing RPS, N4S, and ECCS have independent field sensing, but the field sensing is sometimes connected to one system and used in another. For the modernized PPS, all field data will be sampled by each of the PPS channels and evaluated to determine votes to scram or actuate (or not scram or not actuate). The PPS channel data will be shared to all PPS functions, including RPS, N4S, and ECCS.

The modernization will not affect CR indicator lamps, annunciator windows, and meters not associated with the RPS, N4S, and ECCS functions. The modernization will replace the indicator lamps, meters, recorders, and selected annunciator windows associated with the RPS, N4S, and ECCS functions with displays on PPS and DAS DKTs (see Sections 3.3.5 and 3.4.5). As the LGS transformation progresses, the remaining meters are planned to be absorbed into the DAS, but that evaluation, replacement, and relocation is not part of this LAR. Any CR indications required to be diverse from the PPS application software will be driven directly by field inputs.

Limited manual RPS, N4S, and ECCS switches and pushbuttons will remain in the CR. Automated soft controls will be provided by the DKTs for both the PPS and the DAS, as described in Section 3.3.5.

For each of the manual action pushbuttons and switches retained in the CR, the PPS will sample the state of each switch. The PPS will provide the pushbutton and switch change of state data to the DCS for uses including historical data retention. The PPS software will sample the manual operator action and update internal PPS states as necessary to match the operational state of the plant. The PPS could, but does not, "shadow" the operation of the manual operator actions, to provide a diverse path to ensuring that safety functions occur.

The modernized PPS will have relay outputs to drive sequence of events (SOE) and annunciator first-out windows. The delay through the contacts will be minimized to support SOE and first-out scram indication and to reduce the uncertainty associated with identifying the initiating event. These output contacts will act as safety to non-safety related qualified isolators, providing hardwired SOE and first-out data to the non-safety related user.

The PPS will provide all alarm status, including the SOE and first-out, data over one-way communication links from the PPS to the non-safety related DCS. The non-safety related DCS will then provide contact closures to the annunciator, eliminating the safety-related hardware that would have been required had the PPS driven the annunciator directly.

The safety-related system will not synchronize to the highly accurate date and time provided in the DCS, reducing the complexity of the PPS application and eliminating the need to send non-safety related date and time to the PPS and to synchronize the PPS date and time with the DCS date and time. Thus, the safety-related system will not time tag SOE and non-SOE data. The DCS will time tag the time at which the DCS receives change of state messages. In a future modification (not part of this LAR) that eliminates the annunciator, the DCS could then capture SOE and first-out data using SOE discrete input boards, which the DCS maintains in accurate time synchronization, based on the high accuracy, redundant DCS time source. Efforts will be made in design and implementation to ensure that the delay from the PPS logic through the contact change of state is minimized and deterministic (i.e., fixed and non-varying).

The PPS will provide a maintenance bypass of channels for one channel at a time, as described in IEEE Std. 603 (Reference 4), Clause 6.7, in the RPS, N4S, and ECCS functions. The PPS will ignore the bypass request if a channel other than the channel for which the bypass is being requested is already marked as bypassed or failed.

In the modernized system, when one channel is placed in maintenance bypass, the divisions will automatically implement a reduction in voting requirements (e.g., 2oo4 reduced to two-out-of-three [2oo3] voting) within each division. If another channel fails, the divisions will further reduce the voting requirements (e.g., 2oo4 reduced to 2oo3 for maintenance bypass, then reduced to 2oo2 on the failure of another channel). If insufficient channels remain in service (e.g., one or two channels of the original four, no channels for a 1oo2 voting), the PPS will scram or actuate both divisions.

Similar actions will occur if there are only two channels providing data to multiple divisions, voting either 1oo2 or 2oo2. If one of the channels is in maintenance bypass, the divisions will drop to 1oo1 voting. If the remaining channel fails, the division will actuate.

For the case where 4oo4 voting will be used, while one channel is in maintenance bypass, a four-channel function with multiple divisions will continue to operate, with a reduction in voting requirements (e.g., 4oo4 reduced to 3oo3). If another channel fails, the division will further reduce the voting requirements (e.g., 4oo4 reduced to 3oo3 for maintenance bypass, and then reduced to 2oo2 on the failure of another channel). In 4oo4 voting, if one channel or no channels remain, the PPS will actuate.

Other than a resolution of actual hardware failures, there is no identified reason to place a division in maintenance bypass. Thus, the design of divisions will not include a means to place the division in maintenance bypass. With the elimination of many surveillance tests, the expectation is that the maintenance bypass of a channel will occur much less often. During the time that a channel maintenance bypass is in place, the watchstanding ROs and SRO will operate in heightened awareness.

Requirements for manually implemented service and test functions will be replaced by self-test and self-diagnostics as much as possible, to reduce subsequent impacts on plant performance and to reduce workload. This includes errors in use of test points and installed electrical signal isolation to eliminate lifting/landing signal leads. The existing service and test functions are identified in Sections 3.2 and 3.3.6.3. The required service and test functions will be determined as part of detailed PPS design.

For all PPS inputs that have the potential to require manual test insertion or external measurement of input values (i.e., the use of an external digital multimeter by a technician), test jacks will be provided in the cabinets. For all inputs that have the potential to require manual multipoint calibration checks with external calibration equipment, knife edge disconnects along with test jacks will be incorporated in the field termination panels. The terminal panels, wiring, test jacks, and knife edge disconnects will be commercial grade dedicated and considered basic components. The PPS design will minimize the requirements for calibration checks of the analog inputs to the logic solvers.

There will be additional logic and processing elements embedded in the cabinets. The modernization will replace some obsolete equipment in the cabinets for convenience. These logic and processing elements will include the following systems:

- The RPS cabinets will include the four independent divisions of GE NUMAC LDS. The modernization will replace the existing NUMAC chassis with direct input to PPS input modules and processing logic. The PPS will add display capabilities for all input data (thermocouples, cold junction compensation, and flows) in the CR, which currently does not exist.

- The RPS cabinets will include some data processing for the RWCU System. The modernization will replace these modules with direct input to N4S input modules and processing logic, mostly taking the square root of a differential pressure to generate flow.

- The ECCS cabinets will include the initiation logic for all four EDGs. The modernization will replace the existing relay logic and timers with direct logic implementation in the PPS.

3.3.2 Modernized PPS Architecture: RPS Specifics (DI&C-ISG-06 D.2.2)

The prequalified platform will be used as a basis for the modernization of the four PPS channels and two divisions of RPS logic. The primary architectural differences between the existing and the modified design will be in voting and HSI. The modernized architecture will keep the same analog and discrete process inputs from the field and drive the same discrete SSPVs and SOVs. The logic solvers will be installed in the existing AER cabinets. The PPS HSI will be installed in the CR and in the AER.

The existing RPS system architecture is described in Section 2.1.1. Figure 3-2 above shows the modernized RPS in the context of the PPS and DAS. The channels will generate individual votes to scram for each of the conditions defined in Table 3-3 above. In both figures, the inputs to the voting logic are from the bi-stable channel logic, which is not shown for clarity.

Figure 3-22 below shows the modernized RPS outputs portion of the PPS. The RPS will sample analog and discrete data from field sensors in the channels. The PPS will provide qualified isolators that provide non-safety related data to the DAS. The channels will perform the bi-stable function and provide the votes to scram or actuate to the divisions. The divisions will then output discrete signals to the field to initiate the required protective action.

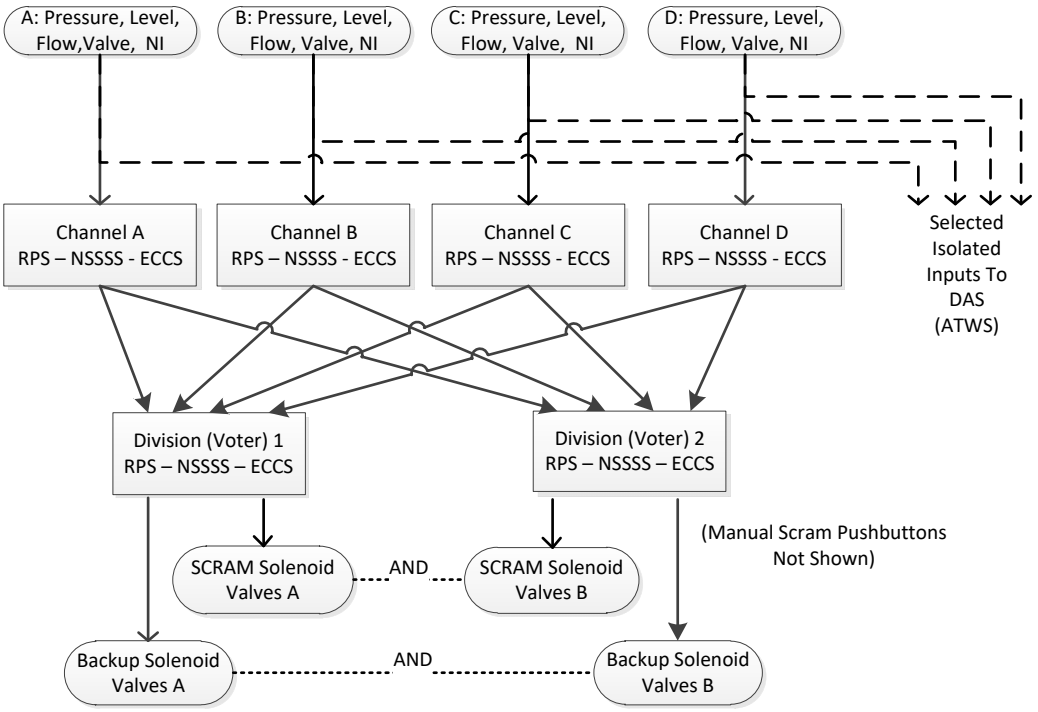

Figure 3-22. Modernized RPS System Signal Flow

The RPS will continue to drive the primary scram, backup scram, and SDV isolation separately. For primary and back scrams as well as for the SDV isolation, both divisions must vote to scram for a scram to occur. For both divisions and all outputs, the discrete outputs are single-failure tolerant, as shown in the Failure Modes, Effects, and Diagnostics Analysis (FMEDA, Reference 55). The primary scram design in each division will directly drive each of four groups of rod scram SSPVs. The logic solver will also drive the backup solenoids as well as the SDV isolation solenoids directly. The logic solver will provide diagnostics and monitoring of the coil continuity.

Each scram system has four rod group discrete outputs. The design will modernize the relay contacts with electronic circuits. The existing divisional set of four CR rod group power / scram lamps will be replaced with indications on DKTs. The existing lamps illuminate to show power being applied to the SOVs. The lamps extinguish when power is removed and the SOV is conditioned to scram. Each indicator provides the individual powered state of each rod group.

The control rod pattern display is not changed, and each control rod still has a light on the rod pattern display. A blue lamp for each of the 185 control rods illuminates when limit switches on each control rod HCU indicate that the rod is fully inserted (i.e., a full scram condition).

In the modernized RPS design, redundant fiber optic communication links will provide data from each channel (existing Channels A1, A2, B1, and B2; modernized Channels A, B, C, and D) to both divisions (existing Divisions A and B; modernized Divisions 1 and 2). If any two channels vote to scram, then the divisions will react to the votes to scram and generate a scram.

The modernized RPS design will provide data separation in the channels and divisions for display and data provision to the non-safety related DCS data network, as shown in Figure 3-20 above. Limited manual RPS controls will remain in the CR, as a pair of pushbuttons that initiate manual reactor scram, which directly cut off the power supplied to the primary and backup scram valves and initiate SDV isolation. Soft controls for all other manual actions (including a manual scram using the application software) will be provided by the DKTs for both the PPS and the DAS, as described in Section 3.3.5.

As required in 10 CFR 50.62 (Reference 8), DAS functions described in Section 3.3.5.3 will support the potential for failures, including software common cause failure, in the RPS. Based on the diversity of the PPS and DAS[6], either the PPS or the DAS will be available to support operation in normal and off-normal conditions.

As shown in Figure 3-23 below, the modernized manual scram buttons in the CR will be installed in a manner such that common cause failure of the channels or divisions cannot prevent the operator from initiating a scram through both the primary and backup SOVs and isolating the SDV. The wiring relocation will be required by the architectural change. The functionality will be changed such that the two scram pushbuttons must both be pushed to initiate a scram, which will release the relays that turn off the power to the SOVs. Other RPS pushbuttons will be moved to the DKTs as soft controls, including the divisional scram resets. The reset inhibit timers will be implemented in logic in the application software. The Divisions will start the reset timer as part of the scram logic. If the operator initiates a manual scram, the Divisions will use the power state from the groups of scram SOVs to initiate the reset timer, where two or more of the four group scrams associated with that division will initiate the divisional scram seal-in and the divisional reset timer, based on PPS knowledge of the operator manual scram action.

[6] The PPS is diverse from both the existing RRCS and the DAS built with DCS hardware.

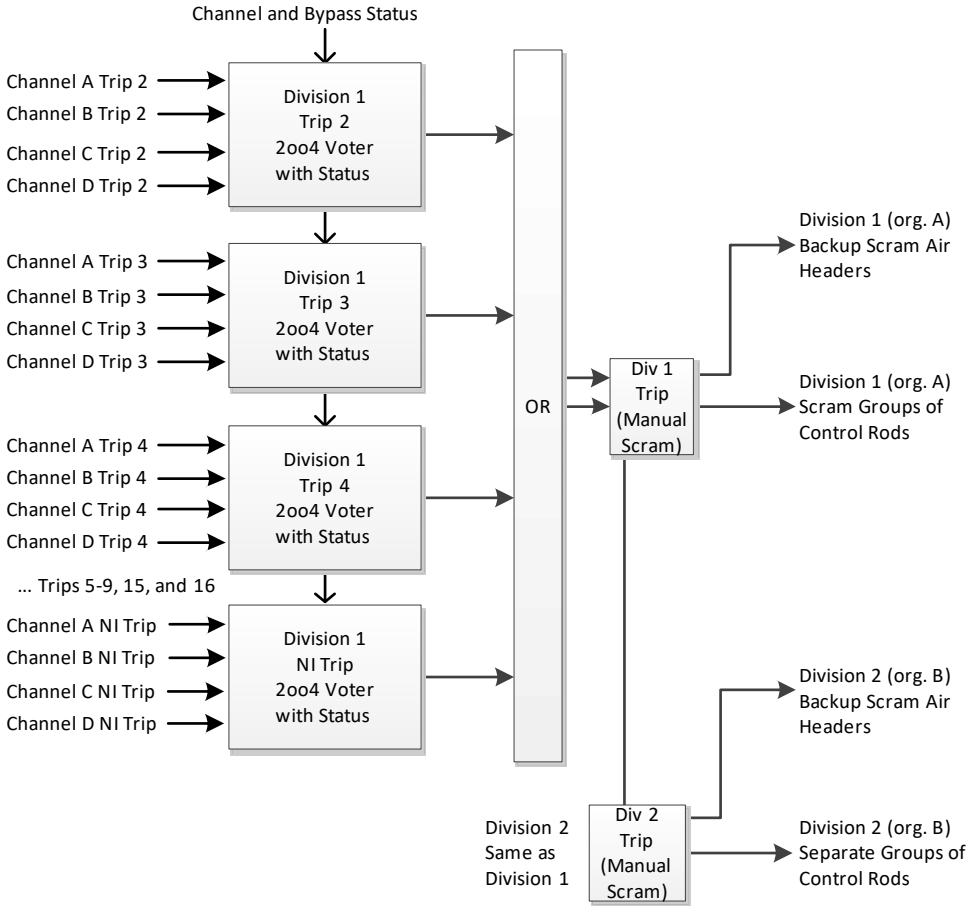

Figure 3-23. Modernized RPS Scram Voting

One other significant change will be provided in power to the RPS. In the existing system, Electrical Power Monitoring (EPM) breakers in each divisional power feed disconnects power to the complete RPS in the event of under voltage, over voltage, or under frequency, to protect (unidentified) RPS components. For the modernized RPS, the EPM is rewired to disconnect power only to the more easily damaged solenoid valves, leaving the PPS powered.

TBD/TBC 17: This may not be the appropriate action for the EPMs, but turning off PPS is not appropriate.

While the data provided by the DKTs is available for use, the RPS function will be not used for PAM.

DAS functions will be required to support the potential for software common cause failure in the RPS. The D3 Analysis (Reference 7) confirms that the ATWS portion of the DAS described in Section 3.3.5.3 provides sufficient coverage for any potential RPS software common cause failure.

3.3.3 Modernized PPS Architecture: N4S Specifics (DI&C-ISG-06 D.2.2)

The prequalified platform will be used as a basis for the modernization of the four N4S channels and four divisions of N4S logic. The primary architectural differences between the existing and the modified design will be in voting and HSI. The modernized architecture will keep the same analog and discrete process inputs from the field and drive the same discrete outputs to the field devices, which include valves and motors.

The existing N4S system architecture is described in Section 2.1.2. Figure 3-21 above shows the modernized PPS, which includes the N4S, without showing the interface to the DAS. The primary difference between the modernized N4S and RPS architecture is the segmentation of two divisions of voting logic within each of the two electrical divisions and the addition of more redundant fiber optic links to link the two new divisions to all four channels. The channels will generate individual votes to actuate for each of the conditions defined in Table 3-5 above. The four divisions will provide the taken-twice requirement, for those N4S functions that operate solely within one electrical division.

Some functions within the modernized N4S will be implemented in only two of the divisions, with data provided to only two of the channels. In the N4S, divisional assignments are provided in UFSAR Table 7.1-6 (Reference 41), which shows the divisional assignments for the N4S subfunctions. The channels will generate individual votes to actuate for each of the conditions defined in Table 3-5 above. The four divisions will provide the taken-twice requirement, for those ECCS functions that operate solely within one electrical division.

The N4S function will control inboard and outboard isolations for the potential leakage of radioactive materials from the reactor and reactor enclosure. The N4S system will provide several subfunctions that isolate specific pipes and ventilation ducts. Both the existing licensed and modernized designs are limited by the availability of field data. Some of the subfunctions have four channels of data available. Some of the subfunctions only require two channels of data, spread across two channels within a single electrical division. Some of the subfunctions only require a single channel of data, provided to only one division. There are parts of the existing and modernized N4S that provide only status information to the CR since the active logic is installed in the field.

In the existing system, some isolation conditions are initiated by each of the two channels in one division. One channel controls the inboard isolation, while the other channel controls the outboard isolation. The modernized design will split Division 1 into Division 1A and Division 1B, replacing the existing direct drive from channels with a voting scheme to divisions. Similarly, Division 2 will be split into a Division 2A and Division 2B. Each of the split divisions will be a separate, independent voting entity and will control the field equipment independently. This design change ensures that faults and failures in a single division will not preclude the isolation function. Using a voting scheme, both the inboard and outboard isolations will occur, and half-isolations will be precluded, since the divisions will be provided with the same votes to actuate.

The modernized N4S system will be changed to a channel and division architecture, rather than having the channels directly drive the isolation outputs. All four channels will provide all data to

the four divisions. Channels A and B and Divisions 1A and 1B will be powered from Division A electrical power. Channels C and D and Divisions 1B and 2B will be powered from Division B electrical power.

The voting within each division will be designed to reflect the isolation actuations that the specific division can perform. If the division has no control over a specific isolation, that division will not vote on that specific isolation, not using the data provided by the channels for that specific isolation.

There are four main steam lines, each of which can be isolated on detection of a leak. Each of the four main steam lines has four differential pressure (flow) sensors. The modernized logic will vote each main steam line (A, B, C, and D) independently. If the 2oo4 vote for one main steam line requires isolation, only that main steam line isolates. Each main steam line is isolated independently. The RPS monitors the isolated steam lines and scrams the unit if three or more main steam lines are isolated.

The PAM capabilities of the N4S function will not be affected, other than enhancing the data display with the DKTs.

As required, DAS functions described in Section 3.3.5.3 support the potential for software common cause failure in the N4S and will be selected based on the D3 Analysis (Reference 7).

3.3.4 Modernized PPS Architecture: ECCS Specifics (DI&C-ISG-06 D.2.2)

The prequalified platform will be used as a basis for the modernization of the four ECCS channels and two divisions of ECCS logic. The primary architectural differences between the existing and the modified design will be in voting and HSI. The modernized architecture will keep the same analog and discrete process inputs from the field and will drive the same discrete outputs to the field devices, which include valves and motors.

The existing ECCS system architecture is described in Section 2.1.3. Most of the modernized ECCS architecture is shown in Figure 3-21 above, without showing the interface to the DAS. The channels will generate individual votes to actuate for each of the conditions defined in Table 3-7 above. The changes from the RPS will be in the function of the field outputs, which will not control the scram like the RPS, but will provide controls for the ECCS equipment.

Some functions within the modernized ECCS will be implemented in only two of the divisions, with data provided to only two of the channels. HPCI is implemented only by Divisions 2 and 4. RCIC and ADS are implemented only by Divisions 1 and 3. The channels will generate individual votes to actuate for each of the conditions defined in Table 3-5 above. The four divisions will provide the taken-twice requirement, for those ECCS functions that operate solely within one electrical division.

The PAM capabilities of the ECCS function will not be affected, other than enhancing data display with the DKTs.

As required, the DAS functions described in Section 3.3.5.3 support the potential for software common cause failure in the ECCS and will be selected based on the D3 Analysis (Reference 7).

Based on the diversity of the PPS and DAS, either the PPS or the DAS will be available to support operation in normal and off-normal conditions.

3.3.5 Modernized HSI (DI&C-ISG-06 D.2.2)

3.3.5.1 Purpose of Modernized HSI

The advantages of a modernized, integrated, digital safety-related and non-safety solution include improved visibility of data in the CR and AER and the resultant plant staff flexibility. To provide this visibility, video displays will replace the traditional indicator lamps, annunciator windows, meters, and recorders in the CR. The expectation in most NRC documentation is that the CR will have strictly separate traditional safety-related video displays and separate, traditional non-safety related video displays. These separated, classified, spatially dedicated video displays show plant status as reflected in the data sampled by the systems, internal plant system status, and active control actions. Soft controls are also possible, where the operator performs manual functions on soft control implemented in the video display.

The requirements for the safety-related content of the DKTs will be evaluated by HFE. The DKT displays will be simple, usable, and easily navigated by ROs and SROs. The information displayed will be meaningful and necessary for use in monitoring and controlling LGS.

The traditional video display includes an interface to the logic solver, a video generator, a display, a keyboard, and an operator input device (e.g., touchscreen, trackball, or mouse) as an integrated unit, similar to a personal computer. Implementing this traditional approach in the CR has a weakness in that the design provides video display functionality only in spatially fixed CR locations. Safety-related video displays are assigned inflexibly to one of the several divisions (along with the divisionalized channels) and placed in fixed locations by division. There is a strict segregation of non-safety from safety-related video displays. The typical design installs safety-related video displays in fixed locations with specific functions, which the vendor designs into the equipment, to interface with the safety-related systems. The typical design installed non-safety related video displays as part of their DCS. These provide essentially unlimited non-safety related control system flexibility for the DCS video displays. While the modernized design will install DCS video displays in fixed locations, these video displays will be capable of interaction with any system within the DCS (as described in Sections 3.3.5.2 and 3.4.5), unless HFE requires fixed functionality on some of the DCS video displays.

As shown in Figure 3-24 below, the modernization proposes the use of a digital DKT architecture that enables sharing data on safety-related DKTs with any control and data system that watchstanding operators could need in the CR. This will include the safety-related systems (any channel or any division), the non-safety related DCS, and other systems such as the corporate business network. The DKT Switches will have redundant internal controllers and redundant power supplies, to maximize reliability. The redundant power supplies will be fed from separate safety-related power feeds for single-failure tolerance. The DKT switching design will ensure that no single failure and most double failures prevent data display and soft control in the CR.

To support this architecture, the DKT interface in the associated, serviced systems will be separate from the DKT. The serviced divisional DKT Interface will connect to both DKT Switches. The DKT Switch is a solid-state implementation of the traditional keyboard, video, and mouse (KVM) switch, which establishes the connection mechanism to the safety-related DKTs distributed throughout the CR. The DKT Interface transmits video signals to the display and receives data from the DKT keyboard and trackball through the DKT Switch. Once a DKT user in a particular location selects a DKT Interface and the equipment connects the DKT with an available DKT Interface, the user cannot tell whether there is a switching network or a direct connection between the DKT and the selected DKT Interface. Each serviced system will provide a sufficient number of DKT Interfaces to support the intended number of simultaneous DKT locations requiring access to a particular serviced system.

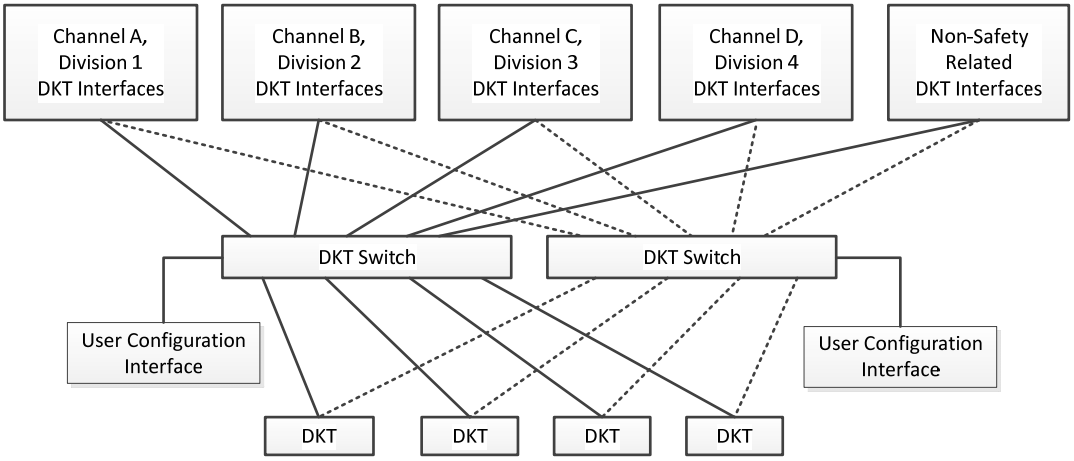

Figure 3-24. Proposed Display Switching Architecture

The only information retained in the DKT Switch system is the set of allowable connections between serviced system DKT Interfaces and DKTs in the internal configurable table. The DKT Switch system switches (i.e., directs) the information between the DKTs and the serviced system DKT Interfaces without retaining any information. The DKT Switch vendor designed and tested the DKT Switch to ensure that no cross linkage between DKT Interfaces or DKTs is possible, including cross-coupling between switched connections on the printed circuit boards within the DKT Switch.

DKT Interfaces will be powered from divisional power and interface with the DKT Switches through optical fibers. Similarly, DKT Switches will interface with the DKTs through optical fibers. The fiber optic connections provide electrical isolation between the DKT Interface and the DKT Switches and ensure that the DKTs have electrical isolation from the DKT Switches. The design of the DKT Switch ensures data isolation between DKT Interfaces.

To the extent practical, all CR and AER data and status display will be through the DKTs. The DKTs will provide soft controls for all operator actions. The required manual operator controls will be retained and reconfigured to support the modernized PPS. One or more reduced functionality DKTs will be provided in the AER to simplify maintenance by providing indication

of the PPS data for calibration or other maintenance activities. These DKTs may also be used to support the PPS EWS.

All DKTs and the DKT Switches (e.g., Thinklogical TLX80) will be commercial grade dedicated and evaluated to ensure compliance with critical characteristics that include separation of video streams and no cross linkage between streams. All of the DKT Interfaces (e.g., Thinklogical redundant video transmitters and receivers), DKT Switches, and DKTs are thus basic components. Thus, there are no concerns about controlling safety-related systems from non-safety related displays, since the design will not include non-safety related DKTs or multi-divisional DKTs. While DKTs can be connected to any safety or non-safety related system, no DKT can be connected to more than one DKT Interface, and, thus, the DKT is limited and restricted to accessing only one system at a time. The DKT Switch behaves as a traditional, mechanical A-B KVM switch, albeit with many more ports, more switching capabilities, software restrictions concerning connections, and much more flexibility. This design resolves DI&C-ISG-04 (Reference 44) concerns about multidivisional displays and use of non-safety related displays to control safety-related systems by eliminating the potential of occurrence of the base concern.

DI&C-ISG-04 (Reference 44) strongly discourages implementing safety functions from non-safety related video displays, especially in DI&C-ISG-04 Section 3.1 Item 3. The proposed DKT Switch architecture used with DKT and DKT Interfaces addresses this concern directly, while at the same time providing for a common and flexible HSI in the CR.

3.3.5.2 Generic HSI Architecture

TBD/TBC 18: LGS to define the current BISI indicators in the control room (and AER) that are related to RPS, N4S, ECCS, or DAS

TBD/TBC 19: The PPS BISI indicator lamps and annunciator windows will be removed by this mod (we are not going to add discrete outputs to drive indicator lamps)

For the proposed switched DKT architecture, each DKT Interface will provide distinct standard communication links from each safety-related division and channel to the DKT Switch. Each non-safety related DKT Interface will have communication links to the DCS virtual terminal server. Fiber optic communication links will connect each DKT Interface to a DKT Switch port and a DKT Switch port to each DKT. As many DKT Interfaces as are required will be implemented. The locations of DKTs will be known, and restrictions will be configured into the DKT Switches to preclude defined locations from performing defined functions.

All data and status sampled by and computed by each channel and division will be available for display by the DKTs in the CR and AER. Data will not be presented in volts, mA, or logical state (e.g., True or False). Analog data will be presented in engineering units. Discrete contact state will be displayed as a meaningful message that provides easily understood meaning (e.g., valve closed, pump running). As an example, the LDS temperature data will be presented with a clear identification of the plant location with the high temperature.

The modernized PPS will move the existing BISI in the CR for the PPS and DAS to DKTs. This design will add switched DKTs to provide the PPS engineering unit values, internal status,

actuated device status, results of self-tests and self-diagnostics, BISI, and other key information to the CR and to the AER on DKTs.

One use for at least one of the DKTs will be for continuously visible BISI, in accordance with NRC RG 1.47 (Reference 56) and NRC Generic Letter 85-06 (Reference 57). The administrative procedures under which the plant operates will be extended to a requirement for the watchstanding operators to choose one or more displays and always have the "continuously visible" BISI parameters on a DKT, which the watchstanding operators can easily identify. LGS concludes that this administrative requirement resolves the "continuously visible" regulatory requirement. Nothing in this LAR Framework Document or the design of the four systems of interest precludes this operation.

Redundant uninterruptible vital power will supply each DKT Interface, DKT Switch, and DKT, to avoid the potential for loss of CR data display. The power to the DKT Interfaces, DKT Switches, and DKTs will not fail with the loss of either electrical division source. At a minimum, the design will provide a power supply/DKT scheme, so that in the event of a loss of one safety-related electrical division source, sufficient DKTs remain operable to support full plant power operation.

Each DKT will be able to select one of the set of DKT Interfaces served by the DKT Switch if the switching network is configured to allow that connection. Each of the video links will provide sufficient bandwidth to support 4K video and will operate with imperceptible jitter. Each of the fiber optic links and the DKT Switches will maintain electrical isolation between electrical divisions as well as between safety-related and non-safety equipment on different power sources.

The expectation is that every DKT Interface and every DKT will provide acceptable video display and keyboard and trackball access to the DKT Interface. The user will be able to select each DKT Interface selection from the same keyboards and trackballs attached to the same DKT Switch, within the acceptable interconnection scheme configured in the DKT Switch.

The modernized design will use dual DKT Switches (e.g., Thinklogical TLX80). The DKT Interfaces will provide a dual fiber optic video interface to connect to each of the redundant DKT Switches, such that all DKT Interfaces can communicate with both DKT Switch chassis. Each of the redundant DKT Switches will not require reconfiguration when a switch module is removed and replaced, which reduces software complexity. To further increase reliability, a dual fiber optic DKT video interface will be attached to each DKT, such that each DKT Interface and each DKT can be reached even if one of the dual DKT Switch chassis fails or is taken out of service for maintenance. With this arrangement, the DKT user will be able to select any DKT Interface configured to be accessible from the DKT being used.

The design will provide dual controllers, dual power supplies, and extra switching modules in the DKT Switch, along with the separate, required modular Control System and On-Screen Display (OSD) Client rack mount chassis for each DKT Switch. The system administrator will use the modular Control System and OSD Client for the required password and controlled configuration capabilities for the DKT Switches, using the software supplied in the module. The DKT Switch

used as an example requires this module to operate. The module provides system wide, nonintrusive monitoring and control of the DKT Switch.

The design will be configured to support the EWS or maintenance computer associated with the PPS or DCS. In this case, the EWS or computer use DKT Interfaces, with appropriate password and physical protections in the EWS, will ensure the CR watchstanding operators are aware of any use of the EWS. Only a very limited number of DKTs will be allowed to connect to the EWS.

The cyber security team will evaluate the use of switched connections for EWS or maintenance computers for potential cyber security concerns as well as the design team evaluation for software change control and configuration management (CM).

The configuration will disable the ability to issue commands for the safety-related and non-safety related systems for the DKTs at the SRO workstation. The SRO will still be able to navigate to various screens and functions, but the SRO will not be able to use soft controls to initiate safety-related or non-safety related control functions. Similarly, the configuration will disable process commands for the safety-related or non-safety related system for any DKTs intended solely for maintenance or engineering use. To prevent the SRO, maintenance, and engineering staff from issuing commands, the DKT Switch will be configured to allow only certain DKTs to connect to certain DKT Interfaces. Thus, the DKT Switch software will restrict the DKT capabilities based on the port to which the DKT is connected. For example, when an RO workstation DKT connects to a DKT Interface, the DKT Interface will support soft controls for the safety function as well as screen navigation. The DKT Switch configuration for the SRO station will not allow connection to DKT Interfaces that support soft controls but will still allow screen navigation. This existing software function is already resident in the DKT Switch and will be qualified for safety-related use. For a non-safety related DCSs standard architecture implementation, the DKT Switch will connect to a DKT Interface (consisting of a Thin Client that communicates to a virtual machine) configured such that the SRO DKT operates in display only mode, disallowing commands to the non-safety related system but still allowing screen navigation. DKTs in the RO CR work area will be configured to connect to a DKT Interface that supports soft controls and screen navigation.

Each DKT Switch will provide internal redundancy and 100,000-hour mean time between failure.

For each configuration, the DKT Switch raises the question of software common cause failure. From a software point of view, the issue is similar whether the design uses a dual DKT Switch or single DKT Switch since both are internally redundant. This question also exists for the software (including firmware and programmable logic) in the DKT Interfaces and DKTs. The issues with software common cause failures will be addressed for the DKT Switch, since supporting the RPS, N4S, and ECCS functions will require the DKT Switch, DKT Interface, and the DKT to be included in the D3 Analysis (Reference 7). The DKTs are based on commercial designs of proven pedigree and from vendors with acceptable, proven obsolescence strategies. The NRC has approved the Westinghouse Common Qualified (Common Q) platform that uses the same video generators in all four safety-related divisions, so there is precedent for this design.

Two internally-redundant DKT Switches will provide true redundant communication for all DKTs, as shown in Figure 3-24 above. This design requires redundancy in the communication paths between the DKT Interfaces, DKT Switches, and DKTs to ensure a signal path exists, even with one DKT Switch out of service.

The safety-related channels and divisions, along with the non-safety related DCS all will provide data to both DKT Switches through individual dual fiber optic connections, one to each DKT Switch. Each DKT Switch fans the connections out to each safety-related (qualified) DKT. With redundant DKT Switches, the design supplies dual fiber optic interfaces on each DKT Interface and dual fiber optic interfaces on each DKT. The dual fiber interface ensures that each DKT can route to any DKT Interface if either of the DKT Switches fails. In that manner, each DKT Switch will have access to all data and each DKT will have access to the data through either DKT Switch. With this arrangement, the highly reliable single DKT Switch now will become significantly more reliable.

Any DKT will be able to interface with any safety-related or non-safety related systems, including issuing commands to both the safety-related and the non-safety related systems. Interfaces to other systems, such as the LGS corporate network, would also be possible.

Each DKT Interface, DKT Switch, and DKT will be qualified and commercial grade dedicated as a safety-related device, such that issuing commands to safety-related equipment occurs from safety-related equipment and commands to non-safety related equipment occur from safety-related, qualified equipment, which meets the expectations of DI&C-ISG-04. Thus, any DKT in the CR can be used for any function.

The detailed design will determine the power source for the DKT Interfaces, DKT Switches, and DKTs. Uninterruptible power is supplied to all of the PPS, but vital power may only be required for part of the DKT system. A Failure Modes and Effects Analysis will verify that the chosen power solution is acceptable and will not result in the loss of display or have the potential to propagate failures from one division to the other.

Vital power will be provided from both divisions for the DKT Switches and DKTs.

3.3.5.3 Use of HSI for PAM

The PPS DKTs will provide the capability to group PAM data available in the PPS logically for display to the CR operator and to other locations where DKT access is provided. All PAM data will be isolated and provided to and sampled by the DAS. The DAS then will provide a diverse display of safety-related information on the DAS DKTs on a system implementing AQ, thus providing a diverse means of CR display of the PAM data available in the PPS, in addition to the diverse non-safety related means provided on the DCS using data communicated from PPS.

By providing PAM data on the PPS DKTs, there will no longer be a need for those existing, separate safety-related meters and recorders in the CR that supply data from the existing RPS, N4S, and ECCS, since the data will be displayed redundantly and diversely on PPS and DAS DKTs. Having safety-related displays on the PPS DKTs will support the existing meters and recorders to be either removed or abandoned in place.

3.3.6 Modernized Architecture for DAS (DI&C-ISG-06 D.2.2)

3.3.6.1 Modernized PPS: General DAS Requirements

Most of the existing safety systems use analog I&C architectures to execute various safety functions. The digital modernization effort performed a D3 analysis (Reference 7) to determine whether a non-safety related DAS must be provided for certain functions that will be migrated to the proposed digital platform. The DAS will serve to mitigate the consequences of a common cause failure of the new digital platform, which could prohibit the safety systems from carrying out their specified safety functions. The existing LGS RRCS provides a diverse means of shutting down the reactor. The RRCS is used to satisfy the NRC's ATWS rule in 10 CFR 50.62 (Reference 8). To this end, the RRCS serves as a DAS for the existing RPS.

The D3 Analysis shows how those selected portions of the N4S and ECCS included in the DAS, along with the existing ATWS mitigation features, provide sufficient defense-in-depth for the N4S, ECCS, and RPS functions, respectively. The D3 analysis provides the rationale for selecting those limited portions of the N4S and ECCS (in addition to the existing ATWS mitigation features) that are required in the non-safety related DAS.

The PPS vendor will supply and validate appropriate analog and discrete isolators for the DAS inputs to the ATWS mitigation functions and select N4S and ECCS functions. The PPS will also supply and validate the priority logic and output isolation required for the outputs common to PPS and the selected N4S and ECCS functions executed by the DAS. The isolators for the ATWS functions will not be used until LGS eliminates the RRCS and installs the ATWS function into the DAS. However, the selected N4S and ECCS functions and the ATWS functions in the DAS will be provided and tested as part of the vendor's PPS system tests, including PPS and DAS integration tests at the vendor facility. The DAS system, hardware, software, and HSI are included in the vendor's scope of supply. The DAS will include processing and communications capacity, inputs, and outputs required to support the future ATWS mitigation functions.

This LAR Framework Document appropriately discusses a separate, future project to replace RRCS in the context of the broader DAS described above. While the RRCS replacement is not part of this LAR, future plans for the DAS, which would include ATWS mitigation functions currently executed by the RRCS, must be addressed at some level in the LAR. The current level of discussion assists in establishing the required analog and discrete input and output isolation where the safety-related platform interfaces with the non-safety related DAS.

TBD/TBC 20: Completion of the D3 analysis required in the complete LAR to support the DAS.

3.3.6.2 Modernized PPS: DAS and ATWS Functions

A separate project will eliminate the safety-related RRCS. In this separate project, the ATWS functions will be incorporated into an appropriately classified non-safety related set of DAS functions, which supports the RPS functions in the PPS.

The DAS will be constructed in a high-quality DCS. The design of the DAS is intended to ensure that the DAS functions are performed when required and that no inadvertent actuation

occurs when the DAS functions are not required. The integrated DAS will provide the required backup functions for the PPS. The separate project will incorporate the ATWS required in 10 CFR 50.62 (Reference 8) using the quality requirements from NRC Generic Letter (GL 85-06, Reference 57) as discussed in Section 3.4.5. The DAS will provide those functions required by the D3 Analysis for the N4S and ECCS functions absorbed into the PPS and expansion capability to support the ATWS functionality.

The DAS will include those functions from the N4S and ECCS that are required based on the D3 Analysis (Reference 7).

As an AQ, non-safety related system, the DAS will be segmented into two DCS controllers, each with separate analog inputs. Each DCS controller will be provided with two channels of isolated, safety-related Reactor Dome Pressure and Reactor Vessel Water Level. Independent software functions will perform the channel-specific comparisons, with two functions (i.e., channels) in each segment controller (i.e., division). The DCS controllers will share the results of the channels and determine if the 4oo4 voting threshold is met. If the 4oo4 vote indicates that the ATWS actuation is required, the actuation sequence provided in the original system will be initiated, with one exception, described below.

The modernized ATWS will not include the feedwater pump runback actuation that exists in the RRCS. This actuation is not required by 10 CFR 50.62 (Reference 8). LGS operational experience with the ATWS indicates that an operator needs to consider plant state and perform this actuation manually and not as an automated ATWS action. Running the reactor feedwater pumps back requires the immediate start of HPCI or RCIC, thus challenging both the safety-related functions in the ECCS and the ability of the plant and operator to maintain decay heat removal and Reactor Vessel Water Level above the top of fuel.

The ATWS portion of the DAS will provide highly reliable, single-failure tolerant load drivers in each division for all outputs. None of the ATWS functions will falsely initiate or fail to initiate when required based on the failure of a single discrete output.

The DAS and PPS outputs for the selected diverse N4S and ECCS functions will use external devices (e.g., EIMs) to provide the priority logic function required in DI&C-ISG-04 (Reference 44) and to ensure that the safety-related PPS and the non-safety related DAS control the plant appropriately.

3.3.6.3 Modernized DAS PAM Requirements

The software and configuration required for this function will provide sampling, engineering units conversions, any alarm limits applied in the DAS, provision of trending capabilities in the DAS, and generation of DAS DKT data displays similar to those provided for the PPS DKTs.

Data will be provided through qualified isolators installed in the PPS. Additional PPS data beyond that supplied for the selected PPS elements implemented for the DAS function can be supplied for display with the addition of PPS isolators, wiring to the DAS inputs, and the same software and configuration items required for the required data for DAS functions.

3.4 NEW AND CHANGED SYSTEM FUNCTIONS (DI&C-ISG-06 D.2.3)

3.4.1 Modernized PPS System Design Functions (DI&C-ISG-06 D.2.3.1)

This section of the LAR Framework Document describes elements that are common to all functions within the PPS. Specific design functions for the RPS, N4S, ECCS, and DAS design functions are then explained individually.

3.4.1.1 Modernized PPS General Requirements

The existing RPS, N4S, and ECCS design functions are documented in Sections 3.2.1.1, 3.2.2.1, and 3.2.3.1. The existing RPS, N4S, and ECCS service and test functions are documented in Sections 3.2.1.2, 3.2.2.2, and 3.2.3.2. The referenced sections identify the safety functions, including the scram and actuation functions. The operational occurrences and postulated accidents will not be changed from those defined in the LGS UFSAR (Reference 41), since the PPS will perform the same safety functions as previously credited and evaluated in the LGS UFSAR (IEEE Std. 603 Clause 4.1). The safety functions, protective actions, and execute features documented in the UFSAR will not change (IEEE Std. 603 Clause 4.2).

All PPS bi-stable functions will have hysteresis on the return to normal, with each bi-stable's trip setpoint value and restore setpoint value individually saved as user modifiable constants. The software will reject any attempt to set the restore setpoint within the trip range.

All PPS outputs that initiate scrams, actuations, or isolations will be single-failure tolerant and diagnosable. Thus, no single failure of a discrete output to the shorted or open state will either prevent a required change of output state or falsely cause an unintended change of output state. Further, failures in the single-failure tolerant output circuits will be detectable by the PPS.

Bypass functions are described in Sections 3.1.2, 3.2, 3.3.1, 3.3.5, 3.7.1, 3.8.1, 3.8.2, and 3.8.5. Manual maintenance bypass functions (IEEE Std. 603 Clauses 6.7 and 7.5) will be extended beyond the existing capabilities, to include the ability to bypass a channel or sensed inputs to the channel. Operational bypass functions (IEEE Std. 603 Clauses 6.6 and 7.4) will not be changed from the existing, licensed design, although existing manual operating bypasses may be automated (IEEE Std. 603 Clause 4.3). The field sensors, field sensor location, field wiring, field actuators, and field power sources will not be changed, so the number and location of the monitored variables and actuated devices is unchanged from the approved licensing basis (IEEE Std. 603 Clauses 4.4 and 4.6).

Manual, RO-initiated maintenance bypasses will be provided for channels and for individual sensors on a channel. The PPS logic will be designed such that bypassing a channel or a sensor changes the voting and copes with the loss of the sensor (IEEE Std. 603 Clause 7.5). For some N4S isolations, where only a single sensor exists in each of two divisions, bypassing that sensor will not disable the function, since the inboard and outboard isolation logic will now consider both sensors.

The logic in the existing functions incorporated into the PPS already assures that protective actions go to completion, whether initiated automatically (IEEE Std. 603 Clause 7.1) or manually (IEEE Std. 603 Clause 7.2), and requires deliberate operator actions to terminate the safety

function. Seal-in is provided in the divisions to ensure that protective actions go to completion. As an example, the RPS function cannot be reset for 10 seconds after initiation, to ensure that control rods are inserted before the operator can reset the RPS (IEEE Std. 603 Clauses 5.2 and 7.3). These features will be retained in the modernized design.

The existing systems have been evaluated and provide the appropriate points in time and plant conditions to initiate, provide automatic controls of the protective action, and determine that the protective action is no longer needed, thus allowing the protective action to be terminated (IEEE Std. 603 Clause 4.10). Any existing equipment protective capabilities or equipment outside of the PPS that might prevent the PPS from performing the required safety functions will not be changed by this modernization (IEEE Std. 603 Clause 4.11).

The location of or format for CR switches and pushbuttons will change based on this modernization, as discussed in Sections 3.3.5, 3.4.5, and 3.7.1.4. Some manual controls are will be moved to soft controls on DKTs. Other manual controls will be duplicated as soft controls on DKTs. However, the manual actions and the operating procedures that define when manual actions are required will not be changed by this modernization. The existing manual actions and operating procedures will be updated to the extent necessary to reflect the operator manual controls and capabilities, but the expectations for when PPS manual control is required are not changed by this modification. Further, the CR environment will be not affected by this modernization, other than by the installation of additional DKTs and removal of unneeded equipment. This modification will provide additional data in the CR that is not available with the existing design. In replacing the existing analog trip units in the AER, the modernized PPS will provide all the PPS plant data on the DKTs, along with significant PPS status (IEEE Std. 603 Clause 4.5). The HFE performed to support this modernization will ensure that the DKTs are installed in appropriate locations in the CR and that displays are designed to ensure operator comprehension (IEEE Std. 603 Clause 5.8, 5.8.1, 5.8.2, 5.8.3, and 5.8.4).

3.4.1.2 Modernized PPS System Cyclic Implementation of Design Functions (DI&C-ISG-06 D.2.3.1)

The original RPS, N4S, and ECCS design used analog trip units and relay logic. The propagation delay through the analog trip units and relay logic was relatively fixed by the design of the analog trip units and the relays themselves. The propagation delay was relatively fixed for a given set of modules and relays, with variability primarily sourced from the time delay relays.

The modernized PPS will use a software-based system, where cyclic timing introduces the potential for variable time delays. However, the PPS architecture design and implementation will ensure that the worst-case propagation delay from channel input to division output will meet LGS UFSAR requirements, as specified in the PPS Functional Requirements document (Reference 9). Worst-case timing occurs when internal functions, including channel analog signal filtering, channel sampling, channel logic processing, channel communication, divisional communication processing, divisional logic processing, and divisional output processing, are not synchronized and events require two cycles of unsynchronized sampling, processing, and communication functions to propagate signals from the PPS inputs to outputs. In all cases, channels and divisions will not operate in synchronism, to avoid the need to send synchronizing

signals between electrical divisions and to avoid synchronization as a potential source of software common cause failure.

3.4.1.3 Modernized PPS System Voting (DI&C-ISG-06 D.2.3.1)

LAR Framework Document Section 2.1.1 defines the existing design functions for the RPS. This section describes the minimal changes in the modernized design.

The modernized RPS function will change from the existing system design of 1oo2 taken twice to 2oo4 voting. For all PPS outputs, the PPS implementation will provide failure tolerant discrete outputs, ensuring that output device failures do not result in false scrams or actuations and that output device failures do not preclude scrams or actuations when required. The field implementation of actuated devices will not be modified. Existing field transmitters made redundant by the PPS architecture will be eliminated from the PPS.

For the RPS, the modernized PPS will provide votes to scram from all four channels to both divisions through redundant fiber optic serial communication links, which will allow the RPS function to detect and respond correctly to situations where both channels in a single division vote to scram, where the existing system would only generate a half scram. The divisions will then independently determine if a scram is required based on voting using individual parameters. Faults and failures within a division will result in the platform hardware and platform software turning off the discrete outputs, setting the RPS into the fail-safe state. In either the existing or the modernized system, failure of one RPS division results in a half scram and failure of both RPS divisions results in a full scram, since the RPS outputs are fail-safe to the de-energized state to scram. While the failure mechanisms of the existing system and the modernized system are different, the failure modes are identical.

Similarly, for those portions of the N4S with four redundant sensors and for all the ECCS, the same voting will occur as for the RPS. The difference is that the N4S actuates isolations and the ECCS actuates emergency core cooling functions, rather than causing a plant scram.

For RPS, ECCS, and some of the isolation functions in the N4S, divisional voting will be predicated on having all four channels online and no channels in maintenance bypass. If four channels of information are valid (i.e., no channel is in maintenance bypass and no channel is failed), the PPS will vote 2oo4. Voting will gracefully degrade as defined in Section 3.3.1. Each RPS division will read the channel maintenance bypass selector switch and determine if the operator is requesting to apply maintenance bypass to a specific channel. Each division will make this determination independently and will then provide the status to the external channel check software running in the non-safety related DCS. If the divisions are making different decisions, the non-safety related DCS software performing the channel check function will alarm.

The modernized design will change the voting scheme significantly, such that each signal type is voted independently and only two or more votes to scram from a single signal type will generate a scram through an independent, divisional logical OR of all voter outputs. If multiple signals exceed the configured limits, then the individual voters will vote to scram. Any occurrence of

two or more votes to scram will generate a scram within both divisions, assuming at least one of the redundant, diagnosed communication links from channels to divisions are functional.

Some of the RPS voting will occur in the existing NUMAC nuclear instrumentation voters. This modernization will not change the NUMAC voters. This information on the existing NUMAC voters is provided for completeness. The existing NUMAC 2oo4 voters combine the bypass, inoperative, and 2oo4 voting for the APRMs and OPRMs. For both the existing and the modernized RPS, two contact closures are provided to each channel, defining the votes to scram from the nuclear instrumentation. The four pairs of IRMs (eight total IRMs) will continue to feed each channel individually, where any single channel evaluates both IRM inputs to determine if a vote to scram will be generated. A separate project plans to install Wide Range Neutron Monitoring to replace the existing Startup and Intermediate Range Neutron Monitoring equipment. That change has no effect on this LAR, except to change the nomenclature on the existing NUMAC voter inputs from Startup Range to Wide Range Neutron Monitoring.

Other than changing the voting scheme and deletion of noncoincident neutron monitoring trip (see Section 3.2.1), the RPS functions for trip, seal-in, and reset will not be affected. After the elimination of many surveillance tests, the remaining service and test functions will be initiated by soft controls on the DKTs.

Other than changing the voting scheme, the ECCS functions for emergency core cooling, seal-in, and reset will not be affected.

Other than changing the voting scheme, the N4S functions for isolation, seal-in, and reset will not be affected. After the elimination of many surveillance tests, the remaining service and test functions will be initiated by soft controls on the DKTs.

3.4.1.4 PPS Use of Internal Self-Tests and Self-Diagnostics

As explained in Sections 3.1.7, 8.1.1, and 8.1.2, malfunctions in the vendor platform will be detected by the self-tests and self-diagnostics evaluated in the vendor's licensing topical report (Reference 42) and in the NRC's SE Report (Reference 43). Malfunctions within the platform, ranging from analog and discrete inputs through the platform itself to the analog discrete outputs, will be detected and alarmed in the CR. The self-tests and self-diagnostics have been demonstrated by the vendor to cover the identified hazards within the vendor platform and provide a sound basis for the simplification of the required TS tests that demonstrate the correct operation of the bi-stables, relay logic, and load drivers. Limited coverage will be provided for analog inputs (e.g., over or under range, open thermocouple). Additional coverage of the validity of inputs and processed outputs is provided in DCS software that checks the values provided by the PPS to alarm in the CR if field sensors are not appropriately clustered and calculated states are not similar.

The PPS will provide discrete outputs to drive the SOE and first-out outputs. All alarm status, including the SOE and first-out, data will also be provided to the DCS over the PPS to DCS unidirectional, fiber optic serial data links. The DCS will apply time stamps to the data in the message using the high-quality time source within the DCS.

3.4.1.5 Modernized PPS Compliance

As explained in Section 8.3, the setpoint values for the RPS, N4S, ECCS, and DAS functions will change to reflect the new PPS hardware, since the uncertainties associated with those variables will need to reflect the PPS uncertainties, rather than those for the analog trip units. Thus, the trip setpoint will change, but the allowable value, analytical limit, and safety limit will remain unchanged (IEEE Std. 603 Clause 4.4). Setpoint values will be computed based on the same approved methodology as the existing system, and setpoint values will be fixed but adjustable constants (Section 8.3 and IEEE Std. 603 Clause 6.8.1). For both the existing and the modernized systems, there are no plant mode dependent setpoint values in the PPS (IEEE Std. 603 Clause 6.8.2).

The PPS will be designed to maintain the required performance and accuracy. Deterministic behavior is explained in Section 3.8.3 and will be validated as described in Sections 5.1.13 and 5.1.14.

The PPS will be designed for maintenance. The PPS will identify, to the chassis and module, the faulted or failed field-replaceable unit. The PPS will be designed to hot swap field-replaceable units for most faults and failures, allowing the PPS to continue operation while the module is replaced, as described in Section 3.3 (IEEE Std. 603 Clause 5.10).

The PPS and DAS will be designed to ensure that appropriate protective actions are performed. The overall design process for the PPS will ensure that system integrity (IEEE Std. 603 Clause 5.5) is maximized. The DAS will ensure that the extremely unlikely software common cause failure of the PPS will not preclude the operation of sufficient safety functions during a Design Basis Event (DBE).

As explained in Section 3.3.1, the analog inputs will be filtered based on the standard vendor capabilities. The signals will be validated during the voting process in the divisions and will be further validated by the external channel check function running in the non-safety related DCS, as described in Section 3.1.7.

All software in the PPS will be classified as safety-related software and required to be designed, implemented, verified, and validated in accordance with the accepted vendor's software lifecycle, as described in Section 5.1. The RPS, N4S, and ECCS functions in the PPS (including those functions that have been absorbed into the PPS, including the LDS and EDG initiation logic) are required to be independent but will use shared signals and votes to actuate or scram from the channels. These PPS functions will use common field sensing inputs in the PPS channels. The voting and safety function implementation of each of these functions will be required to be independent of the actions of any other function. These functions will be required to be implemented in separate applications within the PPS.

The expected ranges of transient and steady-state conditions for electric power will be enveloped by the testing performed for the PPS, DKT system, and any other equipment provided (Section 4.1 and IEEE Std. 603 Clause 4.7). The plant conditions provided in Section 4.1 are the licensed conditions that are expected in the AER and CR (IEEE Std. 603 Clause 4.8). The modernized PPS is intended to protect the plant through the range of transient and steady-state

conditions under which the original RPS, N4S, and ECCS were designed to operate. As shown in Sections 4.2 and 4.3 for the PPS platform and in Sections 4.4 and 4.5 for the additional equipment, the LGS evaluation of the PPS platform and additional equipment type tests will demonstrate that the PPS can operate in the AER and CR where the equipment is installed, as documented in Section 4.1.

The modernized design will substitute self-tests, self-diagnostics, analyses, and PPS platform design for several of the surveillance testing functions required with the existing systems, as described in Sections 3.1.7 and 8.1.1 (IEEE Std. 603 Clause 5.7). Where manual testing will still be required, features will be provided to minimize the potential for human performance error, as discussed in Sections 3.1.5, 3.3.1, 3.4.1, 3.4.4, and 3.8.5 (IEEE Std. 603 Clauses 6.5.1 and 6.5.2).

A reliability analysis is provided for the PPS hardware as discussed in Section 3.8.1.1, including a FMEDA (Reference 55), to demonstrate reliability as well as the ability of the PPS equipment to identify faults and failures within the equipment and to report those faults and failures, which might result in a loss of the ability to perform the safety functions assigned to the PPS, to LGS for resolution (IEEE Std. 603 Clause 4.9).

The PPS design will conform to the regulatory requirements and expectations for D3 (Section 3.1.6, Reference 7) and comply with the appropriate regulatory guidance (Section 3.1.1). As required for safety functions, the PPS hardware and software will be purchased and assessed to be of a quality level commensurate with the requirements of 10 CFR 50 Appendix B and NQA-1 (IEEE Std. 603 Clause 5.3 and IEEE Std. 7-4.3.2 Clauses 5, 5.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, and 5.3.6).

The installed location of the PPS, in the vital AER and CR, will provide administrative controls for access to the modernized equipment. Cyber security will be provided based on the controls and processes invoked during design, development, transport, storage, installation, commissioning, operation in LGS, and maintenance at LGS, as described in Section 9.1 for the PPS and Section 9.2 for the DAS (IEEE Std. 603 Clause 5.9).

All documents associated with the design, implementation, verification, validation, installation, commissioning, operation, and maintenance of the PPS will be identified to meet LGS requirements and retained (IEEE Std. 603 Clause 4.5).

3.4.1.6 PPS Secure Development and Operational Environment (SDOE) and Secure Operating Environment

As stated in Section 9, the PPS will be protected during LGS Operations and Maintenance by the Secure Operating Environment cyber security features incorporated through the SDOE. These features will be implemented by the vendor and LGS actions. LGS will review and accept the potentially enhanced vendor's SDOE program. The PPS will be installed in vital areas (i.e., CR and AER). The PPS logic solvers, DKT Interfaces, and DKT Switches will be installed in the AER in cabinets where opening access doors results in alarms in the CR and to plant security. The controlled access to the EWS DKT in the AER will provide additional physical protection against modifications. DKTs that will be installed in the CR for use by the RO and SRO do not require passwords. The DKT Switches will be configured such that DKTs installed outside the CR cannot attach to the DKT Interfaces provided for the RO and SRO. Strong passwords will be

used in the DKT Interfaces to protect all DKTs installed outside the CR. Other features will be incorporated to ensure that the equipment is not subject to malicious modification.

3.4.1.7 PPS Channel and Division Independence

Compliance with IEEE Std. 603 (Reference 4) Clause 5.6.1 will be ensured by design, since no communication links or other data paths exist between channels or between divisions. The potential to compromise independence through point-to-point communication links from channels to divisions is eliminated by requirement, since only votes to scram or actuate and status are provided across the links, thus providing compliance with IEEE Std. 603 Clause 5.6.1 and IEEE Std. 7-4.3.2-2003 (Reference 5) Clause 5.6. As documented in Section 4, the design complies with IEEE Std. 603 Clause 5.6.2 in that all equipment will be qualified to the expected environmental stressors, and the LGS limits include the worst-case effects of DBEs. Use of fiber optic connections for all serial communication links will further increase the isolation between channels and divisions. The design will comply with IEEE Std. 603 Clause 5.6.3 and IEEE Std. 7-4.3.2-2003 Clause 5.6, since the PPS design will not depend on and is not directly interfaced with non-safety related systems, thus eliminating the potential for non-safety related systems to adversely affect the ability of the PPS to perform its safety functions. The existing systems are designed, and the modernized PPS will be designed to cope with the effects of single random failures in non-safety related systems, as demonstrated in LGS UFSAR Chapter 15 (Reference 41). Further, the existing system installation and the modernized PPS installation provide sufficient separation and barriers, including PPS equipment qualification, to ensure that non-safety related equipment installed in the AER or in the CR cannot adversely affect the PPS.

3.4.1.8 PPS Compliance with DI&C-ISG-04: Interdivisional Communication

The PPS will comply with Staff Positions 1.1 (i.e., Interdivisional Communication, Item 1) and 1.3 in that safety channels will not communicate with other channels and will communicate only unidirectionally with all PPS divisions. During maintenance, PPS channels and divisions will communicate with the EWS. Divisions will receive a defined, fixed communication message from the channels.

The PPS complies with Staff Position 1.2 in that the safety channels will not receive or sample data from outside the inputs assigned to that channel.

The PPS complies with Staff Positions 1.4 and 1.9 in that, as evaluated in the vendor's licensing topical report (Reference 42) and in the NRC's SE Report (Reference 43), the design for communication will provide appropriate separation from logic processing, sufficient such that the logic processing in either the channel or division cannot be adversely affected by faults and failures in the communications process.

The PPS will demonstrate compliance with Staff Positions 1.5 and 1.20 through testing (following appropriate design analysis) to demonstrate worst-case timing, including communication processing and results of data errors. The demonstration is described in Sections 5.1.13, 5.1.14, and 5.2.13.

The PPS channels will be designed to broadcast only predefined, fixed data messages on unidirectional point-to-point links from each channel to each division. The messages will always

include channel status with the votes to scram or actuate or votes to not scram or actuate. A single bit error will not invalidate any state data transmitted. No return paths will be provided, so no data can be returned from the division that could cause the protocol to stall, either deadlock or livelock. Since the same messages will be transmitted every cycle, loading on the dedicated, point-to-point communication links is fixed and will be demonstrated during testing to not exceed link or receiver capacity. This will demonstrate compliance with Staff Positions 1.6, 1.7, 1.14, 1.15, and 1.19.

The PPS channels and divisions will be designed to broadcast only predefined, fixed data messages at a predefined rate (checked by the receiver) on unidirectional point-to-point links from each channel and division to the non-safety related DCS. No return paths will be provided, so no data can be returned from the DCS to either the channel or division that could cause the protocol to stall, either deadlock or livelock, in compliance with Staff Positions 1.8 and 1.16.

The PPS complies with Staff Positions 1.10 and 1.11 in that the EWS will not be connected to a channel or division unless the channel or division is bypassed under administrative control. The EWS will be designed to only connect to one channel or division at a time, in accordance with administrative procedures and SRO control of access to the EWS.

The PPS complies with Staff Positions 1.12, 1.13, and 1.18 through the consideration of each of the bulleted items as provided in the staff position and incorporation of the bulleted items in the design of the communication hardware and software. The messages will be kept as simple as possible, while providing adequate protection from hazards. The design considerations will include: point-to-point links, which preclude several of the errors; careful introduction of redundancy within each message; use of fiber optic splitters at the transmitter to ensure all divisions receive the same message; use of redundant links and comparisons to preclude several of the listed errors; detection of multiple sequential bits of message corruption; safety-related links installed within the boundaries of the AER (reducing the potential for malicious message insertion); use of error detecting code, but not of error correcting code (redundant communication paths are not expected to be subject to the same simultaneous bit errors); and additional protections provided by the vendor.

The PPS complies with Staff Position 1.17, since the fiber optic cable used will be subjected only the environmental stressors in the AER and CR and the fiber optic cable will be qualified for the environment as demonstrated in Section 4.2.2.

3.4.1.9 PPS Compliance with DI&C-ISG-04: Command Prioritization

The N4S and ECCS portions of the PPS will use priority logic in separate EIMs. Since the ATWS function does not use the same field equipment to scram the plant, the ATWS portion of the DAS will not require EIMs.

The EIM complies with Staff Position 2.1 (i.e., Command Prioritization, Item 1) since the EIM will be a safety-related device, built under the vendor's 10 CFR 50 Appendix B Nuclear Quality Assurance (QA) Program as a basic component and designed and validated to provide appropriate priority.

The EIM complies with Staff Position 2.2 as the EIM will be a separate device and not part of the PPS logic solver.

The EIM complies with Staff Positions 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, and 2.10 as demonstrated in the vendor's licensing topical report (Reference 42) and in the NRC's SE Report (Reference 43) that accepted the EIM as a Priority Logic Module.

3.4.1.10 PPS Compliance with DI&C-ISG-04: Multidivisional Display Stations

The PPS will not use multidivisional displays. DKT switching allows DKTs to be connected to either a safety-related or a non-safety related DKT Interface. A DKT can only be connected to a single DKT Interface at any time. As explained in Section 3.3.5, the design and LGS evaluation of the DKT Switches will ensure that the concerns in DI&C-ISG-04 for multidivisional displays are not introduced to LGS.

The DKT Interfaces will accept data from the channels and division in which the specific DKT Interface is installed. The DKT Interfaces assigned to ROs will be able to issue soft controls to the logic solvers as well as navigate between the screens provided by the DKT Interface in use. DKT Interfaces will only provide the controls and capabilities assigned by design to that DKT Interface. The DKT Interfaces assigned to SROs and others will not be able to issue soft controls but will be able to navigate between the screens provided by the DKT Interface in use. All DKTs outside the CR will use strong passwords, in addition to access controls, as barriers to unauthorized use.

The DKT Interfaces will be designed with the same protections provided for communication between channels and divisions as documented in Section 3.4.1.8.

The DKTs, as well as the data displays and soft controls provided on and by the DKTs, will be designed, developed, implemented, verified, validated, and integrated with the PPS in accordance with an HFE program, in accordance with the expectations of DI&C-ISG-04, Section 3.2.

3.4.1.11 PPS Compliance with DI&C-ISG-04: Operator Workstations and D3

The number and location of DKTs will be also influenced by the D3 analysis, including the backup manual controls and indications.

3.4.2 Modernized RPS System Design Functions (DI&C-ISG-06 D.2.3.1)

This section describes the modernized voting and operational bypass capabilities for each of the existing retained scram conditions listed in Table 3-3 above, as explained in Section 3.2.1.1. The modernized division will generate a scram only if the voting conditions are individually satisfied for each scram.

This section provides the scram and logic performed to generate each scram. The combination of the individual Trips 1 through 16 can be considered a large Boolean logic OR, such that any identified scram condition in the division initiates the scram and SDV isolation outputs.
A reactor scram, initiated either automatically or manually by the RO, will initiate a 10 second

timer, which locks out the manual reset until the timer expires, preventing the RO from resetting the scram until the control rods have had time to be fully inserted. After the timer expires, the RO can reset the RPS scram.

The list below provides details for each of the scrams listed in Table 3-3 above.

1. For Trip 1, the operator action of simultaneously pressing the two reactor scram pushbuttons in the CR will disconnect the logic solver outputs, power off the SSPVs, connect power to the backup solenoid valves, and initiate SDV isolation. This is the only trip that is independent of the logic solver and provided solely through external means, which may include relays. The state of both pushbuttons is monitored by the divisions, and each division will start the divisional 10 second reset inhibit timer when both pushbuttons are pressed simultaneously. No bypass for this trip will exist.

2. For Trip 2, the single Reactor Mode Switch will be monitored by all four channels. When the RO moves the Reactor Mode Switch from Run to any Shutdown, Refuel, or Startup mode of operation, the channels monitoring the Run status will provide Reactor Mode Switch votes to scram to the division. Each division will implement a 2oo4 vote on the Reactor Mode Switch votes. If two or more Reactor Mode Switch votes are provided, each RPS division will cause a plant scram and start the reset inhibit timer in each division. No bypass for this trip will exist.

3. For Trip 3, each channel will sample two TSV valve limit switches. If either or both limit switches in each channel indicate that the TSV is open, the channel will supply one TSV vote to not scram to the divisions. If both limit switches indicate that each TSV is not fully open, the channel will supply one TSV vote to scram to the divisions. Each division will perform a 2oo4 vote on the TSV votes from the channels. If two or more TSV votes to scram are received, each RPS division will initiate a plant scram and start the 10 second reset inhibit timer. The divisional 2oo4 vote on the data supplied by the channels will implement a Boolean logic 3oo4 vote. One operational bypass will exist, which will bypass this trip if the reactor power is less than a setpoint. Each channel will place an operational bypass on the channel's vote to trip, which causes the channel's vote to be forced into the not scram state, based on the plant conditions provided in Table 3-3.

4. For Trip 4, each channel will sample the state of one of the four TCVs for Fast Closure. Each division will perform a 2oo4 vote on the single vote to trip or not trip provided by each of the channels. If two or more channels vote for a TCV scram, each RPS division will initiate a plant scram and start the divisional 10-second reset inhibit timer. One operational bypass will exist, which will bypass this trip if the power (as measured by the turbine first stage pressure) is less than a setpoint. Each channel will place an operational bypass on the channel's vote to trip, which will cause the channel's vote to be forced into the not scram state, based on the plant conditions provided in Table 3-3.

5. For Trip 5, each channel will sample both a discrete float switch and a level transmitter from the SDV. The level transmitter will be converted to a trip/no trip signal through a bi-stable with hysteresis. If both the float switch and the level transmitter bi-stable indicate that sufficient volume remains, the channel will provide an SDV vote to not

scram to both divisions. If either the float switch or the level transmitter bi-stable, or both, indicate that a barely sufficient volume remains, the channel will provide an SDV vote to scram to both divisions. If two or more channels vote for an SDV scram, each RPS division will initiate a plant scram and start the divisional 10-second reset inhibit timer. Operational bypasses will exist for the Reactor Mode Switch in Shutdown or Refuel and for use of the SDV High-Level bypass key that will allow the post-scram draining of the SDV. Each channel will place an operational bypass on the channel's vote to trip, which can cause the vote to be locked into the not trip state, based on the plant conditions provided in Table 3-3.

6. For Trip 6, the channels will provide the monitored status of the inboard and outboard MSIV to the divisions. The divisions will determine if either the inboard or output MSIV for each main steam line is not full open. If both the inboard and outboard MSIV on a specific main steam line are full open, the division will generate a MSIV vote to not scram for that specific MSIV. The division will perform this determination for each main steam line. If three or four of the main steam lines show not full open on an all MSIV votes, each RPS division will cause a plant scram and start the reset inhibit timer in each division. An operational bypass will exist if the Reactor Mode Switch is not in the Run position. Each division will place an operational bypass on the MSIV scram, which will cause the scram to be forced into the not scram state, based on the plant conditions provided in Table 3-3.

7. For Trip 7, each channel will be provided with an independent Drywell Pressure. The pressure reading will be converted to a trip/no trip signal through a bi-stable with hysteresis. If the division receives two or more votes for a Drywell Pressure scram from the divisions, each RPS division will initiate a plant scram and start the divisional 10-second reset inhibit timer. No bypass for this trip will exist.

8. For Trip 8, each channel will be provided with an independent Reactor Vessel Pressure. The pressure reading will be converted to a trip/no trip signal through a bi-stable with hysteresis. If the division receives two or more votes for Reactor Vessel Pressure scram from the divisions, each RPS division will initiate a plant scram and start the divisional 10-second reset inhibit timer. No bypass for this trip will exist.

9. For Trip 9, each channel will be provided with an independent Reactor Vessel Water Level signal. The level reading will be converted to a trip/no trip signal through a bi-stable with hysteresis. If the division receives two or more votes for Reactor Vessel Water Level scram from the divisions, each RPS division will initiate a plant scram and start the divisional 10-second reset inhibit timer. No bypass for this trip will exist.

10. For Trips 10 through 14, the NUMAC Voters will provide semi-redundant discrete votes to trip to each channel, as explained in Section 3.2.1.1 in the text beneath Table 3-3 above. Two of the eight SRMs will be assigned to each channel, using the existing assignments. As in the existing system, one or two NUMAC Voter inputs in each channel will generate the votes to scram to both divisions. If neither NUMAC Voter provides a vote to scram, the channel will provide a vote to not scram to the divisions. If two or more channels vote for a NUMAC Voter scram, each RPS division will initiate a

plant scram and start the divisional 10-second reset inhibit timer. All bypass logic for the nuclear instrumentation is processed in the existing, unmodified NUMAC Voter. There will be no bypass conditions applied by the RPS function.

11. For Trip 15, each channel will monitor two IRMs, with individual high-level trips provided by each IRM. Each IRM high-level trip will be bypassed if the Reactor Mode Switch is in Run. If either or both IRMs indicate a high level, the channel will provide a vote to scram to the division; otherwise the IRM will provide a vote not to scram. Each division will perform a 2oo4 vote on the votes to scram from each channel. If two or more channels vote for a scram, each RPS division will initiate a plant scram and start the divisional 10-second reset inhibit timer.

12. For Trip 16, each channel will monitor two IRMs, with individual inoperative trips provided by each IRM. Each IRM INOP trip will be individually bypassed if the Reactor Mode Switch is in Run. If either or both IRMs indicate a high level, the channel will provide a vote to scram to the division; else the IRM will provide a vote not to scram. Each division will perform a 2oo4 vote on the votes to scram from each channel. If two or more channels vote for a scram, each RPS division will initiate a plant scram and start the divisional 10-second reset inhibit timer.

13. As is explained in Section 3.2.1.1 in the text beneath Table 3-3 above, the currently abandoned-in-place Trip 17 will not be implemented in the modernized RPS function.

3.4.3 Modernized N4S System Design Functions (DI&C-ISG-06 D.2.3.1)

The existing design is the basis for the modernized design. In the existing design, some of the existing N4S isolations use a single channel to initiate the inboard isolation and use a second single channel to initiate the outboard isolation. For these, the modernized design will use the data from both channels to vote 1oo2 in the segmented N4S divisions, which will independently isolate the inboard and outboard based on a requirement for either to isolate. Since isolation valves are viewed as the least reliable portion of the system, initiating two valves will at least double the potential for an isolation to be implemented in the field.

Four existing NUMAC chassis currently provide a temperature monitoring function for leak detection. The four existing chassis are installed in the AER and provide only an alarm when a temperature excursion indicative of a steam leak is detected. The four obsolete chassis will be absorbed into the N4S, with all analog input monitoring, evaluation, isolation, and alarming provided by the N4S. The modernized N4S will provide the isolation logic based on data the N4S will directly read from the analog and discrete input data, performing exactly the same functions that the NUMAC chassis performs in the existing system. This will provide a new ability to monitor the temperature indications and individual temperature alarms in the CR as well as providing all temperature data and status to the plant data historian.

Voting in the N4S is not as simple as in the RPS or ECCS function. The N4S has varying numbers of sensors with different voting requirements. For some N4S functions, the existing voting varies from 2oo4 taken twice down to 1oo1 taken once.

For the N4S HVAC isolations, the isolation function is provided in the field, with only the isolation status provided to indicating lamps in the CR. The modernized system will replace the CR indicating lamps with indications on the DKT. Similarly, most of the actuation and manually performed bypasses below will be performed using soft controls on the DKT, unless required to be retained as manual pushbuttons in the CR. The discussion below assumes two pushbuttons will be provided in the CR, which can be replaced with a single soft control with appropriate selection and execution requirements, as discussed in Section 3.3.5.

The existing N4S functions are split into four electrical divisions. The modernized system will retain the isolations provided in the original system for the electrically isolated channels. Divisional isolation will be performed at the functional, rather than the electrical level. Other than this change in the divisional isolation, the sensors, channels, and electrical divisions will be unchanged.

With the replacement of the existing Steam Leak Detection (SLD), the PPS will perform exactly the same algorithms that the divisional NUMAC systems performed. The PPS will provide logical outputs within the PPS that will be used by the N4S algorithms as the contact closures were used in the existing N4S. The SLD algorithms will run in the channels and provide their voting results to the divisions. The divisions will use the SLD algorithm votes to isolate or not isolate in the isolation logic. Since all four divisions will be reporting information, the divisions will use the votes from all four divisional SLD algorithms.

This section describes the existing N4S isolations and groups, based on the existing isolations, groups, and voting in Table 3-5 above. The isolations and groups will be maintained and extended for modernized voting. Voting for each isolation group is explained below. Note that the initial default condition for all decisions to isolate below will be to not actuate (i.e., FALSE). Only if a condition that occurs that requires actuation will the decision to isolate be changed to an isolation (i.e., TRUE).

Group IA isolation will be caused by any of several different isolation sources. Group IA continues to be de-energize-to-actuate and is thus fail-safe. The voting considers:

a. The four channel-specific Reactor Vessel Water levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below Level 1, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate. This vote will apply to all four Main Steam Lines and their Main Steam Line Drains. There will be no bypass for this function.
b. The four channel-specific Main Steam Line pressures will be sampled and processed through a bi-stable in each channel. If the Main Steam Line pressure is at or below the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate. This vote will apply to all four Main Steam Lines and their Main Steam Line Drains. This vote to isolate will be bypassed if the Reactor Mode Switch is not in the Run position.
c. As explained in Section 3.2.2.1, the existing system isolates each Main Steam Line individually. For the individual isolation of each Main Steam Line, each channel will

perform a bi-stable evaluation of the channelized differential pressure (i.e., flow) measurement from each Main Steam Line, which the channels will provide to the divisions. Each division will be provided the channel isolation votes and will perform a 4oo4 vote on each Main Steam Line's four bi-stable votes to isolate, to determine whether to isolate or not isolate that Main Steam Line. This vote will be applied individually to the isolation outputs for Main Steam Line A, Main Steam Line B, Main Steam Line C, and Main Steam Line D and their Main Steam Line Drains.

d. The four channel-specific Condenser vacuum pressures will be sampled and processed through a bi-stable in each channel. If the pressure is at or above the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate. This vote will apply to all four Main Steam Lines and their Main Steam Line Drains. This vote to isolate will be bypassed if the Reactor Mode Switch is not in the Run position. This isolation will be bypassed if the CR operator has manually bypassed this isolation using DKT soft controls.
e. As is described above in this section, the channels will execute the SLD algorithms and provide votes to isolate or not isolate based on the setpoint temperature values provided for each evaluated room or area. For the MSIV Room Temperatures, all channels will provide votes to each division. Each division will perform a 4oo4 vote to determine whether to isolate or not isolate the Main Steam Lines. This vote will apply to all four Main Steam Lines and their Main Steam Line Drains. There will be no bypass for this function.
f. As is described above in this section, the channels will execute the SLD algorithms and provide votes to isolate or not isolate based on the setpoint temperature values provided for each evaluated room or area. For the Turbine Enclosure and Main Steam Tunnel, all channels will provide votes to each division. Each division will perform a 4oo4 vote to determine whether to isolate or not isolate the Main Steam Lines. This vote will apply to all four Main Steam Lines and their Main Steam Line Drains. There will be no bypass for this function.
g. An operator pressing the two manual MSIV Isolation pushbuttons in the CR, or activating the isolation through a soft control, will generate a trip through the logic in both divisions. This vote will apply to all four Main Steam Lines.

A successful vote to isolate in Item c will only isolate a single Main Steam Line and its Main Steam Line Drain. Any successful vote to isolate in Items a, b, and d through g will isolate all four Main Steam Lines and Main Steam Line Drains. Division 1 will control the inboard MSIVs and Division 2 will control the outboard MSIVs. Closing either the inboard or outboard valve will isolate the Main Steam Line. Each division will provide an output to control each divisional solenoid valve.

Group IB isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below Level 2, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 2oo4 vote to determine whether to isolate or not isolate.

b. An operator pressing both of the manual Main Steam and Reactor Sample Lines Isolation pushbuttons in the CR, or activating the isolations through a soft control, will cause the isolation through the logic in both divisions.

Both conditions above will be processed as a logical OR. If either condition is TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates the Main Steam and Reactor Sample Lines. The operator will not be able to bypass this isolation.

Group IIA isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below Level 3, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
b. The four channel-specific Reactor Vessel Pressures will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Pressure is at or above the setpoint value, the channel votes to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
c. An operator pressing both of the manual RHR Shutdown Cooling Isolation pushbuttons in the CR, or activating the isolations through a soft control, will cause the isolation through the logic in both divisions.

The three conditions above will be processed as a logical OR. If any condition is TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates the RHR Shutdown Cooling. The operator will not be able to bypass this isolation.

Group IIB isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below Level 3, the channel votes to isolate. Each division is provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
b. The four channel-specific Drywell pressures will be sampled and processed through a bi-stable in each channel. If the pressure is at or above the setpoint value, the channel votes to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
c. An operator pressing both of the manual RHR Heat Exchanger Sample and Drain to Radwaste Isolation pushbuttons in the CR, or activating the isolations through a soft control, will cause the isolation through the logic in both divisions.

The three conditions above will be processed as a logical OR. If any condition is TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates the RHR Shutdown Cooling. The operator will not be able to remove the RHR Drain to Radwaste

isolation by a bypass. The operator will be able to remove the RHR Heat Exchanger isolation by a bypass.

Group III isolation is caused by any of several different isolation sources.

a. The single channel processing the RWCU Differential Flow High will compare the flow rate to a setpoint using a bi-stable function. If the flow is high, the channel will provide a vote to isolate to both divisions. Each channel will initiate a 45-second time delay once the setpoint value is exceeded. If the condition still exists at the end of the time delay, the channel will vote to isolate.
b. The RWCU Area High Temperature will be read by a single channel, processed through a bi-stable, and provided to both divisions as a vote to isolate.
c. The RWCU Area Delta Temperature will be read by a single channel, processed through a bi-stable, and provided to both divisions as a vote to isolate.
d. Two channels will sample SLCS actuation signals. The channels will sample the contact status and provide a vote to isolate to both divisions. A 1oo2 vote on the contacts indicates that SLCS has been initiated by RRCS.
e. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below Level 2, the channel votes to isolate. Each division will be provided the channel isolation votes and will perform a 2oo4 vote to determine whether to isolate or not isolate.
f. If the CR operator presses both Main Steam and Reactor Sample Line Isolation pushbuttons, this will be considered a vote to isolate.

All six conditions above will be processed as a logical OR. If any of the conditions are TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates the RWCU. The operator will not be able to bypass this isolation.

Group IVA will be performed completely in two channels within Division 2. The isolation is caused by any of several different isolation sources.

a. The two channel-specific Reactor Steam flow measurements for HPCI will be sampled and processed through a bi-stable in each channel. If an individual channel's flow is at or above the setpoint value, that channel will initiate a 3-second time delay. If the condition still exists at the end of the time delay, the channel will vote to isolate.
b. The two channel-specific HPCI Steam Supply pressures will be sampled and processed through a bi-stable in each channel. If the pressure is at or below the setpoint value, the channel will vote to isolate.
c. The two channel-specific HPCI Turbine Exhaust Diaphragm pressures will be sampled and processed through a bi-stable in each channel. If the pressure is at or above the setpoint value, the channel will vote to isolate.
d. Each applicable channel in the SLCS subfunction in N4S will measure the HPCI Room temperature and will provide a vote to isolate if the temperature is at or above the setpoint value.
e. Each applicable channel in the SLCS subfunction in N4S will measure the HPCI Pump Room Delta Temperature and will provide a vote to isolate if the temperature difference is at or above the setpoint value.

f. The two HPCI Isolation pushbuttons in the CR will be sampled. If both pushbuttons are pressed, this will be considered a vote to isolate.

All six conditions above will be processed as a logical OR of the six individual 1oo2 votes in each of Division 2A and Division 2B. If any of the conditions are TRUE, Division 1A and Division 1B will each drive their discrete output to the solenoid valve to cause an isolation of either the inboard or outboard HPCI Isolation solenoid valve. The operator will not be able to bypass this isolation.

Group IVB isolation is caused by two different isolation sources. The voting considers:

a. The four channel-specific Drywell pressures will be sampled and processed through a bi-stable in each channel. If the pressure is at or above the setpoint value, the channel will vote to isolate. The divisions will be provided the channel isolation votes and will perform a 2oo4 vote to determine whether to isolate or not isolate.
a. The two channel-specific HPCI Steam Supply pressures will be sampled and processed through a bi-stable in each channel. If the pressure is at or below the setpoint value, the channel votes to isolate. The divisions will be provided the channel isolation votes and will perform a 1oo2 vote to determine whether to isolate or not isolate.

The two conditions above will be processed as a logical AND. If both conditions are TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates the HPCI Vacuum Breaker. The operator will not be able to bypass this isolation.

Group VA is performed completely in two channels within Division 1. The isolation is caused by any of several different isolation sources.

a. The two channel-specific measurements of Reactor Steam flow to RCIC will be sampled and processed through a bi-stable in each channel. If the flow is at or above the setpoint value, that channel will initiate a 3-second time delay. If the condition still exists at the end of the time delay, the channel will vote to isolate. Division 1A and Division 1B will individually perform a 1oo2 vote to determine if the isolation is required.
b. The two channel-specific RCIC Steam Supply pressures will be sampled and processed through a bi-stable in each channel. If the pressure is at or below the setpoint value, the channel will vote to isolate. Division 1A and Division 1B will individually perform a 1oo2 vote to determine if the isolation is required.
c. The two channel-specific RCIC Turbine Exhaust Diaphragm pressures will be sampled and processed through a bi-stable in each channel. If the pressure is at or above the setpoint value, the channel will vote to isolate. Division 1A and Division 1B will individually perform a 1oo2 vote to determine if the isolation is required.
d. Each applicable channel in the SLCS subfunction in N4S will measure the RCIC Room Temperature and provide a vote to isolate if the temperature is at or above the setpoint value.
e. Each applicable channel in the SLCS subfunction in N4S will measure the RCIC Pump Room Delta Temperature and provide a vote to isolate if the temperature is at or above the setpoint value.

f. The two RCIC Isolation pushbuttons in the CR will be sampled. If both pushbuttons are pressed AND the RCIC initiation signal is not reset, this will be considered a vote to isolate.

All six conditions above will be processed as a logical OR in Division 1A and in Division 1B. If any of the conditions are TRUE, Division 1A and Division 1B will each drive their discrete output to the solenoid valve to isolate HPCI. The operator will not be able to bypass this isolation.

Group VB isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Drywell pressures will be sampled and processed through a bi-stable in each channel. If the pressure is at or above the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 2oo4 vote to determine whether to isolate or not isolate.
b. The two channel-specific RCIC Steam Supply pressures will be sampled and processed through a bi-stable in each channel. If the pressure is at or below the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.

The two conditions above will be processed as a logical AND. If both conditions are TRUE, each division provides an output to control the division's inboard or output solenoid valve that isolates the RCIC Vacuum Breaker. The operator will not be able to bypass this isolation.

Group VIA isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below Level 2, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
b. The four channel-specific Drywell pressures will be sampled and processed through a bi-stable in each channel. If the Drywell Pressure is at or above the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
c. The radiation monitoring system will provide a single contact closure that represents high radiation in the North Stack Effluent. An indicated high radiation contact state will be considered a vote to isolate.
d. The radiation monitoring system will provide two contact closures that represent high radiation in the Reactor Enclosure Ventilation Duct. If both contacts are in the state indicating high radiation, this will be considered a vote to isolate.
e. The radiation monitoring system provides two contact closures that represent high radiation in the Refueling Area Ventilation Exhaust Duct. If both contacts are in the state indicating high radiation, this is considered a vote to isolate.

f. The single channel processing the Outside Atmosphere to Refueling Area Differential Pressure will compare the differential pressure to a setpoint using a bi-stable function. If the differential pressure is at or above the setpoint value, the channel will provide a vote to isolate to both divisions.
g. The single channel processing the Outside Atmosphere to Reactor Enclosure Differential Pressure will compare the differential pressure to a setpoint using a bi-stable function. If the differential pressure is at or above the setpoint value, the channel will provide a vote to isolate to both divisions.
h. A single contact will indicate that the Refuel Floor to SGTS connecting valves failed open. An indicated open contact state will be considered a vote to isolate. The operator will be able to bypass this vote to isolate.
i. A single contact will indicate that the Reactor Enclosures to SGTS connecting valves failed open. An indicated open contact state will be considered a vote to isolate.
j. An operator pressing any of the three manual Primary Containment Purge Supply and Exhaust Isolation pushbuttons in the CR, or activating the isolation through a soft control, will generate a vote to isolate.

All ten conditions above will be processed as a logical OR. If any of the conditions are TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates the Primary Containment Purge Supply and Exhaust. All but one condition causing this isolation will be designed to support bypass, the exception being that initiation caused by the North Stack Effluent high radiation will not be designed to allow bypass.

Group VIB isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below Level 2, the channel will vote to isolate. Each division is provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
b. The four channel-specific Drywell pressures will be sampled and processed through a bi-stable in each channel. If the Drywell Pressure is at or above the setpoint value, the channel will vote to isolate. Each division is provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
c. The radiation monitoring system will provide two contact closures that represent high radiation in the Reactor Enclosure Ventilation Duct. If both contacts are in the state indicating high radiation, this will be considered a vote to isolate.
d. The radiation monitoring system will provide two contact closures that represent high radiation in the Refueling Area Ventilation Exhaust Duct. If both contacts are in the state indicating high radiation, this is will be considered a vote to isolate.
e. The single channel processing the Outside Atmosphere to Refueling Area Differential Pressure will compare the differential pressure to a setpoint using a bi-stable function. If the differential pressure is at or above the setpoint value, the channel will provide a vote to isolate to both divisions.
f. The single channel processing the Outside Atmosphere to Reactor Enclosure Differential Pressure will compare the differential pressure to a setpoint using a bi-stable function. If

the differential pressure is at or above the setpoint value, the channel will provide a vote to isolate to both divisions.

g. A single contact will indicate that the Refuel Floor to SGTS connecting valves failed open. An indicated open contact state will be considered a vote to isolate.
h. A single contact will indicate that the Reactor Enclosures to SGTS connecting valves failed open. An indicated open contact state will be considered a vote to isolate.
i. An operator pressing any of the three manual Primary Containment REECE Isolation and N2 Block Valves Isolation pushbuttons in the CR, or activating the isolations through a soft control, will generate a vote to isolate.

All nine conditions above will be processed as a logical OR. If any of the conditions are TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates. The operator will not be able to bypass this isolation.

Group VIC isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below Level 2, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
b. The four channel-specific Drywell Pressures will be sampled and processed through a bi-stable in each channel. If the Drywell Pressure is at or above the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
c. The radiation monitoring system will provide two contact closures that represent high radiation in the Reactor Enclosure Ventilation Duct. If both contacts are in the state indicating high radiation, this will be considered a vote to isolate.
d. The radiation monitoring system will provide two contact closures that represent high radiation in the Refueling Area Ventilation Exhaust Duct. If both contacts are in the state indicating high radiation, this will be considered a vote to isolate.
e. An operator pressing two of the manual Primary Containment H_2 and O_2 Sampling and Recombiner Lines Isolation pushbuttons in the CR, or activating the isolations through a soft control, will be considered a vote to isolate.

All five conditions above will be processed as a logical OR. If any of the conditions are TRUE, then each division will provide an output to control each inboard and output solenoid valve that isolates. The operator will not be able to use a bypass to restore the Drywell Radiation Sample Supply and Return Lines if conditions a or b are present. The operator will be able to bypass all other isolations.

Group VIIA isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels channel isolation votes sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is

at or below Level 1, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 2oo4 vote to determine whether to isolate or not isolate.

b. The four channel-specific Drywell Pressures will be sampled and processed through a bi-stable in each channel. If the Drywell Pressure is at or above the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
c. The radiation monitoring system will provide two contact closures that represent high radiation in the Reactor Enclosure Ventilation Duct. If both contacts are in the state indicating high radiation, this will be considered a vote to isolate.
d. An operator pressing two of the manual PCIG Isolation pushbuttons in the CR, or activating the isolations through a soft control, will generate a vote to isolate.

All four conditions above will be processed as a logical OR. If any of the conditions are TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates. The operator will not be able to use a bypass to restore the Primary Containment Vacuum Relief Valve Supply Line isolation for conditions a or b. The operator will be able to bypass all other isolations.

Group VIIB isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below Level 2, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
b. The four channel-specific Drywell Pressures will be sampled and processed through a bi-stable in each channel. If the Drywell Pressure is at or above the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
c. The radiation monitoring system will provide two contact closures that represent high radiation in the Reactor Enclosure Ventilation Duct. If both contacts are in the state indicating high radiation, this will be considered a vote to isolate.
d. An operator pressing two of the manual PCIG Isolation pushbuttons in the CR, or activating the isolations through a soft control, will generate a vote to isolate.

All four conditions above will be processed as a logical OR. If any of the conditions are TRUE, then each division will provide an output to control each inboard and output solenoid valve that isolates. The operator will be able to bypass only the Reactor Enclosure Ventilation Duct radiation monitoring system.

Group VIIC has a simple voting scheme. The four channel-specific differential pressure between the PCIG and Drywell will be sampled and processed through a bi-stable in each channel. If the differential pressure is at or above the setpoint value, the channel votes to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate. Closing either the inboard or outboard valve will

isolate the PCIG to ADS. Each division will provide an output to control each divisional solenoid valve. The operator will not be able to initiate or bypass this isolation.

Group VIIIA isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below Level 1, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
b. The four channel-specific Drywell Pressures will be sampled and processed through a bi-stable in each channel. If the Drywell Pressure is at or above the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
c. An operator pressing two of the manual Drywell Chilled Water and RECW Isolation pushbuttons in the CR, or activating the isolations through a soft control, will generate a vote to isolate.

All three conditions above will be processed as a logical OR. If any of the conditions are TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates. The operator will not be able to bypass this isolation.

Group VIIIB, Drywell Sump, Suppression Pool Cleanup, and Traversing In-Core Probes **(TIP)** isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below Level 2, the channel will vote to isolate. Each division will be provided the channel isolation votes and perform a 4oo4 vote to determine whether to isolate or not isolate.
b. The four channel-specific Drywell Pressures will be sampled and processed through a bi-stable in each channel. If the Drywell Pressure is at or above the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and perform a 4oo4 vote to determine whether to isolate or not isolate.
c. An operator pressing two of the manual Drywell Sump, Suppression Pool Cleanup, and TIPs Isolation pushbuttons in the CR, or activating the isolations through a soft control, will generate a vote to isolate.

All three conditions above will be processed as a logical OR. If any of the conditions are TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates. The TIP will be withdrawn as part of this isolation. The operator will not be able to bypass this isolation.

Group VIIIB, ECCS Process Lines isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below

Level 1, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.

b. The four channel-specific Drywell Pressures will be sampled and processed through a bi-stable in each channel. If the Drywell Pressure is at or above the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and will perform a 4oo4 vote to determine whether to isolate or not isolate.
c. The four channel-specific Reactor pressures will be sampled and processed through a bi-stable in each channel. If the Reactor pressure is at or below the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and perform a 4oo4 vote to determine whether to isolate or not isolate.

If the (logical AND of Conditions b and c) OR (Condition a) is TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates. The operator will not be able to initiate or bypass this isolation.

Group VIIIB, Bypass Barrier Block and Vents isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below Level 1, the channel will vote to isolate. Each division will be provided the channel isolation votes and perform a 4oo4 vote to determine whether to isolate or not isolate.
b. The four channel-specific Drywell Pressures will be sampled and processed through a bi-stable in each channel. If the Drywell Pressure is at or above the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and perform a 4oo4 vote to determine whether to isolate or not isolate.
c. The radiation monitoring system will provide two contact closures that represent high radiation in the Reactor Enclosure Ventilation Duct. If both contacts are in the state indicating high radiation, this will be considered a vote to isolate.
d. The radiation monitoring system will provide two contact closures that represent high radiation in the Refueling Area Ventilation Exhaust Duct. If both contacts are in the state indicating high radiation, this will be considered a vote to isolate.
e. An operator pressing two of the manual Bypass Barrier Block and Vents Isolation pushbuttons in the CR, or activating the isolations through a soft control, will generate a vote to isolate.

All five conditions above will be processed as a logical OR. If any of the conditions are TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates. The operator will be able to bypass only the N_2 Supply Vent Valves. The operator will not be able to bypass the other isolations.

Group VIIIB, PCIG Block and Vents isolation is caused by any of several different isolation sources. The voting considers:

a. The four channel-specific Reactor Vessel Water Levels will be sampled and processed through a bi-stable in each channel. If the Reactor Vessel Water Level is at or below

Level 1, the channel will vote to isolate. Each division will be provided the channel isolation votes and perform a 4oo4 vote to determine whether to isolate or not isolate.

b. The four channel-specific Drywell Pressures will be sampled and processed through a bi-stable in each channel. If the Drywell Pressure is at or above the setpoint value, the channel will vote to isolate. Each division will be provided the channel isolation votes and perform a 4oo4 vote to determine whether to isolate or not isolate.
c. The radiation monitoring system will provide two contact closures that represent high radiation in the Refueling Area Ventilation Exhaust Duct. If both contacts are in the state indicating high radiation, this will be considered a vote to isolate.
d. An operator pressing two of the manual PCIG Block and Vents isolation pushbuttons in the CR, or activating the isolations through a soft control, will generate a vote to isolate.

All four conditions above will be processed as a logical OR. If any of the conditions are TRUE, each division will provide an output to control each inboard and output solenoid valve that isolates. The operator will be able to bypass this isolation.

Group VIIIB HVAC isolations (Refuel Floor Heating, Ventilation, and Air Conditioning [HVAC] and Reactor Enclosure HVAC) are installed in the field with the isolated equipment. There are no analog trip units or relay logic in the AER to implement the logic, so these functions are not affected by the modernization. In the existing system, isolated and not isolated status lamps are provided in the CR. For the modernized CR, the indicator lamps will be eliminated, the status will be sampled by the PPS, and the status will be provided on DKTs.

3.4.4 Modernized ECCS System Design Functions (DI&C-ISG-06 D.2.3.1)

The existing ECCS function mostly uses 1oo2 taken-twice voting, which has been updated to 2oo4 voting in the modernized ECCS function, like the RPS.

The modernized PPS will provide votes to actuate from all four channels to both divisions through redundant fiber optic serial communication links, which allows the ECCS to detect and respond correctly to situations where both channels in a single division vote to actuate, whereas the existing ECCS would only generate a half actuation. The divisions will then independently determine if one of the ECCS subfunctions is required, based on voting using individual parameters. The ECCS will actuate when the single-failure tolerant discrete outputs turn on. Faults and failures within a division will result in the platform hardware and platform software turning off the discrete outputs, setting the ECCS into the non-actuated state.

Other than changing the voting scheme, the ECCS logic for conditions for initiation, seal-in, sequencing, trip, isolation, and shutdown of safety functions will be unchanged. After the elimination of many surveillance tests, the remaining service and test functions will be initiated by soft controls on the DKTs.

Divisional voting will be predicated on having all four channels online and no channels in maintenance bypass. If four channels of information exist, the ECCS will vote using the normal scheme. Voting will gracefully degrade as defined in Section 3.3.1, with appropriate specifics for the subfunction. Each ECCS division will read the channel maintenance bypass selector switch and determine if the operator is requesting to apply a maintenance bypass to a specific

channel. Each division will independently make this determination and then will provide the status to the external channel check software running in the non-safety related DCS. If the divisions are making different decisions, the channel check software will alarm.

The ECCS includes the RHR system. The existing LPCI safety-related controls associated with RHR will be incorporated in the PPS. To reduce the potential for human performance error while performing the complex manipulations necessary to change the RHR system into any of the existing non-safety related configurations, the RHR subfunction will be extended to include automation of the interlocks and field actuated device manipulations necessary to set the RHR into any of the in-use RHR modes. The RO will initiate these non-safety related RHR subfunctions using safety-related software in the logic solvers, using the soft controls provided on the DKTs.

The list below describes the voting and logic for each of the conditions that will initiate emergency core cooling and each of the operating modes where ECCS equipment will be used. The safety-related ECCS modes are defined in Section 3.3.3.1 above and will not be changed by this modernization. The modernized division will separate these individual ECCS subsystems as logic solver subfunctions. There will be no bypass conditions for any of these ECCS subfunctions. Each ECCS subfunction will operate independently. Each ECCS subfunction will set the RHR pumps and valves to states appropriate to operate the subfunction. Each safety-related ECCS subfunction will override any non-safety related function.

1. **CS:** The requirement to activate CS in each of the two independent divisions will be satisfied if either division independently detects conditions requiring a CS. The existing logic has six analog trip units in each division, for a total of 12 analog trip units. To simplify the design, each channel will provide a bi-stable output for Low Reactor Vessel Water Level, Low Reactor Vessel Pressure, and High Drywell Pressure. Each division will evaluate each of the four channel's data individually, evaluating the Boolean expression below for each of the channels, where TRUE is defined as the condition existing and each channel is defined as (x):

   CS Vote (x) = {Low Reactor Vessel Water Level (x) OR [Low Reactor Vessel Pressure (x) AND High Drywell Pressure (x)]}

   Each division will then perform a 2oo4 vote on the CS Vote (x) results. The voted result determines whether a CS condition exists for each division. The expectation is that both divisions will operate on similar data, through identical logic, resulting in both divisions identifying a condition requiring CS. CS will be designed to be initiated manually by the RO.

   The existing logic provides two contact outputs in series in a taken-twice vote for the logic in each voter. The modernized logic solver will provide a single electronic output for each Division, with each output being single-failure tolerant.

   CS will terminate when the Reactor Vessel Water Level is restored and (1) the Drywell Pressure high is bypassed, (2) the non-bypassed Drywell Pressure has been restored, and (3) the operator has reset the high Drywell Pressure seal-in.

The RO will be able to manually stop each CS Pump. The RO will be able to manually start each CS Pump for testing. The RO will be able to manually open, close, or stop motion on each division's CS valve. Logic exists that will set all CS valves into the correct state for each of the active functions and for the Standby condition.

CS will provide four active functions in the modernized logic. The CS function will be one of the four. Safeguard Piping Fill, Feedwater Fill, and Flow Testing will be the other three active functions. If not active, the CS system will set itself into the Standby condition.

The **Safeguard Fill** function will provide fill water for RHR, RCIC, and HPCI piping when the normal Condensate Storage and Transfer System Keep Fill Subsystem is inoperable. This CS function will maintain the pump discharge lines in a filled condition, using water from the Suppression Pool. In the existing system, this function is initiated and configured manually. In the modernized PPS, the RO will initiate and terminate this automated function through the DKT using soft controls.

The **Feedwater Fill** function will provide fill water for feedwater system piping following a DBE. This CS function will maintain the feedwater lines in a filled condition, using water from the Suppression Pool. The water will seal the feedwater lines to prevent leakage from the feedwater lines to maintain containment integrity post-accident. In the existing system, this function is initiated and configured manually. In the modernized PPS, the RO will initiate and terminate this automated function through the DKT using soft controls.

The CS **Flow Testing** function will be designed to use the Suppression Pool as a water source, recirculating water back into the Suppression Pool. The Flow Testing function will also be designed to use the Condensate Storage Tank, sending water through the in-reactor CS Spargers. For the Suppression Pool, the CS Test Bypass Valves will be throttled by the modernized logic to control the flow returning to the Suppression Pool to a preset, modifiable demand value. For the in-reactor CS Spargers, no flow control will be provided. In the modernized PPS, the RO will initiate this automated mode in one division using soft controls. The RO will be able to stop this mode in either division using the DKT soft controls. Several different alignments are possible, and all will be automated.

The existing pump minimum flow protection, speed control, and other similar pump and pump system controls are not part of this modernization.

2. **HPCI:** For the single-train HPCI, the existing logic evaluated four separate reactor water levels and four separate high Drywell Pressures, provided to the two channels in the division that controls the HPCI. For the modernized PPS, the duplicate transmitters in the channel will be removed. For HPCI initiation, the division will perform a 2oo4 vote on Low Reactor Vessel Water Level (at or below Level 2) and a 2oo4 vote on High Drywell Pressure. If either vote is TRUE, the logic will initiate HPCI. The RO will be able to initiate HPCI manually. The HPCI logic will include any required support for

testing the system function in the plant. HPCI will terminate automatically when Reactor Vessel Water Level is at or above Level 8.

HPCI will use the Suppression Pool as a safety-related source. Normal alignment will continue to be the Condensate Storage Tank, with all Condensate Storage Tank valves open, and the pump discharging to the Suppression Pool.

If HPCI is not injecting or being tested, valves will be aligned such that main steam is available up to the HPCI Steam Admission Valve, to minimize condensation. Any condensate from the main steam lines will continue to be sent to the Main Condenser, with condensate from the Barometric Condenser Vacuum Tank aligned and pumped to the Radwaste System through the normally open HPCI Condensate Pump Discharge Valves, with the HPCI Pump Discharge Flow control in Auto. The HPCI System discharge piping will be aligned to the Keep Fill System.

If HPCI is in the Test mode, HPCI will recirculate either into the Condensate Storage Tank or Suppression Pool. The existing system requires the operator to manually align the valves. The modernized PPS will automate valve alignment to the operator's selected source. The manual mode will also be used to assist in maintaining Reactor Vessel Pressure.

The modernization will remove the HPCI FIC and will replace the FIC with automatic logic in the logic solver. The logic solver will initially place HPCI in Flow Control mode and set the flow target to a controlled setpoint value. The RO will be able to select between Flow, Reactor Vessel Pressure, or Reactor Vessel Level Controls, which will modulate the steam turbine speed setpoint to achieve the selected flow. Minimum and maximum allowable parameters will be defined for each of the user modifiable Flow, Pressure, and Level demand values. All parameters associated with the control modes will be modifiable constants. This software will be designed to eliminate the potential for cycling HPCI on and off, starting HPCI when water levels are low and stopping HPCI when water levels are high, thus minimizing unnecessary wear on HPCI equipment. Automation will also eliminate manual CR action during accidents and transients.

The existing pump minimum flow protection, overspeed protection, speed control, and other similar pump and pump system controls are not part of this modernization.

3. **RCIC:** RCIC will provide a safe shutdown when the reactor is isolated and Reactor Vessel Pressure is too great for the RHR Shutdown Cooling Mode. The existing RCIC operates automatically only when injecting, with flow set by a FIC. The modernized RCIC will provide additional automated modes for the control of flow into the reactor (default for initiation of injection) and operator selectable control of Reactor Vessel Pressure and Reactor Vessel Water Level.

   For the single-train RCIC, the existing logic evaluated four separate Reactor Vessel Water Levels, provided to the two channels in the division that control RCIC. For the modernized PPS, the duplicate transmitters in the channel will be removed. For RCIC initiation, the division will perform a 2oo4 vote on Low Reactor Vessel Water Level (at

or below Level 2). If water level is low, RCIC will be initiated. The RO can manually initiate RCIC.

There will be four active modes for RCIC. The RCIC will provide Coolant Injection, Reactor Vessel Water Level Control, Reactor Vessel Pressure Control, and Test capabilities.

For RCIC initiation, the division will perform a 2oo4 vote on Low Reactor Vessel Water Level (at or below Level 2). If the vote is TRUE, the division will initiate RCIC. RCIC will terminate automatically when Reactor Vessel Water Level is at or above Level 8. When RCIC initiates, the logic solver will provide a fixed flow rate using an adjustable demand value. The Suppression Pool will be the safety-related water source. The RCIC design will support the use of the Condensate Storage Tank as the normal water source. A logic interlock will prevent simultaneous suction from both the Suppression Pool and the Condensate Storage Tank.

RCIC will provide **Reactor Vessel Water Level Control** when the reactor is isolated from feedwater and the Reactor Vessel Pressure is too high to initiate RHR Shutdown Cooling. The RCIC will also provide Reactor Vessel Water Level Control in the hot standby mode. In this mode, the existing RCIC uses a defined flow rate, set on the FIC. In the modernized PPS, the FIC will be removed and replaced with automated software logic in the logic solver.

RCIC will provide **Reactor Vessel Pressure Control** while removing decay heat by using reactor steam to power the RCIC steam turbine.

The modernized control logic initially will place RCIC in Reactor Vessel Level Control mode and set the controller demand to a controlled setpoint value, set to 600 gpm in the existing system. The RO will also be able to select Flow or Reactor Vessel Water Level Controls, which will modulate the steam turbine speed setpoint to achieve the selected flow. Minimum and maximum allowable parameters will be defined for each of the user modifiable Flow, Pressure, and Level demand values. All parameters associated with control modes will be modifiable constants.

If RCIC is in the **Test** mode, RCIC will recirculate either into the Condensate Storage Tank or Suppression Pool, as selected by the RO. The existing system requires the operator to manually align the valves. The modernized PPS will automate valve alignment. As in the existing system, the manual mode may also be used to assist in maintaining Reactor Vessel Pressure.

If RCIC is not in use, then valves will be aligned such that main steam is available right up to the RCIC Steam Supply Valve, to minimize condensation. As in the existing system, any condensate from the main steam lines will be sent to the Main Condenser, with condensate from the Barometric Condenser Vacuum Tank aligned and pumped to the Radwaste System through the normally closed RCIC Barometric Condenser Drain Isolation Valves and the RCIC Pump Discharge Flow control in auto. The RCIC suction

will be alighted to the Condensate Storage Tank, with all valves open. The HPCI System discharge piping will be aligned to the Keep Fill System.

The existing pump minimum flow protection, overspeed protection, speed control, and other similar pump and pump system controls are not part of this modernization.

4. **RHR:** The RHR will have eight active automated modes of operation. The RHR will operate in one of the following active modes: (1) LPCI, (2) Containment Cooling, (3) Service Water Cross Tie, (4) Shutdown Cooling, (5) Fuel Pool Cooling Assist, (6) Radwaste Discharge, (7) Alternate Decay Heat Removal, and (8) Flow Test. The RHR system will provide heat removal functions for cooling the reactor core and Containment during normal and postulated accident conditions and assist in cooling the Spent Fuel Pool during refueling. The RHR will be able to inject RHR Service Water to the reactor and to Containment. The RHR will be able to transfer Suppression Pool water to the Radwaste System.

   The requirement to activate RHR in LPCI mode in each of the divisions will be satisfied if either division detects conditions requiring RHR to activate in LPCI mode. The existing logic has six analog trip units in each division, for a total of 12 analog trip units. To simplify the design, each channel will provide a bi-stable output for Low Reactor Vessel Water Level, Low Reactor Vessel Pressure, and High Drywell Pressure to the RHR function. Each division will evaluate each of the channel's data individually, evaluating the Boolean expression for each of the channels, where TRUE is defined as the condition existing and each channel is defined as (x):

   RHR LPCI Vote (x) = {Low Reactor Vessel Water Level (x) OR [Low Reactor Vessel Pressure (x) AND High Drywell Pressure (x)]}

   Each division will then perform a 2oo4 vote on the RHR LPCI Vote (x) results. The voted result will determine whether an RHR LPCI condition exists for each division. Division 1 will initiate RHR LPCI Train A and Division 2 will initiate RHR LPCI Train B. The expectation is that both divisions will operate on similar data, through identical logic, resulting in both divisions identifying a condition requiring RHR to activate in LPCI mode. The RO will be able to initiate RHR in LPCI mode.

   The **LPCI** mode of RHR will use water from the Suppression Pool. The water will be injected using the LPCI Injection Lines. The LPCI mode will be automatically initiated as described above, when required.

   Containment Cooling will be performed when cooling the Suppression Pool or in the Containment Spray Cooling mode. The RHR will pump Suppression Pool water through the RHR Heat Exchangers and return the cooled water to the Suppression Pool. In the normal or emergency mode, the RHR Full-Flow Bypass Valves will be modulated automatically to maintain a set flow rate. In the modernized PPS, the RO will set this flow rate into the DKT and initiate either the automated normal or emergency mode manually using soft controls. The RO will be able to stop this mode in either RHR

Division A or RHR Division B using the DKT soft controls. No changes are proposed to the existing interlocks between RHR injection and containment cooling modes.

For **Containment Cooling in the Suppression Pool Cooling mode**, the RHR mode will source water from the Suppression Pool through RHR pumps. The water will be pumped through the RHR Heat Exchangers and return the water to the Suppression Pool. The RHR Full-Flow Bypass Valves will be modulated to maintain a set flow rate. In the modernized PPS, the RO will set this flow rate into the DKT and initiate either the automated normal or emergency mode manually using soft controls. The RO will be able to stop this mode in either RHR division using the DKT soft controls.

For **Containment Cooling in the Containment Spray Cooling mode**, the RHR will source water from the Suppression Pool. The water will be cooled in the RHR Heat Exchangers. The water will be returned through spray nozzles and spray spargers in the Drywell and Wetwell. Containment pressure and temperature are reduced by cooling hot-non-condensable gases and condensing steam in the Drywell and Wetwell. Flow will be controlled by modulating the Suppression Pool Spray Valves and the Containment Spray Cooling Outboard Isolation Valves automatically. In the modernized PPS, the RO will set this flow rate into the DKT and will initiate this automatic mode using soft controls. The RO can stop this mode in either RHR division using the DKT soft controls.

The **Service Water Crosstie** will provide long-term, post-LOCA Containment flooding above the top of the active fuel, when the ECCS is unable to maintain Reactor Vessel Water Level above the active fuel. The RHR Service Water will be the water source. In the modernized PPS, the RO will initiate this automatic mode using soft controls. The RO will be able to stop this mode in either RHR division using the DKT soft controls.

Shutdown Cooling will transfer decay heat and Reactor Primary System sensible heat to the RHR Service Water for cooldown and to maintain cold shutdown. During initial operation, the CR will place only one RHR in Shutdown Cooling mode, to ensure that the other RHR division is available for LPCI. After cooldown below the boiling point, both RHR divisions can be used in this mode. During this mode, the Heat Exchanger flows will be throttled to a setpoint value. In the modernized PPS, the RO will set this flow rate into the DKT and will initiate this automated mode in one division using soft controls. The RO will be able to stop this mode in either RHR division using the DKT soft controls. Several different alignments will be possible and all will be automated.

The **Fuel Pool Cooling Assist** mode will provide additional cooling for the Fuel Pool Cooling and Cleanup System during refueling when new spent fuel may emit more heat than the Fuel Pool Cooling and Cleanup System can remove. This mode will draw water from the Fuel Pool Skimmer Surge Tanks, cool the water in the RHR Heat Exchangers, and return the cooled water to the fuel pool through the RHR to the Fuel Pool Cooling and Cleanup line. There are several valve lineups possible in this model, all of which will be automated and selected through the RO's DKT, assuming the flow paths have been opened in the field by the replacement of blind spool pieces. No flow control will be performed. In the modernized PPS, the RO will initiate this automated mode in one division using soft controls. The RO will be able to stop this mode in either RHR

division using the DKT soft controls. Several different alignments are possible, and all will be automated.

The **Radwaste Discharge** mode will support the transfer of water from the Suppression Pool to the Radwaste System. Excess water will be removed to lower the Suppression Pool level to maintain the level within TS limits. This alignment will take water from the Suppression Pool, through the RHR Heat Exchanger and Heat Exchanger Bypass, and then through the RHR to the Radwaste line. No flow control will be performed. In the modernized PPS, the RO will initiate this automated mode in one division using soft controls. The RO will be able to stop this mode in either RHR division using the DKT soft controls. Several different alignments are possible, and all will be automated.

Alternate Decay Heat Removal will maintain reactor vessel and fuel pool temperatures and will be used when heat loads exceed the capabilities of the Fuel Pool Cooling and Cleanup System and RHR Shutdown Cooling is unavailable or needs to be taken out of service. The RHR Heat Exchangers will be aligned for RHR Alternate Decay Heat Removal. During refueling, heat loads will exceed the capabilities of the Fuel Pool Cooling and Cleanup System. The Fuel Pool Skimmer Surge Tanks will be the water source through the Fuel Pool Cooling and Cleanup to RHR line. One RHR pump and RHR Heat Exchanger will remove heat from the fuel pool. The cooled water will be returned to the Reactor Recirculation Discharge Line through the Shutdown Cooling Return Line. Flow will be throttled automatically to a configurable value. In the modernized PPS, the RO will initiate this automated mode in one division using soft controls, assuming the flow paths have been opened in the field by the replacement of blind spool pieces. The RO will be able stop this mode in either RHR division using the DKT soft controls. Several different alignments are possible, and all will be automated.

Flow Test will be performed by taking water from and returning water to the Suppression Pool. Pumps A, B, C, and D pump through the Full-Flow Bypass Valves. The Full-Flow Bypass Valves will be throttled automatically to control the water flow to configurable values. In the modernized PPS, the RO will initiate this automated mode in one division using soft controls. The RO will be able to stop this mode in either RHR division using the DKT soft controls. Several different alignments are possible and all will be automated.

5. For **ADS**, all five SRVs will be controlled as a group, using individual divisional outputs to each of two SOVs on each SRV. Both the existing and modernized design provide two individual sets of logic in each voting logic and division (Division 1A and 1B will comprise one set of taken twice, while Division 2A and 2B will comprise the other set of taken twice), respectively. Both logic sets in each division will be required to actuate to control the SOV for that division. Both outputs from Division 1A and 1B or both outputs from Division 2A and 2B will be required to open the SOV on the SRV, requiring two sets of logic in the same division in a 2oo2 vote to initiate ADS. The modernized PPS will use data from all four channels and independent voting in the two divisions (four subdivisions) to control the field SOVs. The outputs from the logic solvers to the ADS will be single-failure tolerant.

Dual pairs of divisional Manual Initiation pushbuttons will be provided, which must be pressed simultaneously to initiate ADS in the operator selected division. Logic for manual initiation will require at least one RHR pump or at least one CS pump to be running. The Manual Initiation pushbuttons will start the ADS function immediately, as the ADS Initiation Timer is not used.

The HSI will have soft controls that allow the operator to select individual ADS Solenoid B outputs. These will allow the RO to open individual ADS SRVs for a more controlled depressurization, in accordance with plant procedures. The HSI will provide Auto and Open selections and will require at least two widely separated operator selections to initiate ADS opening. The HSI will show the lifted states of the ADS SRVs.

Each of the four channels will provide a bi-stable reflecting high Drywell Pressure. The divisions will perform a 4oo4 vote and seal in a voted TRUE high Drywell Pressure signal.

Each of the four channels will provide a bi-stable reflecting low Reactor Vessel Water Level at Level 1. The divisions perform a 4oo4 vote.

Each of the four channels will provide a bi-stable reflecting low Reactor Vessel Water Level at Level 3. The divisions perform a 4oo4 vote.

Each division's ADS actuation timer will start when the individually 4oo4 voted high Drywell Pressure, Reactor Vessel Water Level at or below Level 1, and Reactor Vessel Water Level at or below Level 3 are all TRUE and the ADS manual logic inhibit and Reset switches are in the normal (not inhibited and not reset) positions. If any of these conditions are not met, the 105-second actuation timer will not start. After the ADS actuation timer times out, the Reactor Vessel Water Level is not restored, and at least one RHR pump or at least one CS pump is operating, the first logic will be satisfied. One copy of this logic will be provided, using the more conservative design. Two copies of the logic will be run in each division.

Once the voted Reactor Vessel Water Level is at or below Level 1, a 420-second timer will start. When the timer times out, the high Drywell Pressure voter output will be bypassed. With the vote bypassed, the Reactor Vessel Water Level low signals and the same pump running signals will be able to initiate ADS.

In the modernized design, non-divisional dual manual reset switches will be provided for the initiation logic, where both switches must be pressed for the reset to occur. The reset switches terminate the ADS condition and return the solenoid valves to their normal operating position. The reset switches will inhibit ADS operation and reset all ADS timers. The ADS reset switches will unlatch the seal-in circuits if Reactor Vessel Water Level is greater than Level 1.

3.4.5 Modernized HSI System Design Functions (DI&C-ISG-06 D.2.3.1)

The existing RPS, N4S, and ECCS provide manual switches of various types to provide the watch standing RO with the ability to scram, initiate isolations, initiate emergency core cooling functions, and initiate actions using safety equipment to perform non-safety related actions (e.g., the use of the RHR to perform functions other than LPCI). There are also CR switches of various types to support resets and terminations within the constraints established in the relay logic.

Any data indications in the CR are provided by separate meters and recorders, which are hardwired into the analog field instrument loops. Additional status information is provided by various indicator lamps in the CR, which are hardwired to field instrumentation, such as relay coils, relay contacts, and limit switches.

In the modernized PPS, manual switches will be provided for various CR actions with direct control of field state, such as the reactor scram switches, as described in Section 3.4.1.6. The functionality of these manual switches will also be provided through the DKT HSIs, implementing the manual function using the application logic and the normal paths through the application logic. The indicator lamps will be replaced by indications on the DKT HSIs.

For the modernized PPS, data indications in the CR that were provided by separate meters and recorders will be replaced with the capability to display any of the analog field data in engineering units as well as the discrete field data and internal status in English text on the DKT HSIs. During the detailed design, an evaluation of the need for SR trends will be determined. If SR trends are required, the SR DKT Interfaces will be augmented to retain the required trend data for each channel and each division, with Human Factors Engineering involvement.

The DKT HSIs will provide a means of displaying all of the data available in the DAS, providing a diverse means of reading the data, based on the DAS capabilities discussed in Section 3.4.6. The DCS will provide NSR trending capabilities. Native DCS capabilities will be used to provide trend data for SR and NSR data. Trends will be created during detailed design, based on operator needs during expected conditions, with screens designed with Human Factors Engineering involvement.

3.4.6 Modernized DAS System Design Functions (DI&C-ISG-06 D.2.3.1)

The DCS will provide the DAS function for selected actuations in the N4S and ECCS. In a separate project, the DAS will also provide the ATWS functions, replacing the existing RRCS. EIMs will provide discrete outputs for the PPS and DAS. The EIMs will incorporate priority logic to ensure the safe operation of the plant safety-related systems and to provide non-safety to safety-related isolation for the control outputs from the DCS.

The modernized ATWS, providing the DAS for the RPS functions, will duplicate the system design functions from the existing RRCS, with three exceptions:

1. The reactor feedwater pump runback will be removed, as discussed in Section 3.3.6.2.

2. The automatic function that initiates SLCS and isolates RWCU will be augmented with an inhibit capability. The watchstanding RO will activate the inhibit during ATWS maintenance, to ensure that human performance error does not inadvertently initiate SLCS. While SLCS inhibit is active, a control room annunciator will indicate that SLCS is inhibited. When maintenance is complete, the watchstanding RO will remove SLCS inhibit. Inhibiting SLCS will not prevent manual initiation of SLCS.

3. The only ATWS outputs that feed safety-related equipment will be the trip coils in the safety-related reactor recirculation pump breakers. The credited isolation between the non-safety related electric power to the trip coils and the safety-related breaker will be between the trip coil and the trip hardware within the breaker.

The maximum response time for the modernized PPS will be the same as the existing system. This system will not have the same time response as the RPS but will have a sufficient time response to support the analyses in the LGS UFSAR Chapter 15 (Reference 41).

TBD/TBC 21: Find the time response requirements for the DAS, including any impacts on Chapter 15.

TBD/TBC 22: LGS needs to initiate a D3 Analysis under NUREG/CR-6303

TBD/TBC 23: It is assumed that credit can be taken for the trip coils in the Reactor Recirculation Pump Motor Breakers as non-1E to 1E isolation, else use an EIM for this isolation.

All ATWS outputs will be energize-to-actuate. For the each of the actuation outputs, each of the two divisions will be discrete outputs that are single-failure tolerant and diagnosed. Failure of a single discrete output to a shorted state cannot initiate any protective action (e.g., SLCS pumps or fire squib valves) and failure of any single discrete output to an open state cannot preclude the initiation of ATWS functions

The modernized ATWS function in the DAS will retain the existing design for each ARI SOV. The divisional ATWS output load drivers will be wired in series, such that the Division 1 load driver will be wired to 125 V dc power, the output of Division 1 will be wired as the power input to the Division 2 load driver, and the output of the Division 2 load driver will be wired to one of the ARI SOVs. In this manner, both divisions must actuate to actuate one ARI SOV. A similar circuit will exist for the other ARI SOVs. Both load drivers must turn on to actuate. This requirement will provide additional output voting protection used with a 4oo4 in the segmented controllers.

The modernized ATWS function in the DAS will retain the discrete output configuration for the RPT breaker trips. Division 1 will power the trip coil on the RPT 3A and 3B breakers individually. Division 2 will power the RPT 4A and 4B breakers individually. Opening either the 3A or 4A breaker will trip Reactor Recirculation Pump A, and opening either the 3B or 4B breaker will trip Reactor Recirculation Pump B.

The modernized ATWS function in the DAS will not trip (incorrectly labeled as run back in the existing RRCS) the reactor feedwater pumps. LGS has demonstrated that this feature risks uncovering the core, since the feedwater pumps are still sourcing water when this automated action occurs. This automated action in the existing system challenges the safety systems unnecessarily, requiring the HPCI or RCIC to initiate when the existing system trips the reactor feedwater pumps. In the modernized system the operator will make a conscious determination for securing the normal non-safety related Reactor Feedwater Pumps. The modernized PPS will remove this automated function but leave the existing manual Reactor Feedwater Pump controls in the CR unchanged.

The modernized ATWS function in the DAS will retain the field 2oo2 vote for SLCS initiation. Division 1 and Division 2 will both have to energize to initiate the selected two SLCS pumps and open the isolation squib valves.

3.5 SYSTEM REQUIREMENTS DOCUMENTATION (DI&C-ISG-06 D.2.3.3)

The PPS Functional Requirements document (Reference 9) provides the required materials to satisfy DI&C-ISG-06 Sections D.2.3.3, D.2.3.3.1, and D.2.3.3.2 for the RPS, N4S, and ECCS functions. The PPS Functional Requirements document defines the interfaces and interactions between these safety-related systems. The PPS Functional Requirements document states that there are neither interfaces nor interactions between the safety-related RPS, N4S, and ECCS and the DAS.

The DAS Functional Requirements document (Reference 58) provides the required materials to satisfy DI&C-ISG-06 Sections D.2.3.3, D.2.3.3.1, and D.2.3.3.2 for the DAS. The DAS Functional Requirements document states that there are neither interfaces nor interactions between DAS and the PPS. The DAS does use the same transmitters used by the PPS, with appropriate safety-related to non-safety related qualified isolators in each of the transmitter current loops.

3.6 FUNCTIONAL ALLOCATION (DI&C-ISG-06 D.2.4)

3.6.1 Functional Allocation in PPS (DI&C-ISG-06 D.2.4.1)

The functional allocation in the PPS functions will not change, with a few minor exceptions as discussed in this LAR Framework Document section.

The PPS will incorporate the functional requirements for the existing RPS in the RPS function, for the existing N4S in the N4S function, and for the existing ECCS in the ECCS function. The platform software will sample field sensing inputs and convert the values to engineering units. The application software in the channels will check the engineering unit values against setpoint values with appropriate hysteresis to determine if trips or actuations are needed. The channels will provide their independent votes to divisions through fiber optic serial communication links. The divisions will implement voting and logic to place the field actuators in the appropriate conditions and provide appropriate status information to annunciators and other status indicators in the CR. The HSI will provide the watchstanding RO and SRO an accurate view of the plant status. The modernized HSI will replace many indicator lamps and annunciator windows with

displays on DKTs. The DCS will gather and save the plant data for future use. DKTs will provide soft controls to the channels and divisions. All of the logic will be implemented in application software, including bi-stable, voting logic, operating bypass logic, maintenance bypass logic, formatting data for output to displays, and formatting data for output to the data network (see Figure 3-24).

The design will implement the analog trip modules (i.e., bi-stables) in application software in the channels. The design will implement the voting and logic in application software in the divisions. Design and implementation verification and validation (V&V) will verify that these functions are implemented within the time allotted in the Functional Requirements document, LGS UFSAR, and TS.

There are Operator manual actions (e.g., reactor scram) that will be assigned totally to wiring and interposing relays (as necessary). The design will eliminate all manual switches that do not actuate functions (e.g., manual scram), which the design retains, as required in regulation. The PPS design for these manual switches will require a hardware implementation of the switching function, with no potential for the PPS software to preclude the requested Operator action. The design will provide feedback to the PPS that the Operator has requested manual actions, to ensure that the PPS software conditions itself appropriately for the plant's response and updates the status sent to the DCS. The design will implement all the switches as soft controls, including soft control equivalents to the hardwired switches, in PPS application software. The DAS will implement diverse soft controls for those functions implemented in the DAS.

Service functions will be assigned to hardware, software, and operators using the PPS platform and application software and the DKTs.

The PPS will provide data to the DCS, which the DCS retains as historical data and uses to perform continuous online channel checks. When a persistent disagreement of redundant transmitters or decisions is detected by the online DCS channel checks software, the issue will be annunciated in the CR and available for display on a non-safety related DKT.

3.6.2 Functional Allocation in DAS (DI&C-ISG-06 D.2.4.1)

For the ATWS portion of the DAS, the functional allocation will be unchanged, with application software that runs on a platform under an operating system. The hardware will be implemented in standard DCS hardware, and the functions assigned to the operator will remain the same.

For the rest of the DAS, the functional allocation for the PPS will be mirrored in the DAS. The DAS application software will perform the same functions assigned to those portions of the PPS duplicated in the DAS. The DAS will be implemented in the same standard DCS hardware as the ATWS functions. The functions assigned to the operator will remain the same as those assigned to the operator in the portions of the PPS duplicated in the DAS.

Service functions in the DAS will be those required to maintain the DAS application software, DCS platform, and DCS communications.

3.7 SYSTEM INTERFACES (DI&C-ISG-06 D.2.5)

3.7.1 PPS Interfaces (DI&C-ISG-06 D.2.5.1)

3.7.1.1 PPS Interfaces to Other Systems

The existing RPS, N4S, and ECCS in Unit 1 do not interface or interact with the existing RPS, N4S, and ECCS in Unit 2 in any way, and the existing Unit 2 RPS, N4S, and ECCS do not interface or interact with the existing Unit 1 RPS, N4S, and ECCS in any way. The modernized PPS will continue to be unit-specific and will not be connected in any way.

Data flow within the PPS and external to other systems is explained in Section 3.3.

The PPS Functional Requirements document (Reference 9) documents the interfaces between the PPS and other plant process systems. For the GE BWR, the field inputs and field outputs are each considered interfaces to other systems, since the field input transmitters and field output actuators are part of the mechanical system on which the field I&C equipment is installed. The wiring to the field inputs and field outputs is over existing hardwired connections.

The PPS will provide SOE data to the existing system and first-out data to the existing annunciator through qualified, isolated dry relay contact outputs. These outputs will be designed to have minimal, deterministic delays. All alarm status, including the SOE and first-out status, will be provided to the PPS through redundant fiber optic communication links to the DCS.

3.7.1.2 PPS Interfaces and Communication

Serial data communication over redundant fiber optic links is described in Sections 3.1, 3.3.5, and 3.7. The capabilities of the platform, as described in the vendor's licensing topical report (Reference 42) and in the NRC's SE Report (Reference 43), are used to implement all communications, which will include:

- Unidirectional communication from channels to divisions
- Unidirectional communication from the channels to the non-safety related DCS
- Unidirectional communication from the divisions to the non-safety related DCS
- Bidirectional communication between channels and DKTs
- Bidirectional communication between divisions and DKTs
- Bidirectional communication between the EWS video generator and DKTs

There will be no communications from any non-safety related system into the PPS. All communications with non-safety related systems will be through unidirectional links, from the PPS to the non-safety related system.

3.7.1.3 PPS Interfaces to DKTs as HSI

While the safety-related DKTs will connect to and bidirectionally communicate with non-safety systems, there is no potential for data from the non-safety system to affect operation of the PPS or any other safety-related system attached to the DKT system.

The PPS and EWS design will only allow the EWS to interface to one channel or division at a time. Normally, the EWS will be disconnected when the PPS channel or division is not bypassed. The EWS and the DKT supporting the EWS will be mounted permanently in the AER in a locked cabinet.

As stated in Section 3.3.5.2, any DKT that has the capability to perform safety system actions affecting the plant will be restricted to those available to the RO. If a DKT is provided at the RSS panel locations, that DKT will operate in a data display only mode. Only the DKTs installed at an RO location in the CR will have the ability to perform soft controls, which will allow the RO to perform any manual action, including the duplicated function to initiate trips and actuations. The soft controls will be the primary means for the RO to perform all resets, terminations, and other similar actions.

Section 3.3.5.1 also describes how the design and implementation of the DKT Interfaces, DKT Switches, and DKTs ensures that cross-connections between systems are not possible and that no data is retained in the DKT Switch or DKT. There is no potential for actions on one DKT being provided to multiple DKT Interfaces and no potential for data saved in a DKT corrupting a DKT. Thus, systems connected to the DKT network cannot interfere with each other through the DKT system.

3.7.1.4 PPS Interfaces to Hardwired HSI

The PPS interfaces in the CR will include only the required manual scram and actuation switches. The modernized system will provide hardwired functionality for the switches as required, eliminating the potential for a PPS software common cause failure to inhibit the manual performance of required safety functions. The existing system used all of these switches as inputs to the relay logic. The modernized system will provide the required manual scram switches as separate actuations, not affected by a PPS software common cause failure. The actuation switches will be monitored by the PPS, and appropriate actions will be taken by the application logic. The manual scram switches will initiate the RPS reset lockout timer after a manual scram, providing the same PPS functionality as in a scram initiated by the RPS function. The existing interfaces in the CR will include manual operator maintenance bypass switches, which will provide the ability to take a channel out of service for testing and calibration. Where these switches are not required for immediate action during accidents or transients, the modernized system will remove the switches and place their function on the DKTs, duplicating the functionality of the existing system.

The existing CR does not have displays for the RPS inputs. In the existing system, values for the inputs to the trip units are available only on the trip units themselves in the AER. While the existing non-safety related PPC displays do provide some RPS values, these values are isolated through qualified isolators, sampled by PPC analog and discrete input modules, processed through PPC software, and displayed on PPC displays. Accordingly, with the existing systems,

the watchstanding operator does not have access to the PPC data to make decisions about the LGS safety status, other than through hardwired HSI meters and recorders. The modernized DKT will provide the RO and SRO with RPS-sensed plant parameter data as well as appropriately chosen status data within the logic solvers. This modernization will replace, but not eliminate, the hardwired CR meters and recorders associated with the PPS functions.

3.7.1.5 PPS Support Systems

Continued long-term operation of the PPS and DKT system will depend on several support and auxiliary systems.

The PPS and DKT system depend on electrical power. The PPS and DKT system power will be supplied from redundant, uninterruptible vital power that is backed by the EDGs. The existing uninterruptible power sources can be bypassed to connect to the power grid. The PPS and DKT system will be tested for connection to low quality power, so connections to the power grid have no adverse effects on the equipment.

The PPS and DKT system will depend on the HVAC system to cool the AER and CR. While the PPS and DKT equipment can withstand higher temperatures, operation at elevated temperatures increases aging, which decreases overall equipment life and reliability.

3.7.1.6 PPS Application of Hazards Analysis

As explained in Sections 5.1.4 and 5.2.4, hazards evaluation is performed on the complete PPS, DKT system, and DAS and will be used to inform the design, development, review, and test of the systems. Communications hazards, including but not limited to those in DI&C-ISG-04 (Reference 44), have been and will be considered and incorporated in the design. Each division will evaluate the quality of the redundant messages passed from each channel, using the criteria including that in DI&C-ISG-04 to determine if the messages are acceptable, and, thus, if the communication links are functioning.

For the detection of faults and failure, the non-safety related DCS will also receive redundant messages from the PPS. The DCS will time stamp the data in each message and save the time stamped data in the data historian. Data from the PPS, self-tests and diagnostics within the PPS, and other features within the PPS logic solvers and the non-safety related DCS will be used to automate channel checks and eliminate the manual functions previously performed by the CR staff. The DCS will extend that check to an evaluation of the derived PPS status, to ensure that all channels and divisions are operating correctly. The DCS will compare the data from the isolated sensors provided to the DAS to the PPS data for the same sensors, to ensure the isolated data sampled by the DAS is sufficiently close to the data used by the PPS, and will thus validate that the DAS and PPS are operating with similar plant states.

Hazards evaluation drove the DKT Interface design. The DKT Interface will determine if data is being received from its data sources and indicates failure for repair. Further, the DKT displays will provide PPS data directly from the PPS, or indirectly through the DCS. This diverse routing will provide the RO and SRO with multiple paths to the PPS data, compensating for the dual failure of redundant communication links.

The modernized design will be driven by hazards analysis for the PPS application software. The PPS design will provide reliable single-failure tolerant discrete output switching, to ensure that no single failure in an output switch disables or falsely initiates protective actions. Failure of a PPS output switch is viewed as the most likely source of spurious actuations. The single-failure tolerant design for the discrete output switches is intended to ensure that no single failure of a discrete electronic switch results in spurious actuation and that failures in the electronic switches are diagnosed and repaired in a timely manner.

The single-failure criterion will be applied to the complete design, to ensure that no single failure can preclude implementation of the safety function. Application of the single-failure criterion led to splitting the N4S divisions. The split divisions will ensure that either the inboard or outboard isolation valve will close if one of the split divisions in the N4S fails. Similar design choices will be implemented in the PPS application software, to ensure that documentation of identified hazards exists, demonstrating elimination of hazards or defining mitigations employed. In addition to the hazards analysis documentation, mitigations will be documented in the software requirements and detailed design as hazard mitigations, to ensure appropriate care and retention during software modification.

3.7.2 DAS Interfaces to Other Systems and Displays (DI&C-ISG-06 D.2.5.1)

The DAS functions will be standalone segments within the selected DCS. The DAS will be built inside the selected DCS, so that the DAS shares the DCS platform with other functions. The DAS interface with those other DCS functions will be purely at the system level, to provide user interface functions and capture DAS data in the historian for non-control uses. The DAS will not depend on any inputs from or processing in other plant systems.

3.8 FUNDAMENTAL DESIGN PRINCIPLES IN THE NEW SYSTEM (DI&C-ISG-06 D.2.6)

Sections 3.1 and 3.3 describe the systems and define the system architectures for the PPS and DAS, which should be referenced while reviewing Section 3.8.

3.8.1 Design Principle: PPS Redundancy (DI&C-ISG-06 D.2.6.2.1)

Redundancy will be provided in the PPS to ensure that a single failure will not inhibit the performance of the safety functions, as bounded by the LGS UFSAR. The degree of redundancy will vary with the risk that the PPS function or subfunction resolves. A single failure analysis will require not only the assumption of any possible single random failure but also the inclusion in the single failure analysis of all undetectable failures simultaneously with the assumed single random failure. Accordingly, the system will be designed to detect all possible failures through a combination of self-diagnostics and periodic surveillance testing. No identified undetectable failures will remain in the system design.

3.8.1.1 Redundancy in the RPS, N4S, and ECCS

For the modernized RPS and ECCS functions, four redundant sets of field sensors will provide data to four independent, redundant channels. The four channels will independently provide

votes to scram or actuate to the two redundant divisions, which will perform the voting function within each division. The 2oo4 taken-twice voting will allow one channel to be in maintenance bypass and another channel to fail, without compromising the ability of the RPS to perform its safety function and without resulting in an inadvertent actuation of the safety function. The taken-twice nature of the divisions in the field actuating devices will require that the failure of a division drives the division's outputs to achieve the fail-safe, de-energized state, thus generating a half scram, half actuation, full actuation, half isolation, full isolation, or disable an energize-to-actuate or isolate function, depending on the function. If both divisions fail, both divisions de-energize their outputs, which will generate a full scram or may generate (or disable) isolations and actuations.

For the modernized PPS, similar sets of redundant field transmitters and switches in the existing RPS, N4S, and ECCS will be eliminated, retaining one set of redundant field transmitters and switches to be used by all functions within the PPS.

The PPS will use highly reliable, single-failure tolerant, diagnosable load drivers in each division for all outputs.

For the existing N4S, the existing redundancy varies from four field transmitters or switches providing plant status data to all four channels, to two field transmitters or switches providing plant status data to two selected channels, down to one field transmitter or switch providing plant status data to only one channel. The modernized N4S function will be designed within the boundaries of the existing field hardware.

The modernized N4S function will replace all the equipment in the AER but will not replace actuations performed only in field equipment. The actuations performed in field equipment provide status information back to the CR, which the N4S will sample and display on DKTs.

The modernized design will provide additional redundancy in the fiber optic serial communication links from the PPS channels to the PPS divisions. All PPS channels will provide the votes to scram, actuate, or isolate redundantly to ensure communication issues (e.g., failure to send, sending an old message, corruption of the message) will not adversely affect the ability of the PPS to perform the required protective actions. Two channels will be powered from one electrical division. The other two channels will be powered from the other electrical division. Accordingly, the design will add logic to each division such that the failure of both channels in the other division generates a condition where only one additional channel needs to vote to scram, isolate, or actuate to initiate the action. Only one additional channel actuation will be needed, since the failed division will ensure initiation of a half scram or partial initiation of a de-energized protection action.

Alternatively, the modernized channel failure logic may be viewed as being reduced in the following sequence for four redundant field sensors:

- All channels normal, actuation logic is 2oo4
- One channel failed or bypassed, actuation logic reduces to 2oo3 (i.e., the first failed channel is automatically bypassed)

- Two channels failed or one failed and one bypassed, actuation logic reduces to 1oo2 (i.e., the second failed channel is treated as a channel actuation)

- Three or four channels failed, actuation logic results in a safety actuation (i.e., the third failed channel is also treated as a channel actuation resulting in two actuated channels and satisfying the 2oo4 actuation logic).

The design will provide redundant communication processors to transmit and to receive each of the redundant fiber optic communication links, to ensure that the failure of a single transmitter or receiver does not disable data communication from channels to divisions. In order to ensure that each division receives the same data from each channel, a fiber optic splitter will be provided after each transmitter, cloning the message for each of the divisional receivers. This will ensure that both divisions receive the same data, thus producing the same results.

The PPS FMEDA (Reference 55) defines how the system failures affect the unit, as well as how individual inputs, outputs, individual module, and processing module failures affect the operation of the system and thus affect the unit. The FMEDA demonstrates compliance with the single-failure criterion and documents how single failures cannot block the safety function. The FMEDA also assesses the ability of the device self-tests and self-diagnostics to detect faults and failures within the device, for annunciation.

The redundancy and the FMEDA support the revised and unrevised TS Limiting Conditions for Operation (LCO) and SR, as defined in Section 8.

Having redundant channels supports the General Design Criteria (GDC) 21 (Reference 59) requirements for reliability and testability, in that redundancy decreases the impact of faults and failures by having multiple copies of the same action performed separately, thus assuring at least the minimum number of elements to be working when needed. Similarly, having redundant channels allows for calibration checks of one channel, while the other redundant channels continue to operate. For elements of the N4S that have fewer than four channels, the NRC evaluated and accepted the overall system reliability associated with failure of one non-redundant or two redundant channels in the original plant licensing. The modernized system does not change the existing redundancy of field sensing or actuation equipment.

The modernized PPS will retain the same separation of protective and control functions as were implemented in the original RPS, N4S, and most of the ECCS functions. The modernized design will augment the ECCS logic with additional operator selected automatic features to automate control of Reactor Vessel Pressure, Reactor Vessel Water Level, or flow for the HPCI and RCIC water injection systems. This control function is currently expected to be performed by an RO during an event. Automation will eliminate this Operations burden. With the exception of the removal of the FIC, the controls for the HPCI and RCIC will remain the same.

The modernized design copes with single failures within each channel or division as required in IEEE Std. 603 (Reference 4), Clause 5.1, Single-Failure Criterion. Redundancy is provided to deal with faults and failures in the channels by use of appropriate voting. The channels and divisions will have internal redundancy in power supplies, and controllers. The divisions employ a single-failure tolerant design for the redundant discrete output modules.

The analysis of the modernized design will consider reliability analysis, based on systems hazards analysis and demonstration of reliability through the application of the platform for extended periods. Software is not yet amenable to quantitative analysis, but a qualitative analysis of the platform and software tools has been performed by the vendor. The application software will be designed, implemented, verified, and validated under a quality process compliant with 10 CFR 50 Appendix B and NQA-1 requirements. This analysis will comply with the expectations set forth in Clause 5.15, Reliability, of IEEE Stds. 603 and 7-4.3.2 (References 4 and 5).

IEEE Std. Clause 6.7, Maintenance Bypass, requires that active initiation or removal of the maintenance bypass function not impede the ability of the PPS to perform the required safety functions. Maintenance bypasses of single channels will not impede the safety functions in the RPS and ECCS or in the N4S when more than a single sensor and actuator is provided or when the single sensor and actuator are not in the bypassed channel.

The modernized PPS will comply with the requirements of IEEE Std. 603 (Reference 4).

The modernized PPS will comply with IEEE Std. 379 (Reference 36).

3.8.1.2 Redundancy in the DAS

The DAS will use redundancy to enhance reliability, using the inherent redundancy provided by the DCS, which includes power supplies, communications, and controllers. The DAS implementation will run in two segmented, internally redundant controllers. Similar to the four channel, two division concept of the PPS, the DAS redundancy will be designed to ensure that only required protective actions are taken and that no inadvertent, unintended protective actions occur from single faults or failures in the DAS.

The PPS will provide the four channel-specific sets of field sensor data to the DAS, using qualified isolators in the PPS to provide non-safety related analog and discrete field inputs. The PPS current loops and contact sense will be provided to the DAS, with no PPS software used in any way. The two channels in each "divisional" DAS processor will be independent functions running in the same controller as the voting and sequencing logic. In each "divisional" DAS, the analog and discrete input cards for one channel will be separate from the analog and discrete input cards for the other channel. The channel data will be passed over normal DCS communication links between the two DAS processors, which will then implement those N4S and ECCS functions which are required based on the D3 Analysis.

For reliability, the DAS segments will be made up of a controller pair, redundant power supplies, redundant communication links, and similar features required to ensure that a single detected failure would not impact the DAS functionality.

3.8.2 Design Principle: Independence (DI&C-ISG-06 D.2.6.2.2)

3.8.2.1 Independence in the PPS

Independence ensures that failures do not propagate across independent channels and divisions. The modernized PPS elements will be identified at the cabinet level, using similar identification

as has been provided for the existing equipment as required by IEEE Std. 603 (Reference 4) Clause 5.11. The software versions will be configuration controlled and identified by version as required by IEEE Std. 7-4.3.2 (Reference 5) Clause 5.11.

The hardware for the PPS has been qualified for the environmental stressors consisting of temperature, humidity, seismic motion, and electromagnetic compatibility (EMC) expected in the AER and CR, as required by IEEE Std. 603 (Reference 4) Clause 5.6, including assurance that other safety-related and non-safety related systems and equipment installed in proximity to the PPS equipment in the CR and AER cannot prevent the PPS from performing the required safety functions.

There are no identified credible single events in non-safety related systems that could require protective action and prevent the PPS from performing the required safety functions, as required by IEEE Std. 603 (Reference 4) Clause 6.3. This evaluation is summarized in this LAR Framework Document section.

The modernized PPS will provide the same electrical independence between channels and divisions that was provided by the original system. The two redundant, separate hardware channels within each division will be electrically independent as the two channels spread across different electrical divisions, although the two channels within a division use the same ultimate safety-related power sources as the division. The two redundant, separate hardware divisions will be physically separated, with no interconnections other than fiber optic serial communication links from all four channels. The electrical design, including separation requirements (with the caveat noted in Section 3.1.1) will comply with IEEE Std. 384 as well as the fiber optic routing complying with the informative annex of the latest release of IEEE Std. 384.

From the viewpoint of the installation in the divisional cabinets, the modernized PPS will provide the same physical independence between channels and divisions that was provided by the original system. The two electrical divisions of PPS will be physically separated but in the same fire zones, as originally installed.

The modernized PPS will provide functional independence between channels and divisions, as required by IEEE Std. 603 (Reference 4) Clause 5.6. While the original duplicated identical field transmitters will no longer be present, their absence will not diminish the functional independence between the channels and divisions. Rather, since each channel in the RPS, N4S, and ECCS functions will be voting to take protective action on the same engineering unit values, the PPS is now operating as a unified, consistent whole. The elimination of redundant transmitters will also reduce the time required for calibrating transmitters. The RPS, N4S, and ECCS functions will be logically separate in the PPS, to maintain their functional independence. This design will not compromise the requirement in IEEE Std. 7-4.3.2 (Reference 5) Clause 5.6.

The design of the point-to-point communication links in the modernized PPS will be specified, designed, verified, and validated to ensure that each channel operates independently of all other channels and that each division operates independently of the other divisions, as described in Section 3.7.

The PPS will comply with GDC 13 (Reference 59) in that the functions of the PPS are precisely defined in the PPS Functional Requirements document (Reference 9). The roles of the RPS, N4S, and ECCS are precisely defined in the LGS UFSAR (Reference 41) and in the plant design documents. Analyses to support LGS UFSAR Chapter 15 demonstrate that the existing and the modernized I&C, electrical, and mechanical systems controlled by the PPS have the capability to maintain the plant in a safe state for DBEs.

The PPS will be designed to be reliable, complying with the requirements in GDC 21 (Reference 59). For critical safety functions within the PPS, the four channels and two divisions will ensure reliability by ensuring that one channel can be in maintenance bypass and another channel can fail without adversely affecting the ability of the safety systems to perform the required safety functions.

The PPS will be designed to be testable. One of the goals for the modernized PPS is to demonstrate by analysis that the PPS has sufficient self-tests and self-diagnostics to minimize the amount of manual surveillance testing, thus minimizing the potential for human error and decreased reliability. By self-identifying faults and failures within the logic solver, the PPS will minimize the amount of time detectable errors exist. For all inputs that have the potential to require manual test insertion or external measurement of input values (i.e., use of an external digital multimeter by a technician), test jacks will be provided in the cabinets. For all inputs that have the potential to require manual multipoint calibration checks with external calibration equipment, knife edge disconnects will be incorporated into the field terminations panels. The terminal panels, wiring, test jacks, and knife edge disconnects will be commercial-grade dedicated and considered basic components. The PPS design will minimize the requirements for calibration checks of the analog inputs to the logic solvers.

The RHR subfunction within the ECCS will control portions of the RHR equipment that are non-safety related. The RHR subfunction will be extended to automate controls of this non-safety related equipment to avoid challenging safety equipment through human performance errors. By sequencing valves and valve lineups in a controlled manner, the RHR automation of non-safety related functions will reduce the potential for challenging safety systems (e.g., by draining the Suppression Pool through an incorrect manual valve lineup). Other than the RHR subfunction, the PPS will not control any non-safety related equipment. Other than the RHR subfunction, there will be no non-safety related functions in the PPS, compliant to the intent of IEEE Std. 7-4.3.2 Clause 5.6 (Reference 5).

The PPS will provide qualified isolation for plant transmitter analog loops and discrete switches to the DAS, but the use of those isolated analog loops and discrete switches will not affect the operation of the DAS or the PPS. The PPS will provide qualified isolation for SOE and first-out discrete outputs to non-safety related systems.

The RPS function will provide a set of discrete plant scram outputs that are either on or off, which is not complex control. The N4S function will provide a set of discrete isolation outputs that are also either on or off, which is not complex control. The ECCS function will provide a set of emergency core cooling outputs, which have some limited sequencing and logical state requirements, but none of the discrete outputs provide complex control. The HPCI and RCIC subfunctions within ECCS will include a set of initiation, isolation, and trip functions, which are

not complex control. The HPCI and RCIC subfunctions within ECCS will be augmented with the ability to control injection flow rates based on the operator's selection of Reactor Vessel Pressure, Reactor Vessel Water Level, or flow as the control variable for the simple proportional, derivative, and integral (PID) control.

The PPS FMEA (included in the vendor's licensing topical report, Reference 42, and evaluated in the NRC's SE Report, Reference 43) and FMEDA (Reference 55) will evaluate the failure modes of the equipment and the system, demonstrating compliance with GDC 23 (Reference 59). Even with the inclusion of non-safety related automation functions for the RHR subfunction of the ECCS function, the PPS will be designed such that failures in or removal from service of non-safety related systems, including the non-safety related portions of the RHR subfunction, will not prevent the PPS from performing the required, assigned safety functions, demonstrating compliance with GDC 24 (Reference 59).

3.8.2.2 Independence in the DAS

The non-safety related DAS does not require the same level of independence required within the PPS. The DAS design will include two segmented DCS controllers, each controller implementing the software logic for two channels (i.e., bi-stables) and a single logic division (i.e., voter). The dual channels will be implemented as separate, independent software functions within each of the two controllers. Votes to scram or actuate from all four software channels will be shared between the divisions using the DCS data communication system. The DAS then will perform the voting required for the function and will determine whether to scram the reactor (when the ATWS function is added in a future modification) or actuate or terminate safety functions.

The DAS will use the same single-fault tolerant discrete output structures as the PPS, designed to ensure that each driven output is single-failure tolerant. Single failures in the DAS outputs will neither preclude scrams or actuations nor falsely initiate scrams or actuations, just as in the PPS.

3.8.3 Design Principle: Deterministic Behavior (DI&C-ISG-06 D.2.6.2.3)

All functions will be designed to provide sufficiently deterministic behavior and will operate within the propagation times allotted in the plant safety analyses (UFSAR Chapter 15, Reference 41) from sensing inputs through logic to the driven actuated devices. These functions will provide deterministic behavior, in that the system always responds to a given pattern of inputs and transitions in a defined manner, with the same scrams and actuations. The time delay between input sensed and control outputs will be sufficiently deterministic in time, within the limitations of software task cycles, and will be validated during system design and preinstallation system testing. Once validated, the logic solver time response (while operating at its maximum allowed loading), the logic solver time response will not require field testing, since the behavior of the logic solver is deterministic in both behavior and timing.

3.8.3.1 Deterministic Behavior of the PPS

The PPS will provide deterministic behavior and deterministic timing for the RPS, N4S, and ECCS safety functions implemented in the PPS, as required by IEEE Std. 603 (Reference 4) Clauses 6.1 and 7.1. The PPS will provide sufficient time determinism to implement the

required actions performed to protect the plant. The PPS will provide deterministic actuation behavior for the RPS, N4S, and ECCS functions within the PPS. Capabilities will be provided in the PPS soft controls, implemented in the HSI, for the operator manual control of all DAS functions, as required by IEEE Std. 603 Clauses 6.2 and 7.2.

The HPCI and RCIC subfunctions within ECCS will be augmented with the automatic control of each function's injection flow rates based on the operator's selection of Reactor Vessel Pressure, Reactor Vessel Water Level, or flow as the control variable for the simple PID control. This will replace manual operator control actions and provide additional determinism of reactor conditions when either or both are operating.

The PPS divisions will include seal-ins and time delays to ensure that the initiated scrams and actuations are not reset before the control elements have completely been driven into the reactor core or that the plant conditions return to conditions where the engineered safety features functionality is no longer required.

To maximize quality, the PPS will be designed, implemented, verified, validated, and acceptance tested under a nuclear QA program compliant with 10 CFR 50 Appendix B. The reviews and tests performed will ensure the installations of high integrity systems with required determinism.

The PPS platform will provide a deterministic dispatch of the tasks that implement input scanning, logic solving, communication, and data output. There will be no software elements in the design that have the potential for becoming infinite loops.

Worst-case timing from the channel inputs to the division outputs will require no more than the time allocated in the PPS Functional Requirements document (Reference 9) to scan inputs, solve logic, and output a scram or actuate signal to the field. The worst-case timing will consider (1) plant conditions that change from not requiring to requiring the implementation of a safety function immediately after being sampled, and (2) the worst-case non-synchronized tasks and communication that result in the maximum possible time between the plant condition input and the PPS output.

The maximum delay through separate channels and divisions will be designed such that, when all elements are working correctly, the delay is less than or equal to the maximum timing delay. Since the channels and the divisions are not synchronized, the worst-case timing design will include two channel cycles, two communication message cycles, and two division cycles as the maximum delay, as appropriate to the vendor platform. If the input signal, channel dispatch, communication, and division dispatch are ideally synchronized, the minimum delay will be one channel cycle, one communication message cycle, and one division cycle. For all equipment, timing will be tested over sufficient time to build a statistically valid delay-time histogram. This delay-time histogram will demonstrate the known relationship between sensed reactor parameters, systems states, and driven outputs. The V&V and acceptance testing will demonstrate that the system deterministically provides the same outputs in response to a given set of input signals and the sequencing of those signals. The testing will demonstrate that the system behaves in a deterministic manner both in time and in response to given stimuli.

The assumptions from LGS UFSAR Chapter 15 (Reference 41) are documented in the PPS Functional Requirements document (Reference 9) and will be compared to the results of the time response testing above. This testing will show that the use of communications in the RPS will provide deterministic behavior within deterministic timing limits.

The final system-level hazards analysis will demonstrate that identified hazards have been eliminated or mitigated or are mitigated by the DAS, as required by 10 CFR 50.62 (Reference 8).

The system will be designed to make use of the platform's standard data communications as approved in the vendor's licensing topical report (Reference 42) and evaluated in the NRC's SE Report (Reference 43). The communications capabilities will be used in a manner to retain the deterministic behavior of the RPS, as demonstrated in the time response testing. The communications use will be within the boundaries established in the NRC's SE Report for the platform.

The PPS compliance with GDC 13 (Reference 59) will be unchanged from the original RPS, N4S, and ECCS in that the field transmitters and sensors are not changed and have been licensed to provide the required ranges and monitored variables for normal operation, anticipated operational occurrences, and accident conditions. The PPS logic will provide the safety-related means to maintain plant conditions within prescribed operating ranges in the presence of failures in the non-safety related controls.

The PPS will comply with GDC 21 (Reference 59) in that the system is designed and demonstrated to provide deterministic behavior, which will be tested during V&V activities at the vendor, factory acceptance test, PPS and DAS integration testing, commissioning, and as required by procedures after installation. The required deterministic behavior is defined in the PPS Functional Requirements document (Reference 9).

The PPS will comply with GDC 23 (Reference 59) in that the appropriate parts of the PPS system has been designed to fail to the safe state. For the RPS functions, the safe state is the deenergized, scrammed state. For the N4S functions, the safe state is defined as the de-energized state that either isolates or does not isolate based on the evaluation and design of the unchanged field isolation equipment. For the ECCS functions, the safe state is also defined as the de-energized state that does not initiate ECCS functions.

The PPS will comply with GDC 29 (Reference 59) in that the PPS system is designed to be highly reliable and thus accomplish the safety functions assigned to the RPS, N4S, and ECCS functions in the LGS UFSAR (Reference 41). The safety functions performed and the actions taken by the PPS are not changed from those in the original plant design. The PPS modernization will replace old, obsolete, increasingly unreliable equipment with new equipment.

The PPS divisions will be designed to ensure that functions start and complete, as required by IEEE Std. 603 (Reference 4) Clause 5.2. As an example, the RPS functions will include a reset lockout that is sufficiently long for all control rods to insert before the operator can reset the trip.

As required in IEEE Std. 603 (Reference 4) Clause 5.5 and described in Sections 4, 4.1, 4.2, 4.3, and 4.4, the PPS has been and the HSI will be subjected to equipment qualification tests and analyses which will demonstrate that the equipment will remain operable in the presence of the

applicable environmental stressors and will thus be acceptable for installation in the CR and AER.

Determinism is one of the design attributes that the LGS PPS Vendor Oversight Plan (VOP, Section 5.1.16) will ensure the DAS vendor provides.

3.8.3.2 Deterministic Behavior of the DAS

The DAS will be designed to provide sufficiently deterministic behavior, at maximum specified loading, to support the failure of the PPS to perform the required safety function.

The DCS will provide a platform whose design requires the implementation of deterministic behavior and deterministic timing. The DCS will provide sufficient determinism to keep industrial processes operating smoothly, within defined limits, which is achieved based on the deterministic behavior of the platform and the quality of the application software design.

The function block programming used in implementing DAS functions is designed to provide deterministic behavior and deterministic timing. Determinism is one of the design attributes that the LGS DAS VOP (Section 5.2.15) will ensure the DAS vendor provides.

3.8.4 Design Principle: Defense-in-Depth and Diversity (DI&C-ISG-06 D.2.6.2.4)

Defense-in-depth is a key method that is employed to ensure protective actions are taken. Diversity within the safety function is one means of providing defense-in-depth, in addition to the defense-in-depth provided by diverse means of sensing reactor operational parameters.

3.8.4.1 Defense-in-Depth for the PPS

For the PPS, the sensed field parameters are not changed, preserving the defense-in-depth and diversity of the original RPS, N4S, and ECCS field sensors, which are licensed to provide sufficient functional defense-in-depth and diversity to comply with GDC 13 (Reference 59). The original RPS, N4S, and ECCS logic were constructed of the same analog trip modules, pneumatic time delay relays, and electrical relays. The PPS will be constructed using the same vendor platforms, which will not change the diversity within the RPS, N4S, and ECCS. All the original RPS, N4S, and ECCS functions will be implemented in the PPS, preserving the defense-in-depth and diversity of the original RPS, N4S, and ECCS functionality.

The vendor performed a system-level D3 Analysis (Reference 7) to demonstrate that the PPS accomplishes the safety functions in the presence of a postulated software common cause failure. The modernized ATWS function or the existing RRCS will both provide sufficient defense-in-depth and diversity to protect the RPS safety functions. The DAS has been implemented to provide sufficient defense-in-depth and diversity to protect the N4S and ECCS safety functions. The vendor performed the D3 Analysis in accordance with the current draft of BTP 7-19 and with the established guidance of NUREG/CR-6303[7] (Reference 60). The evaluation used a

[7] In accordance with current NRC guidance from open meetings, this topical report does not follow the erroneous separation of reactor trip functions from engineered safety features functions as two separate echelons of defense.

correction to NUREG/CR-6303, where the Reactor Trip System (i.e., RPS) and the Engineered Safety Features Actuation System (i.e., N4S and ECCS) are considered a single echelon of defense appropriately. The DAS will provide sufficient defense-in-depth and diversity to meet the expectations of GDC 22 (Reference 59).

The normal control systems do not use platforms similar to those planned for the PPS. The normal control systems are designed to maintain the plant reliably in a safe state. The PPS will provide defense-in-depth and diversity for the normal control systems, ensuring safe shutdown and release minimization for design basis conditions where the normal control systems fail.

In a future modification, the DAS will implement the ATWS rules for the RPS portion of the PPS. For this LAR Framework Document, the DAS will implement the diverse functions required by the D3 Analysis (Reference 7) of the N4S and ECCS functions. As described in the evaluation of the DAS below, the PPS and DAS will be built on separate platforms, using different architectures, platforms, software tools, and vendors. The safety-related PPS will provide appropriate qualified isolation for those PPS signals provided to the non-safety related DAS. The DAS will be provided as application software running on appropriately segmented portions of the DCS.

The PPS D3 Analysis (Reference 7) evaluates the PPS and determines the required subfunctions within the N4S and ECCS required in the DAS. The ATWS function provides the regulatory required DAS for the RPS function. The PPS and DAS are designed such that common cause software failures in either the PPS or the DAS will not prevent performance of the required, assigned safety functions. These demonstrate compliance with GDC 24 (Reference 59).

3.8.4.2 Defense-in-Depth Provided by the DAS

The DAS will be designed to provide the defense-in-depth required for a software common cause failure of the PPS. The DAS system will implement the BWR ATWS rules, which provides the diverse shutdown for the reactor, so the ATWS portion of the DAS is the defense-in-depth for the RPS.

Based on the findings of the D3 Analysis (Reference 7), the DAS will also implement those functions required to ensure that, in the unlikely event of a software common cause failure in the N4S and ECCS subfunctions in the PPS, the DAS will provide the operators with sufficient automatic actions to ensure that water remains over the reactor core, decay heat is removed, and radiation is retained within the plant.

The PPS and DAS will be built on separate platforms, using different architectures, platforms, software tools, and different vendor design, implementation, and V&V staff. The safety-related PPS will provide the appropriate safety-related to non-safety related isolation of the same analog signals used by the PPS for the DAS.

The ATWS provides defense-in-depth through diversity to ensure that the reactor shuts down, by supplying appropriate reactivity controls when plant conditions require and the PPS fails. The other DAS functions provide defense-in-depth through diversity to ensure that water remains over the top of fuel, decay heat is removed, and radiation remains within the plant.

3.8.5 PPS and DAS Simplicity of Design (DI&C-ISG-06 D.2.6.2.5)

The PPS will be inherently composed of three relatively simple functions: RPS, N4S, and ECCS. Of the three, the N4S will be the most complex, based on the number of different voting schemes and different plant transmitter counts.

The goal for the PPS is to maintain the inherently simple design of the functions in the PPS, adding complexity only where the added complexity is beneficial.

The modernized PPS will eliminate the complexity associated with design, implementation, test, surveillance, and long-term maintenance of contact closures as a means of communicating votes to scram or actuate from channels to the divisions with the complexity of serial data communications, which LGS concludes reduces the overall complexity of PPS maintenance.

The modernized PPS will use serial fiber optic links to communicate data from channels to divisions, from channels and divisions to DKT Interfaces, and from channels and divisions to the non-safety related DCS. The existing system used contact closures to communicate data from the analog trip units into the relay logic, but only within one electrical division. The complexity associated with doubling the number of copper pairs, required to advance from 1oo2 to 2oo4 voting, would inherently be difficult to install, maintain, and verify operability. The use of serial communications links does increase software complexity. However, the use of serial communications will eliminate the otherwise required large number of discrete outputs, wiring, isolation, and discrete inputs to receive the discrete outputs, provide features to support self-diagnostics, and eliminate the surveillance testing required to ensure the discrete outputs and inputs are working correctly.

The use of redundant serial communications links will decrease the potential for a single serial communication link to fail and disable functions associated with that communication link as well as providing a means to detect such failures in the software when the two redundant links produce different messages. The elimination of the hardware required for the discrete inputs, isolators, and outputs will greatly reduce the potential for undetected hardware failure as well as reducing the probability of hardware failure by reducing the module count. The elimination of discrete data communication will also eliminate the requirement to validate the correct operation of the hardware along with the correct installation wiring, which would be required for the non-chosen communication through discrete outputs and inputs.

One failure mode considered in the modernized design is the failure of multiple communication channels to transmit the same information from channels to divisions. In order to ensure that the same messages are sent to all divisions, a passive fiber optic signal splitter will be installed in each of the channel output to the division input transmission paths. The passive splitter will ensure that the same message is copied to all divisions, eliminating the potential for a failure in one of the communication modules to send erroneous (e.g., old data, corrupted data) to one of the divisions. Use of signal splitters will also decrease the overall number of fiber optic communication transmitter modules, since only two redundant transmitters are required in a channel to send data to four divisions.

Modern systems use software, and analog systems are becoming less common, so the increased complexity associated with software is inherent with applying normal industrial practice to the nuclear industry. The platform has self-tests and self-diagnostics, which have been evaluated and accepted previously. These self-tests and self-diagnostics act as continuous surveillances, identifying faults and failures in the PPS almost as the faults and failures occur, long before periodic surveillance tests would detect them. The benefit of timely discovery is timely resolution of the issue, maintaining the reliability and redundancy and eliminating potential sources of undetected errors. The platform self-tests and self-diagnostics will not affect channel or division independence or defense-in-depth. The design of the platform self-tests and self-diagnostics and the application software will ensure that the deterministic behavior of the PPS application software execution is not affected, which will be demonstrated in testing.

Further, the platform self-tests and self-diagnostics will serve to reduce the potential for human error, by reducing the number of manual tests and calibrations required. By reducing the number of manual tests and calibrations, the potential for human performance error will be reduced. The application software design will incorporate support for the remaining testing, to the extent practical, to further reduce the potential for human error. The reduction of human performance issues in safety-related systems will far outweigh the complexity issues introduced by the platform self-tests and self-diagnostics. The vendor designed the platform self-tests and self-diagnostics into the vendor's platform from the initial conception of the platform.

The complexity associated with data and status display in the CR and AER will resolve a large Operations concern. The modernized PPS will provide PPS data in the CR, including data previously available only in the AER. As an example, the LDS data will be provided on DKTs in the CR, no longer requiring sending an Operator to the AER to read the NUMAC chassis screen. The existing system did not provide the watchstanding RO or SRO with any of the plant data the RPS, N4S, or ECCS were using to determine whether protective actions were required. The nuclear industry implemented channel checks as a workaround, since the existing analog and relay systems could not perform data validation. To implement channel checks, an operator visits the AER and CR to write down plant data over the span of about two hours, every shift. Operations management then reviews and approves that data. In the modernized PPS, the PPS will provide the non-safety related DCS with the PPS and DAS data and will compare redundant sensed values and other information from the PPS and DAS to generate alarms if data mismatches exist. The DCS will frequently evaluate and validate sampled data on a continuous basis, thus providing early notification of issues (e.g., one channel significantly disagrees with the other three) which will initiate a more timely resolution of discrepancies.

The PPS hardware design will further reduce the potential for human error in measurements of inputs and outputs as well as signal injection into the PPS. The input and output points will be provided with test jacks. Those points where technicians could need to inject signals will be provided with knife edge disconnects in the terminal blocks. This hardware design means that technicians will no longer need to de-terminate and re-terminate field wiring to perform measurements and signal injection.

The modernized PPS will increase the complexity of voting in divisions. The modernized PPS will eliminate many identified issues with 1oo2 taken twice. The modernized PPS will eliminate those issues by replacing the existing 1oo2 taken twice or similar voting schemes with a scheme

that uses all the data available from all channels in all divisions. The modernized PPS will work within the limitations imposed by the taken-twice aspects of the existing field implementation.

For the RPS, the design will contain four channels and two divisions, with all channel votes to scram or not scram provided to all divisions for 2oo4 voting. The design will support graceful degradation of the RPS function, allowing the RPS to continue functioning while a maintenance bypass and a failed channel occur. The RPS channels will use identical application software and the divisions will use identical software, reducing development complexity and simplifying V&V.

Similar designs will be provided for the ECCS, which has four redundant sets of signals spread across four identical channels. The ECCS has two identical divisions.

The N4S will have varying numbers of signals spread across the four channels and between the four divisions. Neither the N4S channels nor the divisions will be identical, since there are signals that exist in only one channel and division. The N4S application software will be customized to match the input requirements for the channels and the logic required in the divisions. Where possible, identical application software will be provided for subfunctions, such as ADS, that appear in all channels and all divisions. While this increases complexity, short of adding field sensors, field actuators, and field wiring, this complexity is understood and will be a key consideration for V&V and testing. This design choice will also decrease the potential for half scrams in the RPS and equivalent partial activations in the N4S and ECCS, since all divisions will be evaluating the same set of votes to scram or actuate and should produce the same results. The voting design will also eliminate the potential for the system not to scram if two RPS votes to actuate come from one division. The existing design only generates a half scram. The modernized design will generate a full scram.

The modernized PPS design will consider failure modes associated with discrete outputs and determine that single failures in the outputs neither preclude taking the protective action nor inadvertently result in an unnecessary protective action. The discrete outputs controlling field equipment will be designed to be single-failure tolerant, ensuring that no single failure of an electronic output switch to a shorted or open condition results in inappropriate PPS operation.

This modernization will not change the sensed field data, even as now-redundant original sensors are not used. This modernization will simplify the design of the system by absorbing several analog modules and the NUMAC LDS into the PPS. These actions will not change the field sensing elements but merely the processing of those field element signals. This modernization will thus comply with the requirements of IEEE Std. 603 (Reference 4) Clause 6.4 on derivation of system inputs.

4

Hardware Equipment Qualification (DI&C-ISG-06 D.3)

This LAR Framework Document section documents the type testing and analyses performed by the vendor to ensure the vendor platform can implement the assigned safety functions in an environment that envelopes the LGS plant installation environment (i.e., temperature, humidity, radiation, seismic, and electromagnetic fields). The vendor's licensing topical report (Reference 42) documents the PPS platform equipment qualification tests. The NRC's SE Report (Reference 43) evaluates the vendor's equipment qualification testing against references accepted at the time of the SE Report. Any hardware changes are reflected in a supplemental vendor report, which is referenced in this LAR Framework Document and which demonstrates compliance to the required Equipment Qualification levels for temperature, humidity, seismic, radiation, and electromagnetic compatibility. Compliance to applicable NRC Regulatory Guides that have changed after the submission of the vendor's licensing topical report including RG 1.180, Rev. 2 will be addressed in a supplemental vendor equipment qualification report (Reference 61).

The DAS equipment is evaluated separately below, reflecting its testing to similar environmental stressor levels. As non-safety related but AQ equipment, LGS will evaluate the DAS type test results, to ensure that the equipment will function correctly in the installation environment, cope with the environmental stressors to which it is exposed, and not create an unfavorable environment for safety-related systems or equipment located near the DAS.

All equipment is installed in mild environments, which do not require aging, since no significant aging mechanisms exist (Regulatory Position 1 of RG 1.209).

To demonstrate compliance with GDC 2 and GDC 4 (Reference 59), this section lists the regulatory and plant-specific environmental conditions (i.e., temperature, humidity, radiation, seismic activity, and EMC) expected in the CR and AER. Temperature, humidity, and seismic activity conditions were well-defined when the plant was constructed, so specific requirements exist. Since EMC was not well-defined when LGS was constructed, the type testing conforms to the requirements in RG 1.180, Rev. 2 (Reference 62). The test levels used in type testing the PPS, including the DKTs and other ancillary equipment, are documented. LGS then provides conclusions concerning the acceptability of the equipment based on the requirements provided and the type test results. Part of the LGS evaluation of equipment not already evaluated by the NRC in the SE Report (Reference 43) is an evaluation of the type test program to the environmental qualification requirements in IEEE Std. 323 (Reference 31), as endorsed by RG 1.209 Rev. 0, with updates and clarifications from the International Electrotechnical Commission (IEC) / IEEE 60780/323-2016 (Reference 32). Compliance with the requirements in IEEE Std. 603 Clause 5.4 (Reference 4) and IEEE Std. 7-4.3.2 Clause 5.4 (Reference 5) is contained in these evaluations. The LGS PPS and DAS VOPs (References 63 and 64,

respectively) ensure compliance with the expectations of 10 CFR 50 Appendix B Criterion III (Reference 59) on design controls at the vendor. LGS internal procedures ensure design controls are applied by the licensee and by licensee subcontractors.

4.1 PLANT REQUIREMENTS (DI&C-ISG-06 D.3.1)

The required plant-specific room data is defined in plant calculations as referenced in each section below.

4.1.1 Temperature and Humidity at Each Installed Location

Most of the equipment installed by this LAR Framework Document (e.g., logic solvers, DKT Interfaces, DKT Switches) will be installed in the AER, which is referred to as the Plant Generation Control Center in the M-171 Calculation (Reference 65). The expectation is that any EWS required for the logic solvers will be in the AER. The DKTs will be installed in the CR, with the environmental conditions defined in the M-171 Calculation. Table 4-1 below contains the maximum temperature, humidity range, pressure range, and total integrated gamma dose (TID) for 40 years of operation plus a LOCA. This LAR Framework Document assumes that the heat given off by the powered equipment will maintain these rooms above freezing.

Table 4-1: Environmental Conditions

Room	Maximum Temperature	Humidity Range	Pressure	Total Integrated Gamma Dose
Control Room	78°F	50 to 90% Relative Humidity	+0.25” water gauge	264 Rads TID at 0.5 mR/hr; 271 Rads TID post-LOCA
Auxiliary Equipment Room	82°F	50 to 90% Relative Humidity	Atmospheric	264 Rads TID at 0.5 mR/hr; 277 Rads TID post-LOCA

4.1.2 Radiation Qualification

All modernization equipment will be mounted in the AER and CR. Based on the 40 years and 264 Rads TID and 271 or 277 Rads TID post-LOCA (see Table 4-1 above), the continuous exposure rate is very low. Experience with chronic radiation exposure has shown that modern electronics can survive much larger doses, as long as the dose rate is low. Radiation qualification is thus not required for equipment installed in the CR or AER.

4.1.3 Seismic Spectra and Amplitudes at Each Installed Location

The logic solvers, DKT Interfaces, and DKT Switches will be Seismic I in the AER. The expectation is that any EWS required for the logic solvers will be mounted as Seismic II over I in the AER. The conservative seismic spectra for the equipment located in the AER is provided in

Calculation *TBD*, page *TBD* for an Operating Basis Event (OBE) and page *TBD* for an SSE (Reference 66). The logic solvers will be installed in the AER.

TBD/TBC 24: Exelon to provide the seismic spectra and amplitudes for the AER, where the Analog Trip Units and Relays are installed (Seismic I); the logic solvers, DKT Interfaces, and DKT Switches will be installed, where the Engineering Workstation will be installed (Seismic II over I). These should be both normal conditions and accident conditions. Update Reference 66.

The DKT are installed in the CR, for which spectra are defined in Calculation LS-0192 pages 10 for an OBE and 11 for a SSE (Reference 67).

4.1.4 Electromagnetic and Radio Frequency Interference

TBD/TBC 25: RG 1.181 Rev 2 is the appropriate, especially since the NRC will be reviewing this. Assume that these methods and limits are appropriate for all LGS areas where equipment will be, including logic solvers, remote input and output modules, Engineering Workstation, and Control Room. These should be both normal conditions and accident conditions.

Existing qualifications for the logic solvers will have been performed against one of the revisions of the Electric Power Research Institute (EPRI) TR-102323 or against RG 1.180 Rev. 1. The NRC has published RG 1.180 Rev. 2. The HSI (i.e., DKT Interfaces, DKT Switches, DKTs, EWS) will be qualified to current regulatory requirements. There is no survey specific to these areas in LGS, so the new regulatory guidelines will be applied for the NRC review. The project will apply RG 1.180 Rev. 2 and determine how compliance with this new RG is achieved for the prequalified platform.

4.2 EXISTING PPS PLATFORM EQUIPMENT QUALIFICATION (DI&C-ISG-06 D.3.1)

TBD/TBC 26: Need a selected vendor to complete all of Section 4.2 and provide their licensing topical report, equipment qualification documents, and NRC SE Report for LGS review, along with their response to RG 1.180 Rev. 2.

4.2.1 Base System in the SE Report

This LAR Framework Document section discusses the base equipment qualification methods and limits for the equipment qualified as part of the SE Report, with lists of LARs where the NRC evaluated and accepted later equipment.

4.2.2 Additional Equipment Qualification Performed

This LAR Framework Document section discusses any vendor modules whose hardware has changed between the latest of the SE Report submission or subsequent LAR submittals.

TBD/TBC 27: Section 4.2.3 may require AE or Engineer of Choice input as well.

4.2.3 Additional Interface Hardware

This section discusses the equipment qualification results (temperature, humidity, seismic, EMC) for any new safety-related modules, DKT Interfaces, DKT Switches, DKTs, power supplies, terminations, terminal blocks, test points, knife edge disconnect terminal blocks, and wire that

were not included in the original vendor's licensing topical report (Reference 42) and NRC's SE Report (Reference 43).

4.3 EVALUATION OF PPS PLATFORM EQUIPMENT QUALIFICATION (DI&C-ISG-06 D.3.2)

To comply with the regulatory requirements, each of the sections below addresses the environmental test performed/to be performed on the PPS equipment. Most vendors based their testing on the general criteria provided in EPRI TR-107330 and EPRI TR-102323, including the EMC test guidance. The NRC has changed the electromagnetic tests in the current revision of RG 1.180 (Reference 62), which changes the EMC test levels and endorsed revisions of test requirements documents. The project will need to determine how compliance with RG 1.180 Rev. 2 will be achieved. Radiation exposure is not performed, since radiation exposure in the AER and CR environments are mild environments, and the low chronic doses have been demonstrated to not affect the operation of equipment with current technology circuits.

For the prequalified platform selected, the NRC has already evaluated the test plans, detailed test procedures, and test results. The licensee has considered any changes to the platform and additional testing or analysis performed by the vendor in addition to the existing NRC evaluation of type testing for the platform as defined in the vendor's licensing topical report (Reference 42) and evaluation in the NRC's SE Report (Reference 43). This LAR Framework Document section evaluates the platform testing as a whole against the plant and regulatory requirements.

TBD/TBC 28: Need to compare data (from LGS) in Section 4.1 against the equipment qualification data (from the selected vendor) in Section 4.2, incorporating the results in Section 4.3.

4.3.1 Qualification for Temperature and Humidity at Each Installed Location

This section answers the question: Does the equipment proposed remain operable and qualified within the temperature and humidity limits established for the CR and AER?

Qualification is generally to the EPRI TR-107330 temperature and humidity profiles or within the boundaries achievable in the test chamber.

4.3.2 Qualification for Seismic Conditions at Each Installed Location

This section answers the question: Does the equipment proposed remain operable and qualified within the seismic spectra and amplitude established for the CR and AER?

4.3.3 Qualification for Electromagnetic and Radio Frequency Interference

TBD/TBC 29: Cope with new RG 1.180 Rev. 2 requirements

This section answers the question: Does the equipment proposed remain operable and qualified within the EMC established by the NRC in RG 1.180, Rev. 2?

The use of the generic qualification envelopes for the EMC type tests demonstrate that the PPS operates in the worst-case conditions measured for the operating fleet in the development of EPRI TR-102323 and NRC RG 1.180, Rev. 2 (Reference 62). If surveys have been performed,

include the results from those surveys here to further demonstrate that the test EMC exposures are bounding. The utility notes that short-term surveys only show the measured environment during the survey and are not necessarily reflective of the long-term installation environment.

4.3.4 PPS Equipment Qualification Conclusion

This section answers the question: Based on the data provided above, does the equipment meet the requirements for installation in the AER and CR?

4.4 VIDEO HSI EQUIPMENT QUALIFICATION (DI&C-ISG-06 D.3.1)

4.4.1 Video HSI Commercial Grade Dedication

TBD/TBC 30: Define the commercial grade dedication for the DKT Interfaces, DKT Switches, and DKT including the equipment qualification for the AER and CR

The Video HSI will require commercial grade dedication. If this is the case, this section will point to the report or reports generated by the dedicator to support the conclusion that the dedicated equipment is suitable for use as a basic component. If commercial grade dedication of the Video HSI is not required, delete this section.

4.4.2 Video HSI Type Test for Temperature and Humidity at Installed Locations

This section answers the question: Does the video HSI remain operable and qualified within the temperature and humidity limits established for the CR and AER?

The temperature and humidity testing will be performed using a modified version of the profiles provided in EPRI TR-107330, based on chamber limitations, using the EPRI temperature limits that envelops the plant requirements (see Section 4.1). These indicate that the DKT Interfaces, DKT Switches, and DKTs will function correctly after being exposed to the temperature and humidity extremes expected in the CR.

4.4.3 Video HSI Type Test for Seismic Conditions at Installed Locations

This section answers the question: Does the equipment proposed remain operable and qualified within the seismic spectra and amplitude established for the CR and AER?

The seismic testing performed will be performed against the larger of the seismic qualification curves provided in EPRI TR-107330 and the LGS curves for the installed locations. Testing will be performed for the DKT Interfaces, DKT Switches, and DKTs and demonstrate that the DKT Interfaces, DKT Switches, and DKTs will be operable post-earthquake.

4.4.4 Video HSI Type Test for Electromagnetic and Radio Frequency Interference

This section answers the question: Does the equipment proposed remain operable and qualified within the EMC established by the NRC in RG 1.180, Rev. 2?

The use of the generic qualification envelopes for the EMC type tests demonstrate that the DKT Interfaces, DKT Switches, and DKTs will operate in the worst-case conditions measured for the

operating fleet in the development of NRC RG 1.180, Rev. 2 (Reference 62). If surveys have been performed, include the results from those surveys here to further demonstrate that the test EMC exposures are bounding. The utility notes that short-term surveys only show the measured environment during the survey and are not necessarily reflective of the long-term installation environment.

4.4.5 Video HSI Equipment Qualification Conclusion

This section answers the question: Based on the data provided above, does all equipment comprising the Video HSI meet the requirements for installation in the AER and CR?

4.5 DAS System Equipment Qualification (DI&C-ISG-06 D.3.1)

TBD/TBC 31: Need a selected vendor to complete this section.

In this section, define what equipment qualification is required and expected for the DAS. Recognizing that the DAS is AQ industrial equipment, the DAS is able to survive temperature and humidity exposures in the CR and AER. Recognizing that the DAS is not designed to be hardened nuclear safety-related equipment, seismic exposure may be problematic, especially if Seismic II over I is not sufficient. The DAS equipment is tested for EMC for both emissions and susceptibility, against the same levels used for the PPS.

4.5.1 DAS Type Test for Temperature and Humidity at Each Installed Location

This section answers the question: Does the equipment proposed remain operable and qualified within the temperature and humidity limits established for each plant installation location?

The EPRI temperature and humidity profiles, within the boundaries achievable in the test chamber, envelope the CR and AER. The EPRI profiles were used for successful testing.

4.5.2 DAS Type Test for Seismic Conditions at Each Installed Location

This section answers the question: Does the equipment proposed remain operable and qualified within the seismic spectra and amplitude established for each plant installation location?

TBD/TBC 32: Need to answer the question for regulatory expectations: Does the NRC expect the DAS to be operable post-earthquake?

Depending on LGS requirements: The non-safety related DAS is tested to the seismic conditions in the AER. The DAS meets the criteria for Seismic II over I installation.

4.5.3 DAS Type Test for Electromagnetic and Radio Frequency Interference

This section answers the question: Does the equipment proposed remain operable and qualified within the EMC envelope established by the NRC in RG 1.180, Rev. 2 (Reference 62). The equipment was qualified to either one of the revisions of EPRI TR-102323 or RG 1.180 Rev. 1.

Testing is likely required to validate that the DAS remains operable in the presence of the required susceptibility testing and does not emit in excess of the emissions limits.

4.5.4 DAS Equipment Qualification Conclusion

This section answers the question: Based on the data provided above, does all equipment comprising the DAS meet the requirements for installation in the AER and CR?

5

Digital I&C Systems Development Processes (DI&C-ISG-06 D.4)

TBD/TBC 33: **Section 5 requires vendor input from both the safety related and non-safety related vendors, which the project team will then review. Section 5 will be updated to reflect how the individual vendors work with LGS to incorporate the existing functional requirements into the PPS and DAS systems. Throughout Section 5, the language provided is representative of the expected content that the utility and the selected vendor will incorporate in the completed LAR.**

TBD/TBC 34: **All subsections in Section 5.1 require completion based on the selected PPS vendor. This section documents licensee understanding of the chosen vendor's processes and their applicability to the PPS, as well as committing to vendor oversight to ensure the vendor implements the process. The discussion should include how PPS development, defined in Section 5.1, interacts with Section 9 on SDOE. The discussion should also document plans for resolution of detected errors, including all system lifecycle phases.**

TBD/TBC 35: **All subsections in Section 5.2 require completion based on the selected DAS vendor. This section documents licensee understanding and acceptance of the chosen vendor's processes and their applicability to the DAS, as well as committing to vendor oversight to ensure the vendor implements the process. The discussion should include how DAS development, defined in Section 5.2, interacts with Section 9 on SDOE. The discussion should also document plans for resolution of detected errors, including all system lifecycle phases.**

This LAR Framework Document section is organized as two separate discussions. Section 5.1 is for the PPS platform used to implement the RPS, N4S, and ECCS functions. Section 5.2 is for the non-safety related platform used for DAS. The software work products defined in Sections 5.1 and 5.2 are compliant with the expectations for the software work products defined in the EPRI DEG (Reference 2). LGS will verify through inspections and audits that both the PPS Vendor and the DAS Vendor are designing, developing, implementing, verifying, and validating their application software and systems as well as preparing for PPS and DAS integration in accordance with this section. This LGS verification is performed through the application of the LGS PPS VOP (Reference 63), as described in Section 5.1.16, and the LGS DAS VOP (Reference 64) in Section 5.2.15.

5.1 PPS Overall Design and Development (DI&C-ISG-06 D.4.1)

For the PPS platform and application software processes, the NRC has already evaluated the processes in existence at the time of the vendor's licensing topical report (Reference 42) and evaluation in the NRC's SE Report (Reference 43). This section documents any changes to the platform hardware, software, and software tools and application software processes against the precepts found in RG 1.152 and RGs 1.168–1.173. This section also compares any changes to the application software processes against the requirements in NQA-1:2015 and the EPRI DEG (Reference 2). Any changes to platform hardware, software, or software tools are also discussed in Section 6.1.

LGS staff oversight and evaluation of the implementation of the software processes will focus on the creation and maintenance of application software work products, to include translation of the PPS Functional Requirements (Reference 9) into vendor-specific conformed System Requirements Specification and into the expected work products. The work products produced include Software Requirements Specifications, Software Detailed Designs and Architectures, code implementations, requirements tracing, V&V processes and results, software integration, software and hardware integration, system testing, factory acceptance testing, integration with non-safety related DAS. Validation of any partial PPS installations during the multiple outages and validation of the full integration of the complete PPS and DAS is a utility-specific responsibility.

LGS will ensure that the vendor uses the software tools as documented in the vendor's licensing topical report (Reference 42) and evaluated in the NRC's SE Report (Reference 43). LGS will ensure that the vendor's V&V maintains the independence documented in the vendor's licensing topical report (Reference 42) and evaluated in the NRC's SE Report (Reference 43).

LGS will use normal utility processes to generate, review, and approve the installation design change and commissioning tests.

Section 6.2 discusses the use of the Plant-Specific Action Items (PSAIs) or Application-Specific Action Items (ASAIs) for the system described in this LAR.

5.1.1 PPS System, Software and Hardware Design, and Development Lifecycle (DI&C-ISG-06 D.4.2)

The vendor applies their approved software programming manual or equivalent or the licensee will evaluate the processes and work products the vendor produces for application software. This discussion makes the assumption that all platform software is complete, completely evaluated, and not of sufficient size to require revision of the vendor's licensing topical report for the platform and the NRC's SE Report and that any hardware modifications have been subjected to and passed equipment qualification testing or analysis. Thus, any platform changes can be evaluated by the NRC as part of this LAR.

LGS will inspect the vendor's work, using the vendor's approved software program manual as the basis for software evaluations, as well as evaluating the vendor's technical work products. These two evaluations, along with potential Nuclear QA audits, are part of the basis used in the development of the VOP in Section 5.1.16.

If there is no approved software program manual, LGS will use the precepts in NQA-1, the EPRI DEG (Reference 2), and DI&C-ISG-06 Section D.4 (Reference 1) to guide the oversight and review of the vendor's software activities. This will include documentation on how the vendor meets the intent of the software regulatory guides and how any exceptions and clarifications to those plans meet the underlying regulations.

The PPS Functional Requirements document (Reference 9) is conformed to the capabilities of the vendor platform and software tools.

The vendor documents the partitioning of the system-level requirements for software, requirements for hardware, and expectations for human interactions and decisions. The vendor's software lifecycle process is used to implement the work products, reviews, analyses, and tests expected in a safety related software program, including separate software requirements specifications and software detailed design documents, including architecture for the segmented RPS, N4S, and ECCS functions.

The vendor expands each of the segmented functions to generate the software architecture documentation, software detailed design, software implementation, software reviews, software test plans, software test procedures, software test results, and track resolution of all identified anomalies. CM and change control are integral parts of the vendor's processes for everything that comprises the PPS. SDOE is an integral part of this process, as discussed in Section 9.1.

The vendor verifies and validates all generated products, based on the work performed in the previous phase, which was based on the PPS Functional Requirements document. Each phase is informed by systems and software hazards analyses. The vendor will validate the integrated software and hardware.

The vendor will provide factory acceptance testing that includes interfaces with the video switching, video display units, SOE recording on the non-safety related data network, and data transfers to the non-safety related data network. This testing will include the priority logic. Testing will demonstrate that the RPS, N4S, and ECCS along with the priority logic and the DAS work well together, including the interface with the HSIs, SOE, and the data network. At the successful completion of all testing, the four systems will be shipped to LGS for installation and commissioning.

LGS will work with the vendor and oversee the vendor's work to ensure that the system performs the intended functions and that the vendor works within the vendor's software lifecycle process, program, procedures, and instructions. Any changes in the vendor's software lifecycle during the PPS project will be evaluated and accepted (or rejected) by LGS staff. This oversight will start with the contract signing and continue through installation at LGS. This oversight will restart for each change in the software that requires vendor input.

To help ensure the complete implementation of all requirements and to support V&V, the vendor's design organization establishes and maintains bidirectional requirement traceability within all software work products and from system requirements to functional allocations in software, hardware, and human factors requirements specifications. This process is based on the PPS Functional Requirements document, LGS UFSAR, Technical Specifications, and other design basis documents. Bidirectional traceability starts with the conformed System Requirements and continues through the completion of the integrated testing of the PPS, DAS, and EIM. Bidirectional traceability does not extend into software units, such as software functions or logic sheets. Traceability is not required to the individual line or group of code or function boxes. Traceability will extend to the software unit.

For V&V, the LAR Framework Document includes a discussion of the independence of the team implementing the software tests, for the RPS, N4S, and ECCS. The LAR Framework Document also includes expectations for the V&V staff work products, including expectations for an

acceptable level of detail and acceptance criteria within each vendor- and LGS-produced nuclear quality test procedure.

The PPS is implemented under vendor and LGS plans that provide SDOE, from conceptual design through the plant Operation and Maintenance phase.

All activities are performed under the 10 CFR 50 Appendix B nuclear QA programs of LGS, PPS vendor, and any LGS subcontractors.

The LAR Framework Document documents how and where (i.e., at the vendor, at LGS, at both the vendor and LGS) all work products are documented, reviewed, approved, and each is retained as a quality record.

5.1.2 PPS System Development Activities (DI&C-ISG-06 D.4.2.1)

Example text: No changes are required and none have been implemented from the approved methods documented in the vendor's licensing topical report (Reference 42) and evaluated in the NRC's SE Report (Reference 43).

Example text: The licensee has evaluated the following changes to the vendor's approved platform and/or application software process and accepts each based on the discussion provided with each exception or change.

5.1.3 PPS Application Software Development Activities (DI&C-ISG-06 D.4.2.1)

Example text: No changes are required and none have been implemented from the approved methods documented in the vendor's licensing topical report (Reference 42) and evaluated in the NRC's SE Report (Reference 43).

Example text: The licensee has evaluated the following changes to the vendor's approved platform and/or application software process and accepts each based on the discussion provided with each change.

The LAR Framework Document points to the vendor's licensing topical report (Reference 42) sections that define plant interfaces, system functional requirements, software lifecycle processes, and expected work products. These elements are all part of the LGS PPS VOP (see Section 5.1.16).

Working with the vendor, LGS will determine which underlying standards, including international standards, are part of the vendor's process and the level to which the vendor is compliant.

The lifecycle processes documented in NRC regulatory guidance are designed for traditional software coding, using a procedural language. If the software is designed in function blocks or another of the nonprocedural languages (e.g., IEC 61131-3), the lifecycle processes will have been tailored in the vendor's software programming manual.

5.1.4 PPS Plant and I&C Hazards Analysis (DI&C-ISG-06 D.4.2.1.1)

Hazards analysis methods are used throughout the system, software, and hardware lifecycle processes. Hazards analysis results are used to inform the designs, which result in a modified hazards analysis. Changes made to the designs to resolve hazards are documented, provided to LGS, and retained as quality records, to avoid the potential for future modifications to reintroduce previously eliminated hazards.

The PPS is consistent with the safety analysis (Chapter 15) of the UFSAR (Reference 41). Based on the design of the modification described in this LAR, the safety analysis in LGS UFSAR Chapter 15 is still conservative, bounding, and does not require change.

Rather than documenting a separate criticality analysis for each application software function, all software in the PPS is processed in accordance with the V&V guidance provided in IEEE Std. 1012-2004 (Reference 68), as endorsed by RG 1.168 Rev. 2 (Reference 69), and the reviews and audits guidance provided in IEEE Std. 1028-2008 (Reference 70), as endorsed by RG 1.168 Rev. 2. The application software is treated as software integrity level (SIL) 4, as required by RG 1.168 and defined in IEEE Std. 1012.

Since the software is processed as SIL 4, there is no need for a criticality analysis for the safety related software that is the subject of this LAR. All software in the RPS, N4S, and ECCS is processed to the same SIL levels, since the complexity required to isolate software at lower SIL levels is not included in the design, reducing the overall complexity. Processing all application software to the highest SIL level and using qualified staff for V&V activities makes the detection of software design errors more likely. Verification of the PPS Functional Requirements document by LGS subject matter experts and by the vendor reduces the probability of errors of omission or commission in the functional requirements. V&V activities will reduce the potential for remaining latent software errors, reducing the potential for software common cause failure.

The PPS, DAS, and EIM designs are implemented to minimize the potential for spurious actuation. The PPS design has been assessed for any possible adverse effects of spurious actuations, which verified that the assumptions in the safety analysis are not invalidated. This assessment includes spurious actuations from the PPS, DAS, and EIM. The design was informed and modified as necessary to ensure that spurious PPS, DAS, and EIM actuations do not generate new conditions beyond the existing safety analysis in LGS UFSAR Chapter 15 (Reference 41). The analysis and acceptance criteria in Sections 5.1 and 5.2 are included in the analysis.

5.1.5 PPS System Requirements (DI&C-ISG-06 D.4.2.1.2)

The LGS process provides the expected oversight of the PPS vendors through the LGS PPS VOP as described in Section 5.1.16, including nuclear QA. The VOP covers all vendor lifecycle work associated with the PPS, including the PPS HSI.

This section describes how the PPS Functional Requirements (Reference 9) document was generated and verified. LGS concludes that the PPS Functional Requirements document is a complete and correct definition of the required PPS. The PPS Functional Requirements document has been conformed to the vendor's platform capabilities to generate the PPS System Requirements Specification. Requirements traceability is explained in Section 5.1.1.

Example text: If the vendor's software program manual contains a sufficiently detailed description, then reference the vendor software program manual. Otherwise, this section must define the process, which includes the identification of all work products, the lifecycle activities associated with system requirements, the V&V activities and work products, CM activities including baselines, and change control activities.

This section references Section 3, where the technical elements are discussed.

5.1.6 PPS System Architecture (DI&C-ISG-06 D.4.2.1.3)

This section describes the system architecture, primarily through references to Sections 3.1, 3.2, and 3.3.

This section describes the lifecycle activities associated with architecture development, including the work products that define the architecture; the V&V activities and work products that assure compliance with the PPS Functional Requirements document (Reference 9), LGS UFSAR (Reference 56), and vendor equipment capabilities; and the CM and change control activities.

5.1.7 PPS System Design (DI&C-ISG-06 D.4.2.1.4)

This section describes the work done to ensure that the system design provides the capabilities necessary to implement the PPS Functional Requirements document (Reference 9) and provide the capabilities assumed in the LGS UFSAR (Reference 56), including in the accident analysis (Chapter 15), revisions to the TS (see Sections 8.1and 8.2), and ensuring that the PPS self-test and self-diagnostic capabilities are sufficient to support the technical and licensing discussion (i.e., argument) for deletion of most of the periodic surveillance tests. Platform self-tests and self-diagnostics are evaluated in the FMEDA (Reference 55). This section (1) describes the methods used to ensure the system conforms to the licensing requirements at the system field interfaces and (2) the new licensing requirements for the equipment from the field terminations into the logic solvers, HSIs, SOE interfaces to non-safety related systems, and communication interfaces. The traceability of the system requirements to the system design is explained in Section 5.1.1.

This section describes the methods to be used by the vendor to partition functional requirements between hardware, software, and humans as well as the methods necessary to split allocations that require hardware, software, and/or human elements to implement.

This section describes the lifecycle activities associated with developing the system design, including the work products that define the design; the V&V activities and work products that assure compliance with the PPS Functional Requirements document, LGS UFSAR, and vendor equipment capabilities; and the CM and change control activities.

5.1.8 PPS Software Requirements (DI&C-ISG-06 D.4.2.1.5)

This section consists of the partitioned functional requirements assigned to software, considering the hardware in which the software executes and the humans who operate and maintain the PPS.

Traceability will be provided between the PPS System Requirements and the vendor's PPS Software Requirements that includes functionality, external interfaces, and methods to ensure performance/determinism, correctness, unambiguity, reliability, maintainability, availability, inspectability, and cyber security. The traceability of the software requirements to the system requirements is explained in Section 5.1.1. Review of Software Requirements and traceability as well as the oversight of the vendor's independent V&V are part of the LGS PPS VOP as described in Section 5.1.16.

This section describes the effects of any design constraints imposed on the implementation, including those resulting from language choice, assurance of system integrity, resource limitations, and operating environment.

This section describes the lifecycle activities associated with developing the software requirements, including interfaces with the hardware requirements and any human interface requirements; the work products that define the design; the V&V activities and work products that assure compliance with the PPS Functional Requirements document (Reference 9), LGS UFSAR (Reference 56), and vendor equipment capabilities; and the CM and change control activities.

5.1.9 PPS Software Design (DI&C-ISG-06 D.4.2.1.6)

This section describes the methods to be used by the vendor to design and document the software architecture, based on the software requirements, including software-based requirements for interactions with hardware and humans. This section describes the methods used to ensure that allocations split across hardware, humans, and software can be implemented. The detailed design will describe the function of the software, including inputs, logic within the software units, and outputs. The vendor codes software units based on the materials derived during this phase. The software unit designs are reviewed to define unit testing, which is part of the V&V activity. The software architecture and software detailed units design will be part of the LGS oversight, including the traceability of the architecture and software units design to the software requirements, which is explained in Section 5.1.1. These reviews and oversight of the vendor's independent V&V are part of the LGS PPS VOP as described in Section 5.1.16.

The LAR Framework Document describes the lifecycle activities associated with designing the software, including interfaces with the hardware and any human interface requirements; the work products that define the software design; the V&V activities and work products that assure compliance with the PPS Functional Requirements document (Reference 9), LGS UFSAR (Reference 56), and vendor equipment capabilities; and the CM and change control activities.

The architecture and software detailed design documents the interrelation of software units. Testing plans and procedures are generated to test software units and integrated software units, including tests in the hardware and with the human elements.

The design analyses and V&V demonstrate that the design provides the required functionality, completeness, external interfaces, performance, determinism, correctness, unambiguity, reliability, maintainability, availability, inspectability, and cyber security.

The LAR Framework Document documents how the application software interacts with the platform self-test and diagnostics software, which may be limited to the methods used to annunciate faults and failures and provide details to the non-safety related DCS.

5.1.10 PPS Software Implementation (DI&C-ISG-06 D.4.2.1.7)

This section describes the lifecycle activities associated with implementing, verifying, and validating the software, including interfaces with the hardware and any human interface requirements; the V&V activities and work products that assure compliance with the PPS Functional Requirements document (Reference 9), LGS UFSAR (Reference 56), and vendor equipment capabilities; and the CM and change control activities. These reviews and oversight of the vendor's independent V&V are part of the LGS PPS VOP as described in Section 5.1.16.

This section describes the methods to be used by the vendor to implement the software, based on the software design, including implementing the code for the software-based requirements for human and hardware interactions. Consideration is provided to compliance with RG 1.170 (Reference 71), as tailored for the vendor's software lifecycle processes.

The software design documentation provides traceability into the implementation. The software design provides the names of the functions or logic blocks in which the software design is implemented, providing adequate traceability. The software implements the same inputs, logic within the software units, and outputs defined in the software design. The V&V activity will review and test the software units.

If the vendor's approved software program manual does not documents how the software tools used by the vendor for the application software implementation have been reviewed and approved.

This section documents any unused platform code or application library code for long-term acceptability within the system.

This section documents how unit tests are performed and their results evaluated. V&V and design engineer roles are described and independence assessed. The expectations for retrievable, objective evidence of testing are defined.

This section documents how the V&V activities verify and validate any interactions between application software and the platform's self-test and diagnostics software. The V&V work products are described and expectations for nuclear testing are defined. The V&V process considers IEEE Std. 829 (Reference 72) and documents how this standard is tailored to fit within the vendor's software lifecycle processes.

Review and oversight of these activities as well as the oversight of the vendor's independent V&V are part of the LGS PPS VOP as described in Section 5.1.16.

5.1.11 PPS Software Integration (DI&C-ISG-06 D.4.2.1.8)

This section describes the methods used by the vendor to integrate and test the software units, based on the software design, including any code for the software-based requirements for

interactions with humans and hardware. This phase tests each of the functions by itself, including the RPS, N4S, ECCS, EDG initiation logic, and LDS. The software integration testing assures that the functions and the EIM can be integrated into the PPS.

LGS and the vendor Design and V&V staff ensure that each test demonstrates the required functionality, completeness, external interfaces, performance, determinism, correctness, unambiguity, reliability, maintainability, availability, inspectability, and cyber security. These are included as oversight and reviews in the LGS PPS VOP as described in Section 5.1.16.

The V&V work products are described, including recording and evaluation of test data and content of test reports. The V&V process considers IEEE Std. 829 (Reference 72) and documents how this standard is tailored to fit within the vendor's software lifecycle processes.

Review and oversight of these activities as well as oversight of the vendor's independent V&V are part of the LGS PPS VOP as described in Section 5.1.16.

5.1.12 PPS System Integration

This section describes the methods used by the vendor to integrate and test the software and hardware and HSI, based on the system requirements. This phase tests each of the functions after integration into the PPS, including the RPS, LDS, N4S, EDG initiation logic, and ECCS. The system integration testing is part of V&V and assures that the functions and the EIM can be integrated into the PPS.

This section describe the methods used by LGS and the vendor Design and V&V staff to ensure that each test demonstrates the required functionality, completeness, external interfaces, performance, determinism, correctness, unambiguity, reliability, maintainability, availability, inspectability, and cyber security.

The V&V work products are described, including recording and evaluation of test data and content of test reports. The V&V process considers IEEE Std. 829 and documents how this standard is tailored to fit within the vendor's software lifecycle processes.

Review and oversight of these activities as well as the oversight of the vendor's independent V&V are part of the LGS PPS VOP as described in Section 5.1.16.

5.1.13 PPS System Testing (DI&C-ISG-06 D.4.2.1.9)

The testing is based on validating the integrated PPS, priority logic (e.g., equipment interface modules), and human-system interfaces. All testing results are reviewed by LGS as part of the LGS PPS VOP as described in Section 5.1.16.

Example: The LAR Framework Document describes how the testing is based on the successful completion of software unit and software integration testing as well as all V&V for each of the individual functions. Using the system test plan developed earlier, the V&V team demonstrates that the system implementation is correct. This includes an evaluation of normal and off-normal conditions as well as performing the remaining surveillance test and calibration checks.

The Factory Acceptance Testing (FAT) is performed based on detailed procedures generated and reviewed by the vendor, reviewed by LGS, comments incorporated by the vendor, and approved by LGS. The FAT validates the correct operation of all PPS functions, from input to output (including the EIM's priority logic), all HSIs both as displays and soft controls, and the provision of data to the DCS. Outputs are to be loaded as expected when installed in the plant.

This testing validates the worst-case timing analyses for time-critical PPS input to output propagation delays. Worst-case timing from the channel inputs to the division outputs requires no more than the time allocated in the PPS Functional Requirements document (Reference 9) to scan inputs, solve logic, and output a scram or actuate signal to the field. The worst-case timing considers plant conditions that change just after being sampled and the worst-case non-synchronized tasks and communication that result in the maximum possible time between the plant condition input and the PPS output.

Timing for the RPS, N4S, and ECCS functions is validated using automated means, over a sufficient period to demonstrate the effects of non-synchronized cyclic behavior for channels and divisions. This section describes the automated test setup to generate the histogram of time delays through the system and provides a conclusion concerning LGS's acceptance of the variability as still maintaining acceptable deterministic behavior.

Starting testing requires that all identified errors have been corrected, which is confirmed by the LGS PPS VOP as described in Section 5.1.16. The tests validate all functions, hardware, software, and HSI, including interfaces to SOE and data historians in non-safety related systems.

This section documents how these system tests are performed and their results evaluated by the vendor's V&V and design engineer staff as well as by the LGS Oversight, QA, Operations, Maintenance, and technical engineering.

The test plans and detailed test procedures validate, to the extent practicable, that identified hazards have been eliminated or at least mitigated. If validation is not practical, the documented verification is included in the test documentation.

5.1.14 PPS and DAS System Integration and Testing

The location, roles, and responsibilities for PPS, DAS, and EIM integrated testing are defined in this section. The location of the test is defined. This section documents LGS's clearly established expectation of vendor responsibility for the integrated system with the safety related system vendor.

This testing is primarily focused on the validation of the operation of the EIM with both the PPS and the DAS. This requires testing of at least most of the functions in the PPS and testing all DAS functions.

The same expectations and processes used for testing the RPS, N4S, and ECCS functions in Section 5.1.13 are designed, reviewed, approved, performed, and results reviewed and approved for the integrated set of PPS, DAS, and priority logic. All testing are test results are reviewed by LGS as part of the LGS PPS VOP as described in Section 5.1.16.

5.1.15 PPS Project Management (DI&C-ISG-06 D.4.2.2)

The LGS Project Plan (Reference 73) defines the project's organization, planning, execution, monitoring, control, and closure activities for the entire project. The LGS Project Plan, in concert with the LGS PPS VOP as described in Section 5.1.16, meet the quality requirements of IEEE Std. 603-1991 (Reference 4) Clause 5.3 with additional guidance from IEEE Std. 7-4.3.2-2003 (Reference 5) Clause 5.3.

The licensee has evaluated the vendor's project management plans and processes and concludes that the vendor's plans and processes are sufficient to produce the PPS and EIM compliant to LGS's requirements.

LGS's PM will maintain a project risk register for the portions of the project under direct LGS control. LGS will require the vendor and engineer of choice to create their own project risk registers. The vendor and engineer of choice risk registers are expected to include both project and technical risks. LGS's vendor oversight will evaluate these risk registers and use their content to redirect the oversight efforts and other risk mitigation strategies as necessary.

While the vendor is implementing software, the LGS expectation for the vendor PM is that many, more manageable size software milestones (i.e., short duration milestones in comparison to tracking overall completion at large milestones) will be included in the controlled schedule for LGS review with vendor tracking and appropriate corrections made by the vendor to ensure schedule compliance, without adverse effects on quality, reliability, availability, or vendor V&V.

LGS will maintain vendor oversight to ensure that the vendor and engineer of choice progress is maintained and progress reported. LGS will apply their normal Exelon PM practices under the Exelon Nuclear QA program. LGS has developed and will maintain a detailed, resource-loaded schedule to track vendor, engineer of choice, and LGS progress towards project completion.

5.1.16 PPS Vendor Oversight Plan (DI&C-ISG-06 C.2.2)

This section summarizes the licensee's PPS VOP. The summary in this section describes (1) how the licensee oversees the vendor's work to ensure compliance with the expectations in the LAR Framework Document and (2) ensures that the vendor develops application software in accordance with regulatory and licensee expectations and the vendor's prequalified software program manual. The PPS VOP describes the intended ongoing interactions with the vendor, to include LGS's performance of technical inspections, software lifecycle process inspections, and appropriate nuclear QA audits of the vendor and appropriate vendor subcontractors throughout the duration of the project. The PPS VOP describes the technical, process, and licensing interactions between the vendor and the licensee. The PPS VOP addresses interactions between LGS and vendor organizations for design, V&V, system integration, testing, QA, and others as required and appropriate.

Application of the LGS PPS VOP ensures that the vendor generates a PPS and EIM compliant with the boundaries set by the vendor's licensing topical report (Reference 42) and NRC's SE Report (Reference 43), as referenced in the VOP. The LGS PPS VOP also helps ensure that the PPS meets LGS's expectations and requirements as established in the conformed PPS Functional Requirements document (Reference 9). The LGS PPS VOP includes verification that

the project and system incorporate the applicable PSAI or ASAI and ensure the generation and retention of documentation explaining, for each PSAI or ASAI, why the implementation is acceptable or justification for why the PSAI or ASAI is not applicable.

The LGS PPS VOP will evaluate the vendor's and the engineer of choice's schedule compliance and ensure that project risks are minimized.

Application of the PPS VOP ensures that the project operates within the licensee's regulatory commitments, as augmented by any regulatory commitments added by the NRC's SE Report for this modernization.

5.1.17 PPS Software Quality Assurance Processes (DI&C-ISG-06 D.4.2.3)

The licensee has accepted the vendor's Nuclear QA program through an audit performed by the Nuclear Procurement Issues Corporation (NUPIC) or an audit performed by the utility. Any changes to the vendor's Nuclear QA program during the project will be evaluated by Exelon Nuclear QA for acceptance.

The vendor's V&V team is considered part of the vendor's QA process, in that the vendor V&V team is reviewing and testing the work products from the vendor application software design team, to ensure that the vendor's quality plans, processes, and procedures are being implemented correctly.

Final oversight of the whole vendor quality program, which includes oversight of the application software QA program, is the responsibility of the vendor's Nuclear QA program. LGS will provide periodic oversight of the vendor's NQA-compliant Nuclear QA program through the LGS PPS VOP (Reference 63).

The LGS PPS VOP includes the involvement of the LGS Nuclear QA group to audit vendor compliance with their own nuclear quality plans, processes, procedures, and instructions.

The LGS PPS VOP includes the evaluation of any software or hardware modifications made to the platform, including the same oversight by the vendor V&V team, the vendor's Nuclear QA program, the LGS Vendor Oversight Group, the LGS design engineering staff, and the LGS Nuclear QA staff.

5.1.18 PPS Software Verification and Validation Processes (DI&C-ISG-06 D.4.2.4)

Example: No changes are required from the approved methods documented in the vendor's licensing topical report (Reference 42) and approved in the NRC's SE Report (Reference 43). More likely statement: LGS has evaluated the following changes to the vendor's approved platform and/or application software process and accepts each based on the discussion provided with each change.

LGS's VOP will verify that the vendor is following the plans, procedures, processes, and instructions defined and accepted in the vendor's software program manual, as approved by the NRC or, using the precepts found in BTP 7-14 and IEEE Std. 1012, as endorsed by RG 1.168, as tailored to the vendor's system. A key feature of this review is verifying that the vendor is

tracking anomalies through the implementation and appropriate retesting to closure through an appropriate task iteration policy.

The vendor V&V team reviews and tests the work products from the vendor application software design team, to ensure that the vendor's quality plans, processes, and procedures are being implemented correctly. LGS will verify that the completed test procedures and test reports (if produced) are of sufficient nuclear quality.

Cyber security and SDOE and the methods used by V&V to ensure that cyber security and SDOE are appropriately included in the design, development, implementation, review, and test are discussed in Section 9.

5.1.19 PPS System Verification and Validation Processes

LGS has evaluated the vendor's system V&V process against the recommendations in the EPRI DEG (Reference 2) and accepts the process based on the discussion provided in this section.

The discussion is similar to the content of the software V&V LAR Framework Document section, except including hardware, system integration, and the HFE program, all of which are considered in the software process, but evaluated for their impact on the PPS and EIM.

5.1.20 PPS Configuration Management and Change Control (DI&C-ISG-06 D.4.2.5)

This section is based on one of two of the following considerations, which will be explained in this section:

1. There are no changes from the approved methods documented in the vendor's licensing topical report (Reference 42) and approved in the NRC's SE Report (Reference 43).

2. It more likely that this section will say: The licensee has evaluated the following changes to the vendor's approved process and accepts each based on the discussion provided with each change.

The vendor's approved software plans, procedures, instructions, and methods are used to generate the software, in compliance with the intent of NUREG-0800 BTP 7-14. LGS has mapped the vendor's processes to the LGS process and accepts that the LGS system and software requirements are fulfilled.

The normal LGS plans, procedures, processes, and instructions are used to control the overall modification and to establish, maintain, and control any changes to the system configuration after the system is delivered to LGS. Through the PPS VOP, LGS verifies that the vendor CM processes ensure that the final design and implementation supports the performance of periodic surveillance and maintenance in accordance with TS requirements and will support specific plant operating procedures.

Prior to delivery to LGS, the vendor's change control and CM processes are used. LGS's non-safety related VOP verifies that changes are controlled and that configuration is managed appropriately, including baselines, backups (with demonstrated ability to use the backups to

restore when necessary), dual dispersed storage of backups, retention of completed anomaly reports, regression testing of changes, and controlled introduction of changes into the system.

LGS will work with their engineer of choice and vendor to control and manage changes to the PPS Functional Requirements document and other system documentation.

The overall process is based on IEEE Std. 828 as endorsed by RG 1.169 and tailored as documented in this LAR Framework Document (or in the vendor's approved software program manual) needed for the technology being applied.

5.2 DAS DESIGN AND DEVELOPMENT (DI&C-ISG-06 D.4.1)

The content of this section is all new, and based on a graded AQ software process, which LGS has evaluated as appropriate. This section provides the LGS definition of AQ as applied to the DAS functions, including the ATWS. A full safety related software program compliant to BTP 7-14 is not required.

DAS requirements are based on the DAS Functional Requirements document (Reference 58), as conformed.

The AQ process includes the precepts of a good software engineering process designed to minimize design errors. This includes documenting the overall functional design, architecture, detailed software architecture and design (including inputs, processing, and outputs), requirements traceability, peer review by someone other than the person who designed the element being reviewed, and similar independence for the person who designed and performed testing, along with review of test results.

LGS will ensure that the vendor has a documented evaluation of the DCS software tools as being appropriate for use and will evaluate the methods the vendor used to make that determination. LGS will ensure that the staff performing V&V activities are independent of the design staff and did not make any design decisions that defined the design or implementation. The minimum expectations for V&V staff are that the staff are capable of doing the design.

For the DAS, including the ATWS functions, a full description of the processes is required, based on DI&C-ISG-06 Section D.4.1. This section documents compliance with RG 1.173 (Reference 75) on lifecycle models.

TBD/TBC 36: New Decision: LGS to document their definition of augmented quality in Section 5.2

This section (Section 5.2) documents and defines LGS's evaluation of the DAS application software processes as a graded approach, using the intent of the software lifecycle precepts found in RG 1.152 and RGs 1.168 through 1.173 for safety related systems. This section will also compare the project to the precepts in the EPRI DEG (Reference 2). As a commercial platform in significant usage in nuclear power plants, LGS has determined that no further evaluation of the DCS platform and software tools is required.

LGS will evaluate the DAS implementation to ensure compliance with installation requirements (e.g., seismic mounting).

LGS's evaluation will focus on the creation and maintenance of application software work products, including Software Requirements Specifications, Software Detailed Designs, Software Architecture, code implementation, requirements tracing, V&V processes and results, software integration, software and hardware integration, system testing, FAT, integration with safety related systems, and validation of the PPS and DAS integration prior to installation in the plant. LGS will use normal utility processes to generate installation and commissioning tests.

5.2.1 DAS System, Software, and Hardware Design and Development Lifecycle (DI&C-ISG-06 D.4.2)

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.1 above for the PPS. The vendor will apply AQ equivalent system precepts to all phases of the DAS design and development lifecycle, similar to those performed for the PPS above. The system process will include the interface with the EIM.

5.2.2 DAS System Development Activities (DI&C-ISG-06 D.4.2.1)

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.2 above for the PPS. The basic functional requirements are documented by LGS and provided to the vendor for assessment, conformance, design, development, implementation, and V&V using the precepts of the augmented (industrial) QA program, which augments the vendor's existing software lifecycle, as approved by LGS. The vendor's activities are limited to determining how to map and augment the LGS DAS requirements to fit the vendor's hardware and software, with LGS oversight and review.

5.2.3 DAS Application Software Development Activities (DI&C-ISG-06 D.4.2.1)

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.3 above for the PPS. The vendor will apply AQ equivalent system precepts to DAS application software development as were performed for the PPS above.

5.2.4 DAS Plant and I&C System Hazards Analysis (DI&C-ISG-06 D.4.2.1.1)

This section documents the consistency of the DAS with the safety analysis (Chapter 15) documented in the LGS UFSAR (Reference 41), including interoperability with the PPS and EIM. Based on the design of the change described in this LAR, changes are not necessary to the safety analysis in Chapter 15 of the LGS UFSAR. However, changes are necessary in the LGS UFSAR description of and name for the RRCS, including the deletion of the feedwater runback function.

This section documents the AQ expectations for this portion of the overall NSR DAS lifecycle, similar to the SR process described in Section 5.1.4 for the PPS. The vendor will apply AQ equivalent system precepts to DAS hazards analysis through all phases of the DAS design and development lifecycle similar to those performed for the PPS above. The system process will include the interface with the EIM.

5.2.5 DAS System Requirements (DI&C-ISG-06 D.4.2.1.2)

This section documents the consistency of the DAS with the system requirements provided for the ATWS and appropriate portions of the N4S and ECCS, including interoperability with the PPS and EIM. Based on the design of the change described in this LAR, changes are not necessary to the safety analysis in Chapter 15 of the LGS UFSAR. However, changes are necessary in the LGS UFSAR description of and name for the RRCS, including the deletion of the feedwater pump runback function.

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.5 above for the PPS. The vendor will apply AQ equivalent system precepts to generation of the DAS system requirements, based on the architecture documented in the LAR Framework Document and DAS functional requirements, as were performed for the PPS above. The system requirements will include the interface with the EIM.

5.2.6 DAS System Architecture (DI&C-ISG-06 D.4.2.1.3)

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.6 above for the PPS. The vendor will apply AQ equivalent system precepts to the design of the DAS system architecture, based on the architecture documented in the LAR Framework Document and DAS functional requirements, as were performed for the PPS above. The architecture includes the interface with the EIM.

5.2.7 DAS System Design (DI&C-ISG-06 D.4.2.1.4)

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.7 above for the PPS. The vendor will apply AQ equivalent system design processes to the DAS system, based on the architecture documented in the LAR Framework Document and DAS functional requirements, as were performed for the PPS above. The system design description in this section includes the interface with the EIM.

5.2.8 DAS Software Requirements (DI&C-ISG-06 D.4.2.1.5)

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.8 above for the PPS. The vendor will apply AQ equivalent software requirements processes to the DAS software, based on the DAS system requirements, as were performed for the PPS above.

5.2.9 DAS Software Design (DI&C-ISG-06 D.4.2.1.6)

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.9 above for the PPS. The vendor will apply AQ equivalent software design processes to the DAS software as were performed for the PPS above.

5.2.10 DAS Software Implementation (DI&C-ISG-06 D.4.2.1.7)

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.10 above for the PPS. The vendor will apply AQ equivalent code implementation processes to the DAS software as were performed for the PPS above.

5.2.11 DAS Software Integration (DI&C-ISG-06 D.4.2.1.8)

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.11 above for the PPS. The vendor will apply AQ equivalent integration processes to the integration and testing of DAS software as were performed for the PPS above.

5.2.12 DAS System Integration

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.12 above for the PPS. The vendor will apply AQ equivalent integration processes to the DAS software, hardware, and system as were performed for the PPS above.

5.2.13 DAS System Testing (DI&C-ISG-06 D.4.2.1.9)

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.13 above for the PPS. The vendor will define and apply equivalent testing practices to the DAS as is performed for the PPS above.

The integrated testing for the PPS and DAS is described above in Section 5.1.14.

5.2.14 DAS Project Management (DI&C-ISG-06 Section D.4.2.2)

This section documents the AQ expectations for this portion of the overall DAS lifecycle, similar to that described in Section 5.1.15 above for the PPS. The LGS Project Plan (Reference 73) defines the project's organization, planning, execution, monitoring, control, and closure activities for the entire project. The LGS Project Plan, in concert with the LGS PPS VOP, as described in Section 5.1.16, meets the quality requirements of IEEE Std. 603-1991 (Reference 4) Clause 5.3 with additional guidance from IEEE Std. 7-4.3.2-2003 (Reference 5) Clause 5.3. The LGS Project Plan summarizes the LGS definition of the minimum acceptable aspects of AQ.

The licensee has evaluated the vendor's project management plans and processes and concluded that the vendor's plans and processes are sufficient to produce the PPS and EIM compliant to LGS's requirements.

LGS's PM will maintain a project risk register for the portions of the project under direct LGS control. LGS will require the vendor and engineer of choice to create their own project risk registers. The vendor and engineer of choice risk registers are expected to include both project and technical risks. LGS's vendor oversight will evaluate these risk registers and use their content to redirect the oversight efforts and other risk mitigation strategies as necessary.

5.2.15 DAS Vendor Oversight (DI&C-ISG-06 Section C.2.2)

This section summarizes the licensee's non-safety related LGS DAS VOP (Reference 58). This section documents the expectations for the DAS, similar to that described in Section 5.1.16, for AQ.

5.2.16 DAS Software Quality Assurance Processes (DI&C-ISG-06 Section D.4.2.3)

This section documents the expectations for QA for an AQ system, similar to but relaxed from that described in Section 5.1.17.

5.2.17 DAS Software Verification and Validation Processes (DI&C-ISG-06 Section D.4.2.4)

This section documents the expectations for this portion of the overall lifecycle, similar to that described in Section 5.1.18, for AQ.

5.2.18 DAS System Verification and Validation Processes

The discussion is similar to the content of the software V&V in Section 5.1.19, except for including the hardware, system integration, and the HFE program applicable to the DAS, all of which are considered in the software process but evaluated for their potential impact on the DAS and EIM.

5.2.19 DAS Configuration Management and Change Control Processes (DI&C-ISG-06 Section D.4.2.5)

This section documents the expectations for this portion of the overall lifecycle, similar to that described in Section 5.1.20, for AQ.

6

Applying the Referenced SE Report to the PPS (DI&C-ISG-06 D.5)

TBD/TBC 37: Section 6 requires vendor input from the selected safety related PPS vendor, which the project team will then review. Section 5 documents any platform changes made since the last documented NRC acceptance, through a SE Report on a Licensing Topical Report or on a License Amendment request. Throughout Section 6, the language provided is representative of the expected content that the utility and the selected vendor will incorporate in the completed LAR.

TBD/TBC 38: All subsections in Section 6.1 require completion based on the selected PPS vendor and the selected platform. This section demonstrates the licensee understanding of the vendor platform and the vendor changes made to that platform since the last SE Report. This section also ties hardware changes to equipment qualification activities in Section 4.3. Some or all of the platform changes could be resolved in a Licensing Topical Report, if such a report is generated for the modification, in which case, reference to the Licensing Topical Report would be provided, rather than a discussion here. Further, this discussion could be incorporated in the SDOE discussion in Section 9.1.

TBD/TBC 39: All subsections in Section 6.2 provide LGS-specific resolutions to each of the PSAI/ASAI provided in the NRC SE Report that accepted the PPS vendors topical report, including consideration of any additional evaluation of these PSAI/ASAI to resolve platform changes. A subsection will be added for each of the PSAI/ASAI.

This section applies only to the vendor platform used for the PPS. This section does not apply to the DAS.

6.1 PLATFORM CHANGES (DI&C-ISG-06 SECTION D.5.1.1)

6.1.1 Platform Hardware Changes

This section references the vendor's licensing topical report (Reference 42) or LAR where the last evaluation or evaluations were performed on any changed or new hardware not evaluated in the NRC's SE Report (Reference 43). The vendor documents each hardware change since the last time the NRC approved the platform or accepted revisions. The vendor documents how each change was designed, developed, verified, validated, and tested, including how each change has been subjected to, and passed, equipment qualification type testing. Any changes that have the potential to affect the NRC's SE Report are supported by the information and justification provided in this section. It may be possible to argue that some hardware changes are below the level of the architecture required in a LAR and can thus be omitted from this section, as long as those hardware changes have undergone equipment qualification, the changes are incorporated in the failure modes, effects, and diagnostics analyses, and the vendor has documented the changes and the rationale for each change.

6.1.2 Platform Software Changes

This section references the vendor's licensing topical report (Reference 42) or LAR where the last evaluation or evaluations were performed on any changed or new software that was not evaluated in the NRC's SE Report (Reference 43). The vendor documents each change since the last time the NRC approved the platform or accepted revisions. This section should state that the changes were made under the vendor's nuclear QA program, using the vendor's approved processes, if such is the case. Then, the vendor will have documentation that reflects the design, development, verification, validation, and testing, including how each change has been subjected to, and passed, equipment qualification type testing. Any changes that have the potential to affect the NRC's SE Report are supported by the information and justification provided in this section.

6.1.3 Platform Software Lifecycle Process Changes

This section references the vendor's licensing topical report (Reference 42) or LAR where the last evaluation or evaluations were performed on any changed or new platform software lifecycle process that were not evaluated in the NRC's SE Report (Reference 43). The vendor documents each change since the last time the NRC approved the platform or accepted revisions. The vendor documents how each change has the potential to affect the conclusions in the NRC SE Report. Any changes that have the potential to affect the NRC's SE Report are supported by the information and justification provided in this section.

6.1.4 Application Software Lifecycle Process Changes

This section references the vendor's licensing topical report (Reference 42) or LAR where the last evaluation or evaluations were performed on any changed or new application software lifecycle process that were not evaluated in the NRC's SE Report (Reference 43). The vendor documents each change since the last time the NRC approved the platform or accepted revisions. The vendor documents how each change has the potential to affect the conclusions in the NRC's SE Report. Any changes that have the potential to affect the NRC's SE Report are supported by the information and justification provided in this section.

6.1.5 Platform Software Tool Changes

This section evaluates any changes made to software tools since the approval of the vendor's licensing topical report (Reference 42). This section references the vendor's existing topical report or the LAR where the last evaluation or evaluations were performed on any changed, revised, or new software tools used for the platform or application software that were not evaluated in the NRC's SE Report (Reference 43). The vendor documents each change since the last time the NRC approved the platform or accepted revisions. The vendor documents how each change has the potential to affect the conclusions in the NRC's SE Report. Any changes that have the potential to affect the NRC's SE Report are supported by the information and justification provided in this section.

6.2 Resolutions and Applicability of Plant-Specific Action Items or Application-Specific Action Items (DI&C-ISG-06 Section D.5.1.2)

This section describes the methods LGS will use to ensure that all PSAI or ASAI are implemented appropriately, including the use of third-party reviews. Some or all of the PSAI or ASAI could be resolved in a Licensing Topical Report, if such a report is generated for the modification, in which case, reference to the Licensing Topical Report would be provided, rather than a discussion here. This section describes how the VOP (Section 5.1.15) is used to verify vendor compliance with the PSAI or ASAI, which includes verification of the software lifecycle activities as part of the VOP.

This section justifies the rationale behind deciding that a PSAI or ASAI is not applicable to the RPS, N4S, or ECCS functions, documenting why the item does not apply.

6.2.1 PSAI or ASAI 1-n

For each PSAI or ASAI in the selected vendor's licensing topical report (Reference 42) and NRC's SE Report (Reference 43), provide a subsection here that identifies and dispositions the complete PSAI or ASAI for each PSAI or ASAI. For each PSAI or ASAI, summarize how the PSAI or ASAI will be resolved or why the PSAI or ASAI does not apply.

TBD/TBC 40: Section 6.2.x requires the SE input, listing all PSAI, then resolving or justifying why the PSAI does not apply.

7

PPS Compliance with IEEE Stds. 603 and 7-4.3.2 (DI&C-ISG-06 D.6)

TBD/TBC 41: During development of the complete LAR, the contents of the Table 7-1 will be updated to demonstrate compliance and to provide reference to the documented evaluation of the project compliance to these two IEEE standards.

As discussed in Section 3.1.1, the portion of the system that includes digital content complies with current regulatory guidance and consensus IEEE standards. Currently, IEEE Std. 603-1991 (Reference 4) is incorporated into 10 CFR 50.55a. IEEE Std. 603 is the basis for safety related systems in nuclear power plants. IEEE Std. 7-4.3.2-2003 (Reference 5) is the daughter standard to IEEE Std. 603, which provides the required digital augmentation and interpretation to implement the technology-neutral requirements of IEEE Std. 603. IEEE Std. 7-4.3.2-2003 is endorsed in RG 1.152. This LAR Framework Document complies with IEEE Std. 7-4.3.2-2003, as endorsed in RG 1.152, Rev. 3.

Table 7-1 below provides traceability between the IEEE clauses and the sections that show compliance with each clause. There are several IEEE Std. 603 clauses where there is no additional material provided by IEEE Std. 7-4.3.2, which are indicated with an asterisk (*) in the IEEE Std. 7-4.3.2 column in the table.

In the "Compliance" column, each cell states whether the complete LAR submittal complies, partially complies, takes an exception, or does not apply (N/A) for each clause and extended clause in that row. In order for the clause to not apply, either the IEEE standard clause has no requirements, or the requirements in the clause require compliance with each of the subclauses beneath that clause. For each row, the completed LAR demonstrates one of the following:

1. How full compliance/conformance is achieved;

2. Why partial compliance/conformance is acceptable and why full compliance to IEEE Std. 603-1991 is not required in accordance with 10 CFR 50.55a(z), or why deviation from IEEE Std. 7-4.3.2 is acceptable; or

3. Why the alternative exception proposed is acceptable.

The "LAR Section" column currently provides the LAR Framework Document section number or numbers where the IEEE standard requirement is discussed, which will be updated to reflect the section number in the completed LAR. The "DI&C-ISG-06 Section" column refers to the ISG section that discusses the review guidance for that clause for the AR process.

Table 7-1: IEEE Standards 603-1991 and 7-4.3.2-2003 Mapping					
IEEE Std. 603 Clause	**IEEE Std. 7-4.3.2 Clause**	**Title**	**Compliance**	**LAR Section**	**DI&C-ISG-06 Section**
4.1	4*	Safety System Design Basis	Comply	3.5	D.2.3.1, D.3
4.2			Comply	3.5	D.2.3.1
4.3			Comply	3.5	D.2.3.1
4.4			Comply	3.5	D.2.3.1
4.5			Comply	3.5, 3.7.1	D.2.3.1, D.3
4.6			Comply	3.5	D.2.3.1
4.7			Comply	3.5, 4.3, 4.5, 4.7	D.2.3.1, D.3
4.8			Comply	3.5	D.2.3.1
4.9			Comply	3.5	D.2.3.1
4.10			Comply	3.5, 3.1.6	D.2.3.1
4.11			Comply	3.5	D.2.3.1
4.12			Comply	3.5	D.2.3.1
5.1	5.1*	Single-Failure Criterion	Comply	3.5	D.2.6.2.1.1
5.2	5.2*	Completion of Protective Action	Comply	3.5	D.2.3.1, D.2.6.2.3.1
5.3	5.3	Quality	Comply	5.1, 5.2	D.2.3.1, D2.3.3.1, D.3, D.4
	5.3.1	Software Development	Comply	5.1.1, 5.2.2	D.4
	5.3.1.1	Software Quality Metrics	Comply	5.1, 5.2	D.4
	5.3.2	Software Tools	Comply	5.1, 5.2	D.4
	5.3.3	Verification and Validation	Comply	5.1, 5.1.18, 5.1.19, 5.2, 5.2.18, 5.2.19	D.4
	5.3.4	Independent V&V Requirements	Comply	5.1, 5.1.18, 5.1.19, 5.2, 5.2.18, 5.2.19	D.4
	5.3.5	Software Configuration Management	Comply	5.1.20, 5.2.20, 6.1	D.4
	5.3.6	Software Project Risk Management	Comply	5.1.15, 5.2.15	D.4
5.4	5.4	Equipment Qualification	Comply	4	D.2.3.3.1, D.3.1
	5.4.1	Computer System Testing	Comply	5.1.13, 5.1.14, 6.1.13,6.1.14	D.3.1
	5.4.2	Qualification of Existing Commercial Computers	Comply	4.2, 4.4.1	D.3

Table 7-1: IEEE Standards 603-1991 and 7-4.3.2-2003 Mapping					
IEEE Std. 603 Clause	**IEEE Std. 7-4.3.2 Clause**	**Title**	**Compliance**	**LAR Section**	**DI&C-ISG-06 Section**
5.5	5.5	System Integrity	Comply	5.5	D.2.3.1, D.2.6.2.3.1
	5.5.1	Design for Computer Integrity	Comply	3.5	D.2.6.2.3.1
	5.5.2	Design for Test and Calibration	Comply	3.4	D.2.3.1
	5.5.3	Fault Detection and Self-Diagnostics	Comply	3.4	D.2.2.1
5.6	5.6	Independence	Comply	3.8.1	D.2.6.2.2.1
5.6.1		Between Redundant Portions of a Safety System	Comply	3.1.2, 3.9.2	D.2.5.1
5.6.2		Between Safety Systems and Effects of Design-Basis Event	Comply	3.5	D.2.5.1
5.6.3		Between Safety Systems and Other Systems	Comply	2.3, 3.8, 3.9.2	D.2.5.1
5.6.4		Detailed Criteria	Comply	3.9.2	D.2.5.1
5.7	5.7*	Capability for Testing and Calibration	Comply	3.4	D.2.3.1
5.8	5.8*	Information Displays	N/A	N/A	D.2.3.1
5.8.1		Displays for Manually Controlled Actions	Comply	3.1.2	D.2.2.1
5.8.2		System Status Indication	Comply	3.1, 3.4	D.2.2.1
5.8.3		Indication of Bypasses	Comply	3.1, 3.4	D.2.2.1
5.8.4		Location	Comply	3.1, 3.4	D.2.2.1
5.9	5.9*	Control of Access	Comply	3.5.1, 3.8.1.8, 9.1.9	D.2.3.1 D.8
5.10	5.10*	Repair	Comply	3.2.2, 3.6	D.2.3.1
5.11	5.11	Identification	Comply	3.9.2.1, 5.1.5	D.2.6.2.2.1
5.12	5.12*	Auxiliary Features	Comply	3.8.1	D.2.5.1
5.13	5.13*	Multiunit Stations	Comply	2.1	D.2.5.1
5.14	5.14*	Human Factors Considerations[8]	Comply	3.4	D.2.5.1

[8] In this revision of the LAR, Human Factors Engineering is only minimally addressed. Specialist engineers for HFE must be engaged, and the HFE Sections of this LAR must be generated.

Table 7-1: IEEE Standards 603-1991 and 7-4.3.2-2003 Mapping					
IEEE Std. 603 Clause	**IEEE Std. 7-4.3.2 Clause**	**Title**	**Compliance**	**LAR Section**	**DI&C-ISG-06 Section**
5.15	5.15	Reliability	Comply	3.9.3, 5.1.13, 5.1.14, 6.1.13, 6.1.14	D.2.6.2.1.1
6.1	6*	Automatic Control	Comply	3.1, 3.4	D.2.6.2.3.1
6.2		Manual Control	Comply	3.1, 3.4	D.2.6.2.3.1
6.3		Interaction between the Sense and Command Features and Other Systems	N/A	N/A	D.2.6.2.2.1
6.3.1		Requirements	Comply	3.9.4	D.2.6.2.2.1
6.3.2		Provisions	Comply	3.9.5	D.2.6.2.2.1
6.4		Derivation of System Inputs	Comply	3.1.2, 3.9.5	D.2.3.1 D.2.6.2.5.1
6.5		Capability for Testing and Calibration	N/A	N/A	D.2.3.1
6.5.1		Checking the Operational Availability	Comply	3.1.7, 3.4.1	D.2.3.1
6.5.2		Assuring the Operational Availability	Comply	3.1.7, 3.4.2	D.2.3.1
6.6		Operating Bypasses	Comply	3.5.1	D.2.3.1
6.7		Maintenance Bypass	Comply	3.5.1	D.2.3.1, D.2.6.2.1.1
6.8		Setpoints	Comply	3.5	D.2.3.1, D.7.1
7.1	7*	Automatic Control	Comply	3.1, 3.4	D.2.6.2.3.1
7.2		Manual Control	Comply	3.1, 3.4	D.2.6.2.3.1
7.3		Completion of Protective Action	Comply	3.5	D.2.3.1
7.4		Operating Bypass	Comply	3.5.1	D.2.3.1
7.5		Maintenance Bypass	Comply	3.5.1	D.2.3.1, D.2.6.2.1.1
8.1	8*	Electrical Power Sources	Comply	3.1.2	D.2.5.1
8.2		Nonelectrical Power Sources	Comply	3.1.2	D.2.5.1
8.3		Maintenance Bypass	Comply	3.5.1	D.2.5.1

8
Technical Specifications (DI&C-ISG-06 D.7)

TBD/TBC 42: **Section 8 requires vendor input from the safety related vendor, which the project team will then review. Section 8 will be updated as needed to demonstrate that the platform, self-tests, self-diagnostics, FMEDA, and analyses provide sufficient coverage to minimize Tech Spec surveillance tests. Throughout Section 8, the language provided is representative of the expected content that the utility and the selected vendor will incorporate in the completed LAR.**

TBD/TBC 43: **All subsections in Section 8.1 require completion based on the selected PPS platform. This section documents licensee understanding of the test coverage for the existing TS and the coverage provided by the selected platform and application software. This section provides the basis and references for the proposed modifications provided in Section 8.2**

TBD/TBC 44: **All subsections in Section 8.2 require completion based on the selected PPS platform. This section is comprised of the changes to the TS, expressed in standard TS format.**

TBD/TBC 45: **All subsections in Section 8.3 require completion based on the selected PPS platform and the setpoint calculation methodology in use at the utility. The data provided is specific to LGS.**

This section provides standard TS content to use as a base for developing vendor and plant specific TS for the PPS.

8.1 Rationale for Technical Specification Changes (DI&C-ISG-06 Section D.7.1)

This section includes a markup of the proposed TS changes, including the SRs and LCOs. This section includes a rationale supporting the changes.

8.1.1 Use of Platform Features to Simplify TS Surveillance Test Requirements (DI&C-ISG-06 Section D.7.2.1)

TBD/TBC 46: **The vendor must provide the technical argument that shows how their self-tests and self-diagnostics provide coverage for the faults and failures detected by the various surveillance tests on the existing analog trip unit and relay based systems. The format for the description of and the rationale for these changes is to be consistent with NEI 06-02.**

TBD/TBC 47: **If the utility uses Risk Informed Completion Times, the utility will update the discussion and tables in this section to incorporate the appropriate modifications and clarifications.**

This section addresses the elimination of TS required surveillance tests. The precedent being set for Vogtle Electric Generating Plant Units 3 and 4, as well as for the Waterford Steam Electric Station, will also be applicable to a BWR. This section provides the technical rationale for these changes, based on the ability of the selected platform to diagnose and indicate internal faults and failures as well as the ability to determine what the platform can do concerning external devices (e.g., over or under scale 4–20 mA input, coil still present). If a Licensing Topical Report is generated for the modification, the rationale for the simplification could be contained in the

Licensing Topical Report. If a Licensing Topical Report exists, reference the report and provide any additional supporting information, if required, in this section.

The discussion in this section will document how the LAR Framework Document allocates self-test and self-diagnostic features and application software to system elements for those features used to support each TS. The discussion in this section will document how the combination of self-test, self-diagnostic, and application software capabilities defined in the LAR, together with manual testing and external cross-checks, is sufficient to support the remaining TS and any proposed TS changes.

Technical arguments will demonstrate that the faults and failures that logic system functional tests and calibrations find in the existing analog and relay-based system are adequately covered by the platform's self-tests, self-diagnostics, and application programming.

The discussion in this section will provide traceability between the faults and failures that the existing TS surveillance tests would find in the existing system and demonstrate that the self-tests, self-diagnostics, and application software in the modernized PPS will uncover equivalent faults and failures in the software-based system and how the modernized PPS provides equivalent or better coverage. This evaluation includes checking for consistency between the TS and self-tests, self-diagnostics, and application software implemented in the architecture, including system interfaces. Redundancy and independence are to be considered, verifying the consistency between each TS and its assumptions regarding redundancy.

The SRs associated with the revised LCOs that govern system operation will be sufficient to test, calibrate, and inspect the system and its functions. The SRs will validate that the necessary operability aspects of the system are ensured and the LCOs are met. Sufficient proposed SRs will be provided to eliminate the potential for the NRC to identify additional SRs.

The discussion in this section will document compliance with IEEE Std. 338 (References 34 and 35) and will document the appropriate exceptions and the rationale for each exception, based on the credited self-test and self-diagnostics features in the modernized PPS.

TBD/TBC 48: Ensure that any vendor exceptions to IEEE Std. 338 are well documented in this section

The discussion in this section will demonstrate compliance with the review guidance in the Standard Review Plan, BTP 7-17 (Reference 74).

It would be desirable if reductions in calibration checks for the PPS could also be invoked. The LAR Framework Document documents the features the platform has to validate correct operation of the analog input circuitry, analog multiplexors, analog-to-digital converters, analog references, and other sources of drift and uncertainty in the PPS analog input modules.

TBD/TBC 49: Methods to validate correct calibration of the ADC inputs are required. This may either be something done within the platform or something we add to the design (perhaps, monitoring highly reliable 1-volt and 5-volt signal inputs on each 4-20 mA process loop card)

8.1.2 Use of Off-Platform Non-Safety Related Software for Channel Checks (DI&C-ISG-06 Section D.7.2.1)

This is a specific subset of the LAR Framework Document section above, dealing with the elimination of manual channel checks and adding automated continuous checking.

The modernized PPS will replace the existing manual data collection that is required every shift. Data collection requires about two hours, and results in data that is not time contiguous. The collected data depends on the accuracy of reading various meters in the CR and in the field. The modernization will eliminate paper reports, which are reviewed and approved by shift management.

As described in this LAR Framework Document, all PPS data and status will be transferred unidirectionally to the non-safety related DCS. Software in the DCS will use the same checking data embedded in the message to validate that the message is not stale. Software in the DCS will then compare the data from redundant transmitters, checking that all readings are within an acceptance range defined for each transmitter. The software will also compare the isolated data from the DAS both to the redundant data from the DAS and against the PPS readings of the same transmitters, determining if the readings are within an acceptance range defined for each transmitter. The software will also compare the votes to scram and actuate to validate that the divisions are working correctly. As the software is designed, additional checks may be added. The software will time stamp a completion time in the data historian to demonstrate that the software has completed the automated replacement for the channel check. Persistent errors will be alarmed to the CR and saved in the DCS historian.

Reports will not be generated or retained. Rather, the software completion and any alarm generated by the software will be retained in the data historian. The detection of stale data and deviations with the resulting alarming in the CR will detect channel and division inoperability. Saving the software status in the data historian can be used to demonstrate that the software comparison function continues to execute in the DCS.

8.2 TECHNICAL SPECIFICATION CONTENT (DI&C-ISG-06 SECTION D.7.2.1)

Implementation of the PPS will also require significant modifications to the TSs. Due to the scope of these changes and in consideration of the requirements of 10 CFR 50.36 Technical Specifications, this LAR Framework Document proposes two new LCOs:

- LCO 3.3.1 – PPS Instrumentation: This LCO consolidates the requirements associated with the existing instrumentation LCOs for the RPS, ECCS, RCIC, and N4S into one LCO[9]. The new LCO makes use of four tables to organize the instrumentation associated with these systems. This is consistent with the PPS architecture in that the PPS now executes the functions of all four systems. The SRs associated with the new LCO reflect

[9] The LCO associated with degraded 4 KV bus voltages in LCO 3.3.3, ECCS Actuation Instrumentation, was not consolidated into the new LCO 3.3.1. The instrumentation that executes this function will not be modified as part of this modification. Therefore, the existing language in LCO 3.3.3 will need to be revised to eliminate all functions except Function 5 (Loss of Power).

the elimination of many legacy SRs, such as channel checks and logic system functional tests. Additionally, for many analog inputs to the PPS, the new LCO reflects that only three of four channels are required for operability. This is consistent with the requirements of 10 CFR 50.36 and satisfies single-failure criteria requirements.

- LCO 3.3.2 – PPS Logic and Manual Trip: The requirements of 10 CFR 50.36(c)(2)(ii)(3) dictate that an LCO must be established for SSCs which are part of the primary success path and function or actuate to mitigate a design basis accident or transient. The introduction of 2oo4 voters as part of the PPS architecture necessitates that a new LCO be established to ensure that operability of this equipment is maintained under all applicable modes. Consistent with these requirements, a new LCO has been developed that addresses the general elements of the four PPS logic channels (e.g., bi-stable logic, coincidence logic processors). These components are germane to all PPS functions, including those for reactor protection, containment isolation, and core cooling.

The existing LGS TSs do not follow the format defined in NRC NUREG-1433, *Standard Technical Specifications – General Electric BWR/4 Plants* (Reference 76). To support broad industry applicability and streamline the existing LGS TSs, the LCOs and SRs in the following pages are applicable to the PPS and were developed consistent with the Standard TS (STS) format in NUREG-1433. The LCOs and SRs developed for the PPS are based on the STS model, and replace all I&C LCOs and SRs for the RPS, N4S, ECCS, and RCIC systems, with some exceptions. LGS will adapt these LCOs and SRs for their existing TSs.

The STSs are broken down into five separate sections. Section 3.0 of the STSs contains LCOs and SRs that must be satisfied to support unrestricted operation of the plant. This section is divided into several subsections which are organized by system type or technical discipline (e.g., reactivity, emergency systems, plant support systems, electrical systems). In the context of STSs, implementation of the PPS will necessitate changes to Subsection 3.3.

Subsection 3.3 includes the LCOs and SRs applicable to the instrumentation used to support operation of various plant systems. These LCOs are largely organized into a set of action statements and supporting tables that are organized based on the functions performed by each set of instrumentation. The tables serve two primary functions: (1) detail the SRs that must be completed to ensure operability for a particular set of instrumentation and (2) direct actions for operators to take in the event that a required instrument is found to be inoperable. The LCOs and SRs outlined below were developed consistent with this approach. Additionally, from a stylistic perspective, the proposed changes to STS Subsection 3.3 have been developed consistent with the guidance in the *Writer's Guide for Plant-Specific Improved Technical Specifications* (TSTF-GG-05-0, Reference 77), which LGS will adapt to the LGS LCOs and SRs.

The numbering convention for the remainder of this section follows the STS for the proposed TSs and not the numbering convention of this LAR Framework Document.

3.3 INSTRUMENTATION

3.3.1 Plant Protection System (PPS) Instrumentation

LCO 3.3.1 The PPS instrumentation for each Function in Table 3.3.1-1, Table 3.3.1-2, Table 3.3.1-3, and Table 3.3.1-4 shall be OPERABLE.

APPLICABILITY: According to Table 3.3.1-1, Table 3.3.1-2, Table 3.3.1-3, and Table 3.3.1-4.

ACTIONS

---------- NOTE ----------

1. Separate Condition entry is allowed for each PPS channel.
2. Penetration flow paths may be unisolated intermittently under administrative controls.

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One channel of Reactor Protection or Nuclear Steam Supply Shutoff Function(s) channels inoperable.	A.1.1 Place channel in BYPASS status. AND A.1.2 Restore channel to OPERABLE status. OR A.2.1 Place channel in TRIP status. AND A.2.2 Restore channel to OPERABLE status.	1 hour 48 hours 48 hours 7 days

CONDITION	REQUIRED ACTION	COMPLETION TIME
B. Two channels of Reactor Protection or Nuclear Steam Supply Shutoff Function(s) inoperable.	B.1 Place one channel in TRIP status and the other in BYPASS status. AND B.2 Restore one channel to OPERABLE status.	1 hour 48 hours
C. One or more Function(s) with Reactor Protection trip capability not maintained.	C.1 Restore Reactor Protection trip capability.	1 hour
D. One or more automatic Functions with primary containment isolation capability not maintained.	D.1 Restore primary containment isolation capability.	1 hour
E. One or more automatic Functions with secondary containment isolation capability not maintained.	E.1 Restore secondary containment isolation capability.	1 hour
F. Required Action and associated Completion Time of Condition A, B, C, D, E, or F not met.	F.1 Enter the Condition referenced in Table 3.3.1-1 or Table 3.3.1-2 for the affected Function(s).	Immediately

CONDITION	REQUIRED ACTION	COMPLETION TIME
G. As required by Required Action F.1 and referenced in Table 3.3.1-1.	G.1.1 Isolate the associated zone(s). OR	1 hour
	G.1.2 Declare associated secondary containment isolation valves inoperable. AND	1 hour
	G.2.1 Place the associated standby gas treatment (SGT) subsystem(s) in operation. OR	1 hour
	G.2.2 Declare associated SGT subsystem(s) inoperable.	1 hour
H. One or more ECCS channels inoperable.	H.1 Enter the Condition referenced in Table 3.3.1-3 for the channel.	Immediately

CONDITION	REQUIRED ACTION	COMPLETION TIME
I. As required by Required Action H.1 and referenced in Table 3.3.1-3.	I.1 ----------NOTES---------- 1. Only applicable in MODES 1, 2, and 3. 2. Only applicable for Functions 1.a, 1.b, 2.a, and 2.b. ----------	
	Declare supported feature(s) inoperable when its redundant feature ECCS initiation capability is inoperable.	1 hour from discovery of loss of initiation capability for feature(s) in both divisions
	AND	
	I.2 ----------NOTE---------- Only applicable for Functions 3.a and 3.b. ----------	
	Declare High Pressure Coolant Injection (HPCI) System inoperable.	1 hour from discovery of loss of HPCI initiation capability
	AND	
	I.3 Place channel in trip.	24 hours

CONDITION	REQUIRED ACTION	COMPLETION TIME
J. As required by Required Action H.1 and referenced in Table 3.3.1-3.	J.1 ----------NOTES---------- 1. Only applicable in MODES 1, 2, and 3. 2. Only applicable for Functions 1.c, 2.c, and 2.d. ---------- Declare supported feature(s) inoperable when its redundant feature ECCS initiation capability is inoperable. <u>AND</u> J.2 Restore channel to OPERABLE status.	 1 hour from discovery of loss of initiation capability for feature(s) in both divisions 24 hours
K. As required by Required Action H.1 and referenced in Table 3.3.1-3.	K.1 ----------NOTE---------- Only applicable if HPCI pump suction is not aligned to the Suppression Pool. ---------- Declare HPCI System inoperable. <u>AND</u> K.2.1 Place channel in trip. <u>OR</u> K.2.2 Align the HPCI pump suction to the Suppression Pool.	 1 hour from discovery of loss of HPCI initiation capability 24 hours 24 hours

CONDITION	REQUIRED ACTION	COMPLETION TIME
L. As required by Required Action H.1 and referenced in Table 3.3.1-3.	L.1 Declare Automatic Depressurization System (ADS) valves inoperable. AND L.2 Place channel in trip.	1 hour from discovery of loss of ADS initiation capability in both trip systems 96 hours from discovery of inoperable channel concurrent with HPCI or reactor core isolation cooling (RCIC) inoperable AND 8 days
M. As required by Required Action H.1 and referenced in Table 3.3.1-3.	M.1 ----------NOTE---------- Only applicable for Functions 4.c, 4.d, 4.e, and 4.h. ---------- Declare ADS valves inoperable. AND M.2 Restore channel to OPERABLE status.	 1 hour from discovery of loss of ADS initiation capability in both trip systems 96 hours from discovery of inoperable channel concurrent with HPCI or RCIC inoperable AND 8 days

CONDITION	REQUIRED ACTION	COMPLETION TIME
N. Required Action and associated Completion Time of Condition I, J, K, L, M, or N not met.	N.1 Declare associated supported feature(s) inoperable.	Immediately
O. One or more RCIC channels inoperable.	O.1 Enter the Condition referenced in Table 3.3.1-4 for the channel.	Immediately
P. As required by Required Action P.1 and referenced in Table 3.3.1-4.	P.1 Declare RCIC System inoperable. AND P.2 Place channel in trip.	1 hour from discovery of loss of RCIC initiation capability 24 hours
Q. As required by Required Action P.1 and referenced in Table 3.3.1-4.	Q.1 Restore channel to OPERABLE status.	24 hours
R. As required by Required Action P.1 and referenced in Table 3.3.1-4.	R.1 ----------NOTE---------- Only applicable if RCIC pump suction is not aligned to the Suppression Pool. ---------- Declare RCIC System inoperable. AND R.2.1 Place channel in trip. OR R.2.2 Align RCIC pump suction to the Suppression Pool.	 1 hour from discovery of loss of RCIC initiation capability 24 hours 24 hours

CONDITION	REQUIRED ACTION	COMPLETION TIME
S. Required Action and associated Completion Time of Condition Q, R, or S not met.	S.1 Declare RCIC System inoperable.	Immediately
T. As required by Required Action F.1 and referenced in Table 3.3.1-1.	T.1 Reduce THERMAL POWER to < 29.5% RTP.	4 hours
U. As required by Required Action F.1 and referenced in Table 3.3.1-1.	U.1 Be in MODE 2.	6 hours
V. As required by Required Action F.1 and referenced in Table 3.3.1-1.	V.1 Be in MODE 3.	12 hours
W. As required by Required Action F.1 and referenced in Table 3.3.1-1.	W.1 If the condition exists due to a common-mode OPRM deficiency, then initiate alternate method to detect and suppress thermal-hydraulic instability oscillations. AND W.2 Restore required channels to OPERABLE status. OR W.3 Reduce THERMAL POWER to <25% RATED THERMAL POWER.	12 hours 120 days 4 hours

CONDITION	REQUIRED ACTION	COMPLETION TIME
X. As required by Required Action F.1 and referenced in Table 3.3.1-1.	X.1 Initiate action to fully insert all insertable control rods.	1 hour
Y. As required by Required Action F.1 and referenced in Table 3.3.1-1.	Y.1 Initiate action to fully insert all insertable control rods in core cells containing one or more fuel assemblies.	Immediately
Z. As required by Required Action F.1 and referenced in Table 3.3.1-2.	Z.1 Isolate associated main steam line. OR Z.2.1 Be in MODE 3. AND Z.2.2 Be in MODE 4.	12 hours 12 hours 36 hours
AA. As required by Required Action F.1 and referenced in Table 3.3.1-2	AA.1 Isolate the affected penetration flow path(s).	1 hour

CONDITION	REQUIRED ACTION	COMPLETION TIME
BB. As required by Required Action F.1 and referenced in Table 3.3.1-2	BB.1 Restore the manual initiation function to OPERABLE. OR BB.2.1 Isolate the affected penetration flow path(s). AND BB.2.2 Declare the affected system inoperable OR BB.3.1 Be in Mode 3. AND BB.3.2 Be in Mode 4.	8 hours 1 hour 1 hour 12 hours 24 hours
CC. As required by Required Action F.1 and referenced in Table 3.3.1-2 OR Required Action and associated Completion Time for Condition AA or BB not met.	CC.1 Be in MODE 3. AND CC.2 Be in MODE 4.	12 hours 24 hours

CONDITION	REQUIRED ACTION	COMPLETION TIME
DD. As required by Required Action F.1 and referenced in Table 3.3.1-2	DD.1 Declare associated Standby Liquid Control System (SLCS) inoperable. OR DD.2 Isolate the Reactor Water Cleanup System.	1 hour 1 hour
EE. As required by Required Action F.1 and referenced in Table 3.3.1-2	EE.1 Initiate action to restore channel to OPERABLE status. OR EE.2 Initiate action to isolate the Residual Heat Removal (RHR) Shutdown Cooling System.	Immediately Immediately
FF. As required by Required Action F.1 and referenced in Table 3.3.1-2	FF.1 Suspend CORE ALTERATIONS. AND FF.2 Suspend movement of RECENTLY IRRADIATED FUEL assemblies in the secondary containment.	Immediately Immediately

SURVEILLANCE REQUIREMENTS

---------- NOTE ----------

Refer to Table 3.3.1-1, Table 3.3.1-2, Table 3.3.1-3, and Table 3.3.1-4 to determine which SR shall be performed for each PPS Function.

	SURVEILLANCE	FREQUENCY
SR 3.3.1.1	Perform CHANNEL CHECK.	In accordance with the Surveillance Frequency Control Program
SR 3.3.1.2	Perform CHANNEL CALIBRATION on each trip channel, including operating bypass removal functions.	In accordance with the Surveillance Frequency Control Program
SR 3.3.1.3	----------NOTE---------- Not required to be performed until 12 hours after THERMAL POWER ≥ 25% RTP. ---------- Verify the absolute difference between the average power range monitor (APRM) channels and the calculated power is ≤ 2% RTP while operating at ≥ 25% RTP.	In accordance with the Surveillance Frequency Control Program
SR 3.3.1.4	Adjust the channel to conform to a calibrated flow signal.	In accordance with the Surveillance Frequency Control Program
SR 3.3.1.5	----------NOTE---------- Not required to be performed when entering MODE 2 from MODE 1 until 12 hours after entering MODE 2. ---------- Perform CHANNEL FUNCTIONAL TEST.	In accordance with the Surveillance Frequency Control Program

SURVEILLANCE		FREQUENCY
SR 3.3.1.6	Perform CHANNEL FUNCTIONAL TEST.	In accordance with the Surveillance Frequency Control Program
SR 3.3.1.7	Calibrate the local power range monitors.	In accordance with the Surveillance Frequency Control Program
SR 3.3.1.8	----------NOTES---------- 1. Neutron detectors are excluded. 2. For Function 2.a, not required to be performed when entering MODE 2 from MODE 1 until 12 hours after entering MODE 2. ---------- Perform CHANNEL CALIBRATION.	In accordance with the Surveillance Frequency Control Program
SR 3.3.1.9	----------NOTES---------- 1. Neutron detectors are excluded. 2. For Function 1, not required to be performed when entering MODE 2 from MODE 1 until 12 hours after entering MODE 2. ---------- Perform CHANNEL CALIBRATION.	In accordance with the Surveillance Frequency Control Program
SR 3.3.1.10	Verify the APRM Flow Biased Simulated Thermal Power - High time constant is ≤ [7] seconds.	In accordance with the Surveillance Frequency Control Program

SURVEILLANCE		FREQUENCY
SR 3.3.1.11	Perform LOGIC SYSTEM FUNCTIONAL TEST.	In accordance with the Surveillance Frequency Control Program
SR 3.3.1.12	Verify Turbine Stop Valve - Closure and Turbine Control Valve Fast Closure, Trip Oil Pressure - Low Functions are not bypassed when THERMAL POWER is ≥ 29.5% RTP.	In accordance with the Surveillance Frequency Control Program
SR 3.3.1.13	----------NOTE---------- 1. Neutron detectors are excluded. ---------- Verify that the REACTOR PROTECTION SYSTEM RESPONSE TIME is within limits.	In accordance with the Surveillance Frequency Control Program
SR 3.3.1.14	Verify the ISOLATION SYSTEM RESPONSE TIME is within limits.	In accordance with the Surveillance Frequency Control Program
SR 3.3.1.15	Verify the ECCS RESPONSE TIME is within limits.	In accordance with the Surveillance Frequency Control Program

Table 3.3.1-1
Reactor Protection Function Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[a]	CONDITIONS	SURVEILLANCE REQUIREMENTS
1. Intermediate Range Monitors				
a. Neutron Flux – High[b]	2	3 per division	V	SR 3.3.1.1 SR 3.3.1.5 SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11
	3[f], 4[f]	3 per division	X	SR 3.3.1.1 SR 3.3.1.5 SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11
	5[f]	3 per division	Y	SR 3.3.1.1 SR 3.3.1.5 SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11
b. Inoperative[b]	2	3 per division	V	SR 3.3.1.5 SR 3.3.1.6 SR 3.3.1.11
	3[f], 4[f]	3 per division	X	SR 3.3.1.5 SR 3.3.1.6 SR 3.3.1.11
	5[f]	3 per division	Y	SR 3.3.1.5 SR 3.3.1.6 SR 3.3.1.11
2. Average Power Range Monitor				
a. Neutron Flux – Upscale (Setdown)	2	3	V	SR 3.3.1.1 SR 3.3.1.5 SR 3.3.1.7 SR 3.3.1.8 SR 3.3.1.11

Table 3.3.1-1
Reactor Protection Function Instrumentation

	FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[(a)]	CONDITIONS	SURVEILLANCE REQUIREMENTS
b.	Simulated Thermal Power – Upscale	1	3	U	SR 3.3.1.1 SR 3.3.1.3 SR 3.3.1.4 SR 3.3.1.6 SR 3.3.1.7 SR 3.3.1.8 SR 3.3.1.10 SR 3.3.1.11 SR 3.3.1.13
c.	Neutron Flux – Upscale	1	3	U	SR 3.3.1.1 SR 3.3.1.3 SR 3.3.1.6 SR 3.3.1.7 SR 3.3.1.8 SR 3.3.1.11 SR 3.3.1.13
d.	Inoperative	1, 2	3	V	SR 3.3.1.6 SR 3.3.1.7 SR 3.3.1.11
e.	2-Out-Of-4 Voter	1, 2	3	V	SR 3.3.1.1 SR 3.3.1.5 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.13
f.	OPRM Upscale	(h)	3	W	SR 3.3.1.1 SR 3.3.1.5 SR 3.3.1.6 SR 3.3.1.7 SR 3.3.1.9
3.	Reactor Vessel Steam Dome Pressure - High	1, 2[(c)]	3	V	SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11 SR 3.3.1.13
4.	Reactor Vessel Water Level – Low, Level 3	1, 2	3	V	SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11 SR 3.3.1.13
5.	Main Steam Line Isolation Valve - Closure	1[(d)]	1 per valve	U	SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11

Table 3.3.1-1
Reactor Protection Function Instrumentation

	FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[a]	CONDITIONS	SURVEILLANCE REQUIREMENTS
					SR 3.3.1.13
6.	Drywell Pressure – High	1, 2[e]	3	V	SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11
7.	Scram Discharge Volume Water Level – High				
	(a) Level Transmitter	1, 2	3	V	SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11
		5[f]	3	Y	SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11
	(b) Float Switch	1, 2	3	V	SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11
		5[f]	3	Y	SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11
8.	Turbine Stop Valve – Closure[g]	≥ 29.5% RTP	1 per valve	T	SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11 SR 3.3.1.12 SR 3.3.1.13
9.	Turbine Control Valve Fast Closure, Trip Oil Pressure – Low[g]	≥ 29.5% RTP	1 per valve	T	SR 3.3.1.6 SR 3.3.1.9 SR 3.3.1.11 SR 3.3.1.12 SR 3.3.1.13
10.	Reactor Mode Switch Shutdown Position	1, 2	2	V	SR 3.3.1.6 SR 3.3.1.11
		3, 4	2	X	SR 3.3.1.6 SR 3.3.1.11
		5	2	Y	SR 3.3.1.6 SR 3.3.1.11

Table 3.3.1-1
Reactor Protection Function Instrumentation

	FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[(a)]	CONDITIONS	SURVEILLANCE REQUIREMENTS
11.	Manual Scram	1, 2	2	V	SR 3.3.1.6 SR 3.3.1.11
		3, 4	2	X	SR 3.3.1.6 SR 3.3.1.11
		5	4	Y	SR 3.3.1.6 SR 3.3.1.11

(a) Each channel provides inputs to both PPS divisions, unless noted otherwise.

(b) This function shall be automatically bypassed when the reactor mode switch is in the Run position.

(c) This function is not required to be OPERABLE when the reactor pressure vessel head is removed per LCO 3.10.1.

(d) This function shall be automatically bypassed when the reactor mode switch is not in the Run position.

(e) This function is not required to be OPERABLE when PRIMARY CONTAINMENT INTEGRITY is not required.

(f) With any control rod withdrawn. Not applicable to control rods removed per LCO 3.9.10.1 or 3.9.10.2.

(g) This function shall be automatically bypassed when turbine first stage pressure is equivalent to a THERMAL POWER of less than 29.5% of RATED THERMAL POWER.

(h) With THERMAL POWER ≥ 25% RATED THERMAL POWER. The OPRM Upscale trip output shall be automatically enabled (not bypassed) when APRM Simulated Thermal Power is ≥ 29.5% and recirculation drive flow is < 60%. The OPRM trip output may be automatically bypassed when APRM Simulated Thermal Power is < 29.5% or recirculation drive flow is ≥ 60%.

Table 3.3.1-2
Nuclear Steam Supply Shutoff Function Instrumentation

FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[a]	CONDITIONS	SURVEILLANCE REQUIREMENTS
1. Main Steam Line Isolation				
a. Reactor Vessel Water Level				
1) Low, Low – Level 2	1, 2, 3	3	Z	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
2) Low, Low, Low – Level 1	1, 2, 3	3	Z	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
b. Main Steam Line Pressure – Low	1	3	U	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
c. Main Steam Line Flow – High	1, 2, 3	3 per Main Steam Line	Z	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
d. Condenser Vacuum – Low	1, 2[c], 3[c]	3	Z	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
e. Outboard MSIV Room Temperature – High	1, 2, 3	1 per area	Z[e]	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
f. Turbine Enclosure – Main Steam Line Tunnel Temperature – High	1, 2, 3	1 per area	Z[e]	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
g. Manual Initiation	1, 2, 3	1	BB	SR 3.3.1.11

Table 3.3.1-2
Nuclear Steam Supply Shutoff Function Instrumentation

	FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[(a)]	CONDITIONS	SURVEILLANCE REQUIREMENTS
2.	RHR System Shutdown Cooling Mode Isolation				
a.	Reactor Vessel Water Level Low – Level 3	3, 4, 5	3	EE	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
b.	Reactor Vessel (RHR Cut-in Permissive) Pressure – High	1, 2, 3	3	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
c.	Manual Initiation	1, 2, 3	1	BB	SR 3.3.1.11
3.	Reactor Water Cleanup Isolation				
a.	RWCU Δ Flow – High	1, 2, 3	1 per division	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
b.	RWCU Area Temperature – High	1, 2, 3	1 per area	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
c.	RWCU Area Ventilation Δ Temperature – High	1, 2, 3	1 per area	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
d.	SLCS Initiation	1, 2	(f)	DD	SR 3.3.1.11
e.	Reactor Vessel Water Level – Low, Low – Level 2	1, 2, 3	3	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
f.	Manual Initiation	1, 2, 3	1	BB	SR 3.3.1.11

Table 3.3.1-2
Nuclear Steam Supply Shutoff Function Instrumentation

	FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[(a)]	CONDITIONS	SURVEILLANCE REQUIREMENTS
4.	High Pressure Coolant Injection System Isolation				
a.	HPCI Steam Line Δ Pressure – High	1, 2, 3	3	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
b.	HPCI Steam Supply Pressure – Low	1, 2, 3	3	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
c.	HPCI Turbine Exhaust Diaphragm Pressure – High	1, 2, 3	3	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
d.	HPCI Equipment Room Temperature - High	1, 2, 3	1 per area	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
e.	HPCI Equipment Room Δ Temperature – High	1, 2, 3	1 per area	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
f.	HPCI Pipe Routing Area Temperature – High	1, 2, 3	1 per area	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
g.	Manual Initiation	1, 2, 3	1	BB	SR 3.3.1.11
5.	Reactor Core Isolation System Isolation				
a.	RCIC Steam Line Δ Pressure – High	1, 2, 3	1	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
b.	RCIC Steam Supply Pressure – Low	1, 2, 3	2	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
c.	RCIC Turbine Exhaust Diaphragm Pressure – High	1, 2, 3	2	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11

Table 3.3.1-2
Nuclear Steam Supply Shutoff Function Instrumentation

	FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[(a)]	CONDITIONS	SURVEILLANCE REQUIREMENTS
d.	RCIC Equipment Room Temperature - High	1, 2, 3	1 per area	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
e.	RCIC Equipment Room Δ Temperature – High	1, 2, 3	1 per area	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
f.	RCIC Pipe Routing Area Temperature – High	1, 2, 3	1 per area	AA	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
g.	Manual Initiation	1, 2, 3	1	BB	SR 3.3.1.11
6.	Primary Containment Isolation				
a.	Reactor Vessel Water Level				
	1) Low, Low – Level 2	1, 2, 3	3	CC	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
	2) Low, Low, Low – Level 1	1, 2, 3	3	CC	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
b.	Drywell Pressure – High	1, 2, 3	3	CC	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
c.	North Stack Effluent Radiation – High	1, 2, 3	1	AA	SR 3.3.1.1 SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
d.	Reactor Enclosure Ventilation Exhaust Duct – Radiation – High	1, 2, 3	2 per division	CC	SR 3.3.1.1 SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14

Table 3.3.1-2
Nuclear Steam Supply Shutoff Function Instrumentation

	FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[(a)]	CONDITIONS	SURVEILLANCE REQUIREMENTS
e.	Drywell Pressure – High/Reactor Pressure – Low	1, 2, 3	3	CC	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
f.	Primary Containment Instrument Gas to Drywell Δ Pressure – Low	1, 2, 3	1 per isolation valve	CC	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
g.	Manual Initiation	1, 2, 3	1	BB	SR 3.3.1.11
7.	Secondary Containment Isolation				
a.	Reactor Vessel Water Level - Low, Low – Level 2	1, 2, 3	3	G	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
b.	Drywell Pressure – High	1, 2, 3	3	G	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
c.	Refueling Area Ventilation Radiation				
1)	Unit 1 Ventilation Exhaust Duct Radiation – High	(b)	2 per division	G	SR 3.3.1.1 SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
		(d)	2 per division	G	SR 3.3.1.1 SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14

Table 3.3.1-2
Nuclear Steam Supply Shutoff Function Instrumentation

	FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[(a)]	CONDITIONS	SURVEILLANCE REQUIREMENTS
	2) Unit 2 Ventilation Exhaust Duct Radiation – High	(b)	2 per division	G	SR 3.3.1.1 SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
		(d)	2 per division	G	SR 3.3.1.1 SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
d.	Reactor Enclosure Ventilation Exhaust Duct – Radiation – High	1, 2, 3	2 per division	G	SR 3.3.1.1 SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.14
e.	Reactor Enclosure Manual Initiation	1, 2, 3	1	G	SR 3.3.1.11
f.	Refueling Area Manual Initiation	(b)	1	G	SR 3.3.1.11

(a) Each channel provides inputs to both PPS divisions, unless noted otherwise.

(b) Required when handling RECENTLY IRRADIATED FUEL in the secondary containment.

(c) May be bypassed under administrative control, with all turbine stop valves closed.

(d) During operation of the associated Unit 1 or Unit 2 ventilation exhaust system.

(e) In the event of a loss of ventilation the temperature – high set point may be raised by 50°F for a period not to exceed 30 minutes to permit restoration of the ventilation flow without a spurious trip. During the 30 minute period, an operator, or other qualified member of the technical staff, shall observe the temperature indications continuously, so that, in the event of rapid increases in temperature, the main steam lines shall be manually isolated.

(f) Two channels must be OPERABLE for the inboard isolation valve and one channel must be OPERABLE for the outboard valve.

Table 3.3.1-3
Emergency Core Cooling System Instrumentation

	FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[(a)]	CONDITIONS	SURVEILLANCE REQUIREMENTS
1.	Core Spray System				
a.	Reactor Vessel Water Level - Low, Low, Low – Level 1	1, 2, 3	3	I	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.15
b.	Drywell Pressure – High	1, 2, 3	3	I	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.15
c.	Reactor Vessel Pressure – Low (Permissive)	1, 2, 3	3	J	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.15
d.	Manual Initiation	1, 2, 3	1	J	SR 3.3.1.11
2.	Low Pressure Coolant Injection Mode of RHR System				
a.	Reactor Vessel Water Level - Low, Low, Low – Level 1	1, 2, 3	3	I	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.15
b.	Drywell Pressure – High	1, 2, 3	3	I	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.15
c.	Reactor Vessel Pressure – Low (Permissive)	1, 2, 3	3	J	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.15
d.	Injection Valve Differential Pressure – Low (Permissive)	1, 2, 3	3	J	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
e.	Manual Initiation	1, 2, 3	1	J	SR 3.3.1.11

Table 3.3.1-3
Emergency Core Cooling System Instrumentation

	FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[a]	CONDITIONS	SURVEILLANCE REQUIREMENTS
3.	High Pressure Coolant Injection System				
a.	Reactor Vessel Water Level - Low, Low – Level 2	1, 2[b], 3[b]	3	I	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.15
b.	Drywell Pressure – High[d]	1, 2[b], 3[b]	3	I	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.15
c.	Condensate Storage Tank Level – Low	1, 2[b], 3[b]	3	K	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
d.	Suppression Pool Water Level – High	1, 2[b], 3[b]	3	K	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
e.	Reactor Vessel Water Level – High - Level 8	1, 2[b], 3[b]	3	J	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11 SR 3.3.1.15
f.	Manual Initiation[d]	1, 2[b], 3[b]	1	J	SR 3.3.1.11
4.	Automatic Depressurization System				
a.	Reactor Vessel Water Level - Low, Low, Low – Level 1	1, 2[c], 3[c]	3	L	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
b.	Drywell Pressure – High	1, 2[c], 3[c]	3	L	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
c.	Core Spray Pump Discharge Pressure – High (Permissive)	1, 2[c], 3[c]	1 per pump	M	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11

Table 3.3.1-3
Emergency Core Cooling System Instrumentation

	FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[(a)]	CONDITIONS	SURVEILLANCE REQUIREMENTS
d.	RHR LPCI Mode Pump Discharge Pressure – High (Permissive)	1, 2[(c)], 3[(c)]	1 per pump	M	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
e.	Reactor Vessel Water Level – Low – Level 3 (Permissive)	1, 2[(c)], 3[(c)]	3	L	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
f.	Manual Initiation	1, 2[(c)], 3[(c)]	1	M	SR 3.3.1.11

(a) Each channel provides inputs to both PPS divisions, unless noted otherwise.

(b) With reactor steam dome pressure greater than 200 psig.

(c) With reactor steam dome pressure greater than 100 psig.

(d) The injection functions of Drywell Pressure – High and Manual Initiation are not required to be OPERABLE with reactor steam dome pressure less than 550 psig.

Table 3.3.1-4
Reactor Core Isolation Cooling System Instrumentation

	FUNCTION	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED CHANNELS[a]	CONDITIONS	SURVEILLANCE REQUIREMENTS
1.	Reactor Vessel Water Level - Low, Low – Level 2	1, 2[b], 3[b]	3	P	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
2.	Reactor Vessel Water Level – High – Level 8	1, 2[b], 3[b]	3	Q	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
3.	Condensate Storage Tank Level – Low	1, 2[b], 3[b]	3	R	SR 3.3.1.2 SR 3.3.1.6 SR 3.3.1.11
4.	Manual Initiation	1, 2[c], 3[c]	1	Q	SR 3.3.1.11

(a) Each channel provides inputs to both PPS divisions, unless noted otherwise.

(b) With reactor steam dome pressure greater than 150 psig.

(c) With reactor steam dome pressure greater than or equal to 550 psig.

3.3 INSTRUMENTATION

3.3.2 Plant Protection System (PPS) Logic

LCO 3.3.2 Four PPS logic channels shall be OPERABLE.

APPLICABILITY: MODES 1, 2, 3, 4, and 5.

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One PPS logic channel inoperable.	A.1.1 Place channel in BYPASS	1 hour
	AND	
	A.1.2 Restore channel to OPERABLE status.	48 hours
	OR	
	A.2.1 Place channel in TRIP status	48 hours
	AND	
	A.2.2 Restore channel to OPERABLE status.	7 days

CONDITION	REQUIRED ACTION	COMPLETION TIME
B. Two channels of PPS logic inoperable.	B.1 Place one channel associated with the affected Reactor Protection, Nuclear Steam Supply Shutoff, and Emergency Core Cooling Functions in TRIP status and the other in BYPASS. AND B.2 Restore at least one channel to OPERABLE status.	1 hour 48 hours
C. Required Action and associated Completion Time of Condition A or B not met.	C.1 Be in MODE 3. AND C.2 Be in MODE 4.	12 hours 36 hours
D. Two channels of PPS logic inoperable during CORE ALTERATIONS or during movement of RECENTLY IRRADIATED FUEL assemblies.	D.1 Suspend CORE ALTERATIONS. AND D.2 Suspend movement of RECENTLY IRRADIATED FUEL assemblies.	Immediately Immediately

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
SR 3.3.1.1	Perform a CHANNEL FUNCTIONAL TEST on each Reactor Protection logic channel in the PPS.	In accordance with the Surveillance Frequency Control Program
SR 3.3.2.2	Perform a CHANNEL FUNCTIONAL TEST on each Nuclear Steam Supply Shutoff logic channel in the PPS.	In accordance with the Surveillance Frequency Control Program
SR 3.3.2.3	Perform a CHANNEL FUNCTIONAL TEST on each ECCS logic channel in the PPS.	In accordance with the Surveillance Frequency Control Program
SR 3.3.2.3	Perform a CHANNEL FUNCTIONAL TEST on each RCIC logic channel in the PPS.	In accordance with the Surveillance Frequency Control Program

8.3 SETPOINT CHANGE METHODOLOGY APPLIED (DI&C-ISG-06 SECTION D.7.2.2)

As noted in the LGS UFSAR (Reference 41), Section 7.1.2.5.25, LGS uses a setpoint methodology generated by GE[10] and submitted for NRC review on November 19, 1986. The methodology has been accepted by the NRC as demonstrated by the issuance of a Supplement SE Report (SSER) for the Power Re-Rate for LGS. LGS will use the approved setpoint methodology for the PPS and DAS inputs. The only changes for the PPS and DAS will be the substitution of uncertainties appropriate to the platform to replace uncertainties from the PPS analog trip modules and creating uncertainties for the DAS analog inputs. This section will reference the PPS vendor's licensing topical report (Reference 42) sections that define the platform uncertainties, and any supplemental materials required for hardware changes and/or additional modules and/or features that reduce uncertainties.

TBD/TBC 50: LGS to check the validity of the GE setpoint methodology for PPS note supplied by GE and to supply reference for the SSER.

The setpoint methodology used is in compliance with the guidance provided in RG 1.105 and RIS 2006-17. LGS will prepare, review, approve, and retain the setpoint calculations as quality records.

[10] UFSAR Reference 7.1-1, "Letter from J.F. Carolan (Chairman, LRG Instrumentation Setpoint Methodology Group) to T.M. Novak (NRC), 'Action Plan to Answer the NRC Staff concerns on Setpoint Methodology for General Electric Supplied Protection System Instrumentation,' (June 29, 1984).

9

Secure Development and Operational Environment (DI&C-ISG-06 D.8)

TBD/TBC 51: **Section 9 requires vendor input from both the safety related and non-safety related vendors, which the project team will then review. Section 9 will be updated to reflect how the individual vendors work with LGS to ensure that the two vendors' systems development environments support the operational environments for both the PPS and DAS function in the DCS. Throughout Section 9, the language provided is representative of the expected content that the utility and the selected vendor will incorporate in the completed LAR.**

TBD/TBC 52: **Subsections within Section 9.1 document the required basis for the PPS vendor's SDOE program, integration vendor's SDOE program for the PPS and DAS integration as well as the PPS vendor's responsibilities during integration, and for the utility's SDOE program after installation. The SDOE program provides a basis for the utility's cyber security program. These sections can only be completed after the DAS vendor and the integration vendor are selected. The discussion should include how PPS development, defined in Section 5.1, interacts with Section 9 on SDOE. The discussion should also document plans for resolution of detected errors, including all system lifecycle phases.**

TBD/TBC 53: **Subsections within Section 9.2 document the required basis for the DAS vendor's SDOE program, integration vendor's SDOE program for the PPS and DAS integration as well as the DAS vendor's responsibilities during integration, and for the vendor's maintenance of cyber security after delivery as well as the utility's cyber security program after installation. The SDOE program provides a basis for the utility's cyber security program. These sections can only be completed after the DAS vendor and the integration vendor are selected. The discussion should also document plans for resolution of detected errors, including all system lifecycle phases.**

The SDOE environment is important for ensuring that the PPS and DAS are designed, developed, verified, validated, tested, shipped, stored, installed, operated, maintained, and retired in accordance with the guidance in RG 1.152, Rev. 3 or later.

The PPS vendor, DAS vendor, and LGS will need to cooperatively complete this section. LGS will then need to review and accept the process, which would be incorporated into the PPS VOP and DAS VOPs. The broad categories of information required are listed in each LAR Framework Document section.

9.1 PPS: Evaluation of Changes from Vendor SE Report

This section contains a summary of the vendor's SDOE as evaluated in the NRC's SE Report (Reference 43). This section then discusses any changes made to the vendor's SDOE program since the NRC's SE Report was finalized. The following sections discuss both the platform and application software.

Starting at the beginning of the design, a vulnerability assessment is performed and updated throughout the PPS lifecycle to ensure that changes to the PPS and changes to the threats are still covered by the Secure Operating Environment portions of the SDOE process defined in RG 1.152.

9.1.1 PPS Concepts

This section contains a discussion of any changes in vendor methods (e.g., firewalls, processes, procedures, use of personal computers, printers, and network storage) used to protect the conceptual design from malicious or unapproved change or disclosure. This discussion includes the cyber security aspects of lifecycle activities applicable to this phase, including requirements traceability, V&V, change control, CM, and interfaces with licensee and licensee's subcontractors.

9.1.2 PPS Requirements

This section contains a discussion of any changes in vendor methods used to protect the system, software, and hardware requirements documents from malicious or unapproved change or disclosure while system and software requirements are generated. This discussion includes the cyber security aspects of lifecycle activities applicable to this phase, including requirements traceability, V&V, change control, CM, and interfaces with licensee and licensee's subcontractors.

9.1.3 PPS Design

This section contains a discussion of any changes in vendor methods used to protect the system, software, and hardware design documents (e.g., calculations, drawings, printed circuit board layouts, bill of materials) from malicious or unapproved change or disclosure during the design process. This discussion includes the cyber security aspects of lifecycle activities applicable to this phase, including requirements traceability, V&V, change control, CM, and interfaces with licensee and licensee's subcontractors.

9.1.4 PPS Implementation

This section contains a discussion of any changes in vendor methods used to protect the system, software, and hardware design documents and implementations from malicious or unapproved change or disclosure during code implementation and unit test. This discussion includes the cyber security aspects of lifecycle activities applicable to this phase, including requirements traceability, V&V, change control, CM, and interfaces with licensee and licensee's subcontractors.

9.1.5 PPS Integration and Test

This section contains a discussion of any changes in vendor methods used to protect the system, software, and hardware design documents and implementations from malicious or unapproved change or disclosure during software, systems, and hardware integration and testing. This discussion includes the cyber security aspects of lifecycle activities applicable to this phase, including requirements traceability, V&V, change control, CM, and interfaces with licensee and licensee's subcontractors.

9.1.6 PPS Installation, Checkout, Acceptance Testing at the PPS Vendor, and Shipment to the PPS and DAS Integration Vendor

This section contains a discussion of any changes in vendor methods used to protect the system, software, and hardware design documents and implementations from malicious or unapproved change or disclosure during activities including installation activities at the vendor's site, checkout, factory acceptance testing, and shipment to the integration vendor. This discussion includes the cyber security aspects of lifecycle activities applicable to this phase, including requirements traceability, V&V, change control, CM, and interfaces with licensee and licensee's subcontractors.

9.1.7 PPS and DAS Receipt, Storage, Setup, Checkout, Testing, and Shipment at the Integration Vendor

This section contains a discussion of methods used by the system vendor and integration vendor to protect the system, software, and hardware design documents and implementations during all activities associated with this phase, including resolution of detected errors. The PPS vendor remains responsible for design documents and any equipment retained at the vendor's location. This discussion includes the cyber security aspects applicable to this phase, including interfaces with licensee and licensee's subcontractors. The PPS vendor's cyber security program continues to protect the portions of the PPS design basis and test equipment in the vendor's possession.

9.1.8 Licensee and Vendor Responsibility for Receipt, Storage, Setup, Plant Installation, Checkout, and Acceptance Testing for PPS and DAS

This section discusses PPS vendor, DAS vendor, and integration vendor responsibilities for SDOE during PPS and DAS integration through installation and acceptance. The integration vendor remains responsible for the cyber security of the safety related PPS platform, application, and software tools as well as the HSI and DKT system up to the time the equipment is unloaded at the LGS Receiving dock. LGS will maintain the PPS cyber security, including use of cyber-qualified staff to inspect the incoming equipment, as the equipment is receipt inspected and stored before installation. LGS will maintain cyber security as staff moves the equipment from the storage location to the CR and AER LGS will maintain cyber security during installation and commissioning. LGS will maintain PPS cyber security during the transition to the normal operating unit cyber security program. The PPS vendor's cyber security program continues to protect the portions of the PPS design basis and test equipment in the vendor's possession, just as the DAS vendor's cyber security program continues to protect the portions of the DAS design basis and test equipment in the vendor's possession.

9.1.9 Licensee and Vendor Responsibility for Operation for PPS and DAS

The PPS will operate under the LGS approved cyber security program. The PPS design maximizes self-protection from malicious or unapproved change or disclosure as part of the Cyber Security Level 4 program. Once installation of the equipment in the AER and CR is complete, the existing vital area access controls are in place to protect access to the PPS equipment. The equipment installed outside the CR uses levels of password protection to minimize the ability of unauthorized staff to make changes. The PPS vendor's cyber security

program continues to protect the portions of the PPS design basis and test equipment in the vendor's possession, just as the DAS vendor's cyber security program continues to protect the portions of the DAS design basis and test equipment in the vendor's possession.

TBD/TBC 54: Will there be AER cabinet doors to restrict access to the PPS logic solvers and DKT equipment? Should we alarm these doors to protect from unauthorized or inappropriate access (i.e., for cyber security)?

9.1.10 Licensee and Vendor Responsibility for Maintenance for PPS and DAS

PPS application software maintenance will be performed under an umbrella established by the LGS cyber security program, with the vendor's cyber security program added for application software modification. Any modifications to the vendor's cyber security program since the last LGS use of that program requires LGS review and approval. The vendor will implement any required changes under the vendor's cyber security program. The vendor will modify the vendor's controlled copy of the software and verify and validate the incorporation of only the intended, evaluated changes. All software modifications are performed under the vendor's approved application software process, including vendor plans, procedures, and instructions.

Installation, commissioning, and acceptance of the modified application software is LGS's responsibility, with help as required from the vendor. LGS is also responsible for any licensing actions required to modify and install the software. The PPS vendor's cyber security program continues to protect the portions of the PPS design basis and test equipment in the vendor's possession, just as the DAS vendor's cyber security program continues to protect the portions of the DAS design basis and test equipment in the vendor's possession.

9.1.11 PPS and DAS Retirement

At the time when the system is to be retired, the licensee and vendor will determine an appropriate path for the destruction of the cyber secure portions of the system, including the documentation, software, hardware, EWS, and software tools. The PPS vendor's cyber security program continues to protect the portions of the PPS design basis and test equipment in the vendor's possession, just as the DAS vendor's cyber security program continues to protect the portions of the DAS design basis and test equipment in the vendor's possession.

9.1.12 Conclusion

The activities performed by the vendor and by LGS are adequate to fulfill the requirements for PPS SDOE to meet the requirements of the NRC's SE Report (Reference 43) and the SDOE description in RG 1.152, Rev. 3.

9.2 DAS: LICENSEE EVALUATION OF VENDOR SDOE PROGRAM

The DAS vendor is not expected to have an NRC SDOE evaluation, since the NRC has not evaluated the commercial DCS platform that implements the DAS. Instead, LGS is responsible for evaluating the vendor's program against the requirements in RG 1.152 Rev 3, Section C.2. The DAS includes the ATWS function.

Starting at the beginning of the design, a vulnerability assessment is performed and updated throughout the PPS lifecycle to ensure that changes to the PPS and changes to the threats are still covered by the Secure Operating Environment portions of the SDOE process defined in RG 1.152.

9.2.1 DAS Concepts

This section contains the LGS evaluation of vendor SDOE methods (e.g, firewalls, processes, procedures, use of personal computers, printers, network storage) used to protect the conceptual design from malicious or unapproved change or disclosure. This discussion includes the cyber security aspects of lifecycle activities applicable to this phase, including requirements traceability, V&V, change control, CM, and interfaces with licensee and licensee's subcontractors.

9.2.2 DAS Requirements

This section contains the LGS evaluation of vendor SDOE methods used to protect the system, software, and hardware requirements documents from malicious or unapproved change or disclosure while system and software requirements are generated. This discussion includes the cyber security aspects of lifecycle activities (applicable to this phase, including requirements traceability, V&V, change control, CM, and interfaces with licensee and licensee's subcontractors.

9.2.3 DAS Design

This section contains the LGS evaluation of vendor SDOE methods used to protect the system, software, and hardware design documents (e.g., calculations, drawings, printed circuit board layouts, bill of materials) from malicious or unapproved change or disclosure during the design process. This discussion includes the cyber security aspects of lifecycle activities applicable to this phase, including requirements traceability, V&V, change control, CM, and interfaces with licensee and licensee's subcontractors.

9.2.4 DAS Implementation

This section contains the LGS evaluation of vendor SDOE methods used to protect the system, software, and hardware design documents and implementations from malicious or unapproved change or disclosure during code implementation and unit test. This discussion includes the cyber security aspects of lifecycle activities applicable to this phase, including requirements traceability, V&V, change control, CM, and interfaces with licensee and licensee's subcontractors.

9.2.5 DAS Integration and Test

This section contains the LGS evaluation of vendor SDOE methods used to protect the system, software, and hardware design documents and implementations during testing from malicious or unapproved change or disclosure during software, systems, and hardware integration and testing. This discussion includes the cyber security aspects of lifecycle activities applicable to this phase,

including requirements traceability, V&V, change control, CM, and interfaces with licensee and licensee's subcontractors.

9.2.6 DAS Installation, Checkout, and Acceptance Testing at DAS Vendor

This section contains the LGS evaluation of vendor SDOE methods used to protect the system, software, and hardware design documents and implementations from malicious or unapproved change or disclosure during activities including installation activities at the vendor's site, checkout, factory acceptance testing, and shipment to the integration vendor. This discussion includes the cyber security aspects of lifecycle activities applicable to this phase, including requirements traceability, V&V, change control, CM, and interfaces with licensee and licensee's subcontractors.

9.2.7 DAS Shipment to the Integration Vendor

The DAS vendor remains responsible for the cyber security of the non-safety related DAS platform, application, and software tools up to the time the equipment is unloaded at the integration vendor's dock. The installation vendor is then responsible for maintaining the PPS and DAS cyber security. The DAS vendor's cyber security program continues to protect the portions of the DAS design basis documentation and test equipment in the DAS vendor's possession, with the responsibility for control of the shipped DAS equipment maintained in accordance with Sections 9.1.7 through 9.1.11.

9.2.8 Licensee Responsibility DAS Design and Retained Equipment

Section 9.1.7 defines the SDOE responsibilities of the integration vendor. Section 9.1.8 defines the SDOE responsibilities of the licensee from receipt at LGS through acceptance testing. Sections 9.1.9, 9.1.10, and 9.1.11 define the SDOE LGS responsibilities for Operation, Maintenance, and Retirement. Through all these activities, the DAS vendor remains responsible for the vendor aspects of SDOE for the DAS, including any error corrections, for the DAS equipment at the integration vendor and all equipment and design documentation maintained by the DAS vendor.

The joint responsibilities activities during these phases are described in Sections 9.1.8 through 9.1.11.

9.2.9 Conclusion

The activities performed by the vendor and by LGS are adequate to fulfill the requirements for SDOE for the DAS portion of the DCS and fulfills the SDOE description in RG 1.152, Rev. 3.

10 References

TBD/TBC 55: Highlighted references require vendor selection, creation of an Exelon document, or other data to complete.

TBD/TBC 56: Provide seismic spectra and amplitudes for the AER cabinets where Analog Trip Units and Relays are installed (Seismic I) and Engineering Workstation will be installed (Seismic II over I), and Control Room (Seismic I).

1. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls Interim Staff Guidance #6, Rev. 2, *Licensing Process*

2. Electric Power Research Institute, Product 3002011816, *Digital Engineering Guide: Decision Making Using Systems Engineering*

3. Nuclear Energy Institute, NEI 06-02, Rev. 6, *License Amendment Request (LAR) Guidelines*

4. IEEE Std. 603-1991, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*

5. IEEE Std. 7-4.3.2-2003, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*

6. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.152, Rev. 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"

7. VENDOR Document *TBD*, *Defense-in-Depth and Diversity Analysis for Modernized Limerick PPS*

8. Title 10 of the Code of Federal Regulation, Part 50, Energy, Section 62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants"

9. Exelon, Document *TBD*, *Vendor Conformed Functional Requirements for the Limerick Plant Protection System (PPS)*

10. IEEE Standard 279-1971, *IEEE Standard Criteria for Protection Systems for Nuclear Power Generating Stations*

11. IEEE Std. 308-1971, *IEEE Standard Criteria for Class 1E Electrical Systems for Nuclear Power Generating Stations*

12. IEEE Std. 308-1974, *IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations*

13. IEEE Std. 317-1972, *IEEE Standard for Electric Penetration Assemblies in Containment Structures for Nuclear Power Generating Stations*

14. IEEE Std. 323-1971, *IEEE Trial-Use Standard: General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations*

15. IEEE Std. 336-1971, *IEEE Standard Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations*

16. IEEE Std. 338-1971, *IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems*

17. IEEE Std. 338-1975, *IEEE Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Class IE Power and Protection Systems*

18. IEEE Std. 338-1977, *IEEE Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Class IE Power and Protection Systems*

19. IEEE Std. 344-1971, *IEEE Trial-Use Guide for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations*

20. IEEE Std. 344-1975, *IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*

21. IEEE Std. 379-1972, *IEEE Trial-Use Guide for the Application of the Single-Failure Criterion to Nuclear Power Generating Station Protection Systems*

22. IEEE Std. 379-1977, *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Class 1E Systems*

23. IEEE Std. 382-1972, *IEEE Trial-Use Guide for Type Test of Class 1 Electric Valve Operators for Nuclear Power Generating Stations*

24. IEEE Std. 383-1974, *IEEE Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations*

25. IEEE Std. 384-1974, *IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits*

26. IEEE Std. 384-1977, *IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits*

27. IEEE Std. 603-2018, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*

28. IEEE Std. 7-4.3.2-2016, *Standard Criteria for Programmable Digital Devices in Safety Systems for Nuclear Power Generating Stations*

29. IEEE Std. 308-2001, *IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations*

30. IEEE Std. 308-2012, *IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations*

31. IEEE Std. 323-2003, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*

32. International Electrotechnical Commission (IEC)/IEEE 60780/323-2016, *Nuclear facilities – Electrical equipment important to safety – Qualification*

33. IEEE Std. 336-2010, *IEEE Recommended Practice for Installation, Inspection, and Testing for Class 1E Power, Instrumentation, and Control Equipment at Nuclear Facilities*

34. IEEE Std. 338-1987, *IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems*

35. IEEE Std. 338-2012, *IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems*

36. IEEE Std. 379-2003, *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*

37. IEEE Std. 379-2014, *IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*

38. IEEE Std. 383-2015, *IEEE Standard for Qualifying Electric Cables and Splices for Nuclear Facilities*

39. IEEE Std. 384-1992, *IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits*

40. IEEE Std. 384-2018, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*

41. Limerick Generating Station, Document *TBD*, *Limerick Generating Station Updated Final Safety Analysis* (UFSAR)

42. VENDOR, Document *TBD*, *Licensing Topical Report*

43. NRC, Document *TBD*, *Safety Evaluation Report for Vendor's Licensing Topical Report*

44. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls Interim Staff Guidance #4, Rev. 1, *Highly-Integrated Control Rooms – Communications Issues (HICRc)*

45. IEEE Std. 497-1981, *IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations*

46. Limerick Generating Station Drawing 071-03a, "Rod SCRAM Groups," Rev. 1, September 17, 2003

47. Limerick Generating Station Drawing 071-04a, "SCRAM Relay (K14) Development," Rev. 1, September 17, 2001

48. Limerick Generating Station Drawing 071-06a, "A1 Auto SCRAM Channel," Rev. 1, September 17, 2003

49. Limerick Generating Station Drawing 074-08, "Average Power Range Monitoring (APRM) Function," Rev. 1, June 30, 2008

50. Limerick Generating Station Drawing 072-05, "Typical NSSSS (N4S) Inboard & Outboard Isolation Logic," Rev. 0, November 18, 2005

51. Limerick Generating Station Drawing 072-07, "MSIV Logic Power Supplies," Rev. 0, November 18, 2005

52. Limerick Generating Station Drawing M-1-E11-1040-3-009, Sheet 1, "Elementary Diagram Residual Heat Removal System," Rev. 19

53. Limerick Generating Station Drawing M-1-E41-1040-E-005, Sheet 1, "Elementary Diagram HPCI System," Rev. 30

54. Limerick Generating Station Drawing 050-01, "ADS," Rev. 0, June 13, 1997

55. VENDOR, Document *TBD*, *PPS Failure Modes, Effects, and Diagnostics (FMEDA) Analysis*

56. NRC Regulatory Guide 1.47, Rev. 1, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"

57. NRC Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That is Not Safety Related"

58. Exelon, Document *TBD*, *Vendor Conformed Functional Requirements for the Limerick Diverse Actuation System Function in the Distributed Control System*

59. Title 10, Energy, of the Code of Federal Regulation, Part 50, Domestic Licensing of Production and Utilization Facilities, Appendix A, "General Design Criteria for Nuclear Power Plants"

60. Nuclear Regulatory Commission, NUREG/CR-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*

61. VENDOR, Document *TBD*, *Supplement to the Licensing Topical Report*

62. Nuclear Regulatory Commission, Regulatory Guide 1.180, Rev. 2, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety Related Instrumentation and Control Systems

63. Limerick Generating Station, Document *TBD*, *Safety Related PPS Vendor Oversight Plan*

64. Limerick Generating Station, Document *TBD*, *Non-Safety Related Augmented Quality DAS Vendor Oversight Plan*

65. Limerick Generating Station, Calculation M-171, Rev. 17, "Specification for Environmental Service Conditions, Limerick Generating Station, Units 1 and 2"

66. Limerick Generating Station, Calculation *TBD* Rev. *TBD*, "Auxiliary Equipment Room Floor OBE and SSE Spectra"

67. Limerick Generating Station, Calculation LS-0192, Rev. 2, "Dynamic Qualification Requirements for Control Room Panels"

68. IEEE Std. 1012-2004, *IEEE Standard for Software Verification and Validation*

69. Nuclear Regulatory Commission, Regulatory Guide 1.168, Rev. 2, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

70. IEEE Std. 1028-2008, *IEEE Standard for Software Reviews and Audits*

71. Nuclear Regulatory Commission, Regulatory Guide 1.170, Rev. 1, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

72. IEEE Std. 829-2008, 8, *IEEE Standard for Software and System Test Documentation*

73. Limerick Generating Station, Document *TBD*, *Project Plan for Limerick Plant Protection System Modernization*

74. Nuclear Regulatory Commission, NUREG 0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition*

75. Nuclear Regulatory Commission, Regulatory Guide 1.173, Rev. 1, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

76. Nuclear Regulatory Commission, NUREG-1433, Rev. 4, *Standard Technical Specifications – General Electric BWR/4 Plants*, Volume 1, Specifications.

77. Technical Specifications Task Force, TSTF-GG-05-01, *Writer's Guide for Plant-Specific Improved Technical Specifications*

Appendix D

Research Decision Matrix

Appendix D
Research Decision Matrix

Introductory Notes:

When developing a design concept to replace nuclear plant instrumentation and control (I&C) systems, the research team must consider all the existing design bases, requirements, constraints, and regulatory commitments. The team must also consider other items such as (but not limited to): the technical, programmatic, and economic objectives driving the I&C upgrade; the as-built condition of the units being upgraded; upgrade physical boundaries and interfaces; perceived technical and regulatory risks; technologies available to support the upgrade; and methods to integrate the upgrade with the rest of the target unit. In such a dynamic environment, the design team must balance all these items. Decisions must be made based upon the team's knowledge and experience to provide direction.

Decisions of this nature are necessarily utility and unit specific. For this research effort, Exelon Generation's Limerick Generating Station (LGS) was chosen as the basis facility on which first echelon safety-related I&C upgrade research would be conducted. The Research Decision Matrix provided in this Appendix captures a snapshot of decisions that the research team made in order to produce the vendor-independent functional requirement baselines (Appendices A and B) and the LAR Framework Document (Appendix C). Research Decisions captured herein were discussed during meetings with the resulting disposition documented to support the direction to be pursued by the research.

This Research Decision Matrix is, of necessity, a snapshot of a working document. Research decisions documented below may be changed by users of this appendix as a design progresses, as more information is gathered, or as needs dictate. Additional decisions will also need to be made and documented throughout the entire effort to bring the identified upgrades to completion.

Utilities leveraging the results of this research need to be aware of the research decisions made by the research team, because they directly impact the vendor-independent functional requirement design baselines and the LAR Framework Document produced by this research. Utilities will need to critically evaluate whether or not the decisions made by the research team meet particular utility objectives and their particular unit's needs. It is expected that utilities will need to either tailor the decisions captured below or make new decisions as their situation dictates. This will drive the need to assess the functional requirement baselines and the LAR Framework Document for impacts.

When creating this appendix, other columns were used for status tracking (e.g. open/closed) and for assigning responsibility and due dates for the tracking and disposition of issues, which required decisions. The addition of such columns is recommended when using this tool as a working document. These were removed from the table below to promote readability.

Research decisions captured in this matrix are intended to be tracked going forward to design/regulatory artifacts, which provide a basis for each decision. Several research decisions and resolutions captured in the matrix identify sections in the LAR Framework document where they are addressed. Going forward, an effort to more formally track this traceability is recommended.

The LWRS Program appreciates the research support provided by Exelon Generation. This Decision Matrix makes no commitments for Exelon Generation.

Acronyms:

Acronym	Definition	Acronym	Definition
1oo1	One-out-of-One (Voting)	EPM	Electric Power Monitor
1oo2	One-out-of-Two (Voting)	FIC	Flow Indicating Controller
2oo2	Two-out-of-Two (Voting)	FSAR	Final Safety Analysis Report
2oo3	Two-out-of-Three (Voting)	GE	General Electric
2oo4	Two-out-of-Four (Voting)	HPCI	High Pressure Coolant Injection
3oo3	Three-out-of-Three (Voting)	HSI	Human-System Interface
4oo4	Four-out-of-Four (Voting)	I/O	Input / Output
10 CFR 50.59	Title 10 of the Code of Federal Regulation, Part 50, Energy, Section 59	I&C	Instrumentation and Controls
ADS	Automatic Depressurization System	IEEE	Institute of Electrical and Electronics Engineers
APRM	Average Power Range (Neutron) Monitor	IRM	Intermediate Range (Neutron) Monitor
ATWS	Anticipated Transient Without Scram	ISG	Interim Staff Guidance
BISI	Bypassed Indication and Status Indication	LAR	License Amendment Request
CCF	Common Cause Failure	LGS	Limerick Generating Station Units 1 and 2
CBA	Cost-Benefit Analysis	LPCI	Low Pressure Coolant Injection
ConOps	Concept of Operations	LWRS	Light Water Reactor Sustainability Program
D3	Defense-in-Depth and Diversity	MSIV	Main Steam Isolation Valve
DAS	Diverse Actuation System (not a system, but a function running in DCS)	N4S	Nuclear Steam Supply Shutoff System
DCS	Distributed Control System	NRC	United States Nuclear Regulatory Commission
DI&C-ISG-04	Digital Instrumentation and Controls Interim Staff Guidance 4, Revision 1	OPRM	Oscillation Power Range (Neutron) Monitor
DKT	Display, Keyboard, Trackball	O&M	Operations & Maintenance
ECCS	Emergency Core Cooling System	PAMS	Post Accident Monitoring System
EDG	Emergency Diesel Generator	PPS	Plant Protection System
EIM	Equipment Interface Module	RCIC	Reactor Core Isolation Cooling

Acronym	Definition	Acronym	Definition
RG	Regulatory Guideline	SE	Safety Evaluation (Report, by the NRC)
RHR	Residual Heat Removal	SLC(S)	Standby Liquid Control (System)
RO	Reactor Operator	SOE	Sequence of Events (secure operating environment – not used)
RPS	Reactor Protection System	SOV	Solenoid Operated Valve
RRCS	Redundant Reactivity Control System	SRM	Source Range (Neutron) Monitor
RSP	Remote Shutdown Panel	SRO	Senior Reactor Operator
scram	Rapid Shutdown (Reactor Trip)	UFSAR	Updated Final Safety Analysis Report
SDOE	Secure Development and Operational Environment	WCAP	Westinghouse Commercial Atomic Power (letter designator)

Research Decision Matrix:

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
1. The existing consensus standards included in the Limerick licensing basis do not reflect the resolution of various issues that IEEE NPEC committees have resolved in current, consensus standards.	Based on the Limerick UFSAR, Limerick is licensed to: IEEE Std. 279-1971; IEEE Std. 308-1971 and -1974; IEEE Std. 317-1972; IEEE Std. 323-1971; IEEE Std. 336-1971; IEEE Std. 338-1971, -1975, and -1977; IEEE Std. 344-1971 and -1975; IEEE Std. 379-1972 and -1977; IEEE Std. 382-1972; IEEE Std. 383-1974; and IEEE Std. 384-1974 and -1977. These standards are not sufficient or appropriate for modern digital systems. We need to use a licensing basis for the logic solvers in the four systems (RPS, N4S, ECCS, and RCCS) to be pursued initially that is appropriate for modern equipment. However, we do not wish to disturb the existing field wiring terminations in the RPS, N4S, ECCS, or RCCS cabinets to provide the separation required in modern standards. Further, the vendors and NRC have evaluated the prequalified equipment to current endorsed standards. We need to install the equipment in accordance with the standards against which the NRC evaluated and accepted the prequalified platforms.	a. This LAR does not change the plant licensing basis. However, within the limitations imposed by the existing field wiring at the input and output terminations within the RPS, N4S, ECCS, and RRCS cabinets, Limerick will comply with modern IEEE standards. Limerick will implement these systems in compliance with modern IEEE standards, whether endorsed by the NRC or not. These standards include, but are not limited to, IEEE Stds. 603-1991 and -2018; 7-4.3.2-2003, with additional clauses from 7-4.3.2-2016; 379-2014; 384-2018; and IEC/IEEE 60780/323-2016. b. If additional field wiring outside the cabinets is required (e.g., to new sensors), it will follow current separation requirements for the station. c. To the extent practicable, Limerick will separate the system wiring attached to the input and output terminations, based on the limitations present in the field wiring terminations. Limerick will comply with the fiber optic cable separation defined in informative Annex C of IEEE Std. 384-2018. d. IEEE Std. 338-2018 provides guidance for the types of testing previously required, but this LAR considers the rationale for the requirements in IEEE Std. 338 and eliminates an appropriate choice of channel functional tests, instrument channel checks, and the logic solver portion of channel calibration, based on the capabilities of the system.	Execute Resolution at left. Licensing approach supports envisioned architecture. Minimizes impact to field wiring. This drives cost affordability. This is a critical design attribute.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
1(a). Requirements for Diverse Actuation System for safety systems.	Since the NRC has requirements for defense-in-depth and since the RPS, N4S, and ECCS are critical to safety, some means is likely required to provide a backup for these functions for the digital PPS, which was not required with an analog system. This should not be implemented as a separate system.	A separate Diverse Actuation System (DAS) is not provided in this design concept. Rather, the DAS function is provided as a segmented function in the non-safety related plantwide Distributed Control System (DCS). A Defense-in-Depth and Diversity (D3) Analysis will be performed to determine the N4S and ECCS functions that are required to be duplicated in the DAS. Our evaluation concludes that the ATWS function provides a sufficiently diverse implementation of the RPS functions, which is required by 10 CFR 50.62 and the LGS license. Thus, the ATWS function will also be incorporated into the DAS function in the DCS just as another DCS function.	The concept of DAS, as a function in the DCS, is accepted. All mention of DAS in this Decision Matrix is based on this idea, without restating the idea in each decision.
2. Capturing Sequence of Events (SOE) data in the safety systems would result in an increased complexity in those systems and would not serve a safety function.	SOE data is extremely important to analyze transient and trip behavior. Data from the safety systems can provide the only source of data for useful insights.	The safety systems shall provide fast acting (e.g., reed relay) dry contact outputs for SOE capture by SOE cards in the standard DCS. Efforts shall be made in design and implementation to ensure that the delay from the logic in the system through the contact change of state is minimized and deterministic (i.e., fixed and non-varying). The project team needs Exelon to define the RPS, N4S, ECCS, and RRCS signals to be monitored for SOE purposes.	No known system with an NRC SE Report provides SOE and the time stamped function. SOE will be provided by non-safety DCS with SOE inputs from appropriately isolated safety-related PPS. This is the minimum cost solution that provides functionality.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
3. Several regulatory guidance documents mandate that data be continuously visible, and the regulator has not accepted continuously available as an acceptable substitute.	The glass cockpit envisioned eliminates, to the extent practicable, separate meters, recorders, and indicator lamps. These have been the methods used for "continuously visible" in the existing analog control rooms. We do not want to dedicate video display units to the continuous display, but we want to comply with the requirement.	The administrative procedures under which the plant operates shall be extended (in the future) to a requirement to choose one or more displays and always have the "continuously visible" parameters on a display, of which the watchstanding operators are cognizant. This administrative requirement resolves the "continuously visible" regulatory requirement without changing the wording to "continuously available." Nothing we are doing with the four systems of interest or the LAR would preclude this operation. The post-accident monitoring system (PAMS) does not need to be on a diverse platform. The PPS displays provide sufficient capabilities for safety-related variables. The DCS displays also provide safety-related information, along with future non-safety related plant information.	Enables glass cockpit concept in direct support of ConOps. Best executed with DKT Switch concept.
3(a) BISI.	Along with the glass cockpit, we need to consider the Bypassed Indicators and Status Indicators (BISI) as continuously visible displays.	The project team needs Exelon to define the current BISI indicators in the control room. The project team needs Exelon to define the additional items to be added to BISI (e.g., maintenance bypasses for channels). We need select a technology for BISI sensing and display, preferably non-safety related data network.	Enables glass cockpit concept in direct support of ConOps. Best executed with DKT Switch concept.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
4. Surveillance testing and calibration are manual operations and require large resource investments.	We should be able to eliminate a large part of the surveillance testing and calibration by documenting how the internal self-tests and self-diagnostics supplied with the platform cover the likely faults and failures in the new system, considering the faults and failures uncovered by surveillance testing on the current system. The application programming may be required to provide additional support. The current assumptions regarding percent-reduction of surveillance testing field time in the CBA: • Channel Checks: 100% elimination • Channel Functional Tests: 100% elimination • Calibration/Functional Tests: 75% elimination • Logic System Functional Tests: 90% elimination • Response Time Testing: 85% elimination There are some instances where these rules of thumb will not apply. These assumptions are consistent with ongoing licensing activities at Vogtle 3 and 4 that may set precedent for the LGS modifications.	Update the Tech Specs and Tech Spec Bases to reflect the elimination of many manual operations by automation. Using data from the Cost/Benefit Analysis and data from the selected vendor's topical report, determine which surveillance tests and calibrations can be eliminated and which can be extended.	Critical attribute to support O&M cost reductions. Resolution at left accepted.
4(a). Analytics of digital sensor data used to minimize calibrations.	Sensor calibrations are based upon a calendar date require inordinate resources to perform.	Safety-related digital platform functional requirements baselines, and LAR Framework Document require that all sensor data be provided digitally to the non-safety system. This will support future analytics to identify calibration issues so that calibrations are only performed when necessary. Provide what is believed to be sufficient data to DCS where analytics application is expected to be hosted.	Research industry initiatives (e.g. LWRS research, Analysis and Measurement Services Corporation activities in this area, etc.). Disposition in same manner as #5 below.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
4(b). Analytics of field switches.	Field switches are difficult to calibrate and exhibit latent failure modes.	Replacing switches with transmitters and using analytics together could address both issues. Not incorporated in current project.	No new transmitters to be added for this purpose.
4(c). Analytics and elimination of redundant sets of safety-related transmitters.	Eliminate replicated transmitters used to support the separate trains of RPS, ECCS, N4S.	Eliminate sampling of identical sets of four-way redundant transmitters and use one set of redundant transmitters to feed all RPS, N4S, and ECCS functions in the PPS. Transmitters to be dispositioned in separate project. Future application of analytics is supported by this architecture, which may further support reductions in calibration frequency. A preliminary list of transmitters provided in the Cost/Benefit Analysis. Deletions to be finalized during detailed design.	Licensing accepts path forward as minimal licensing risk.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
4(d). Surveillance Testing of Logic.	New divisionalized safety systems (4 channels/4 divisions/2oo4) voting vs the current system of 4 channels × 3 systems with 1oo2 taken twice). Consolidate 12 channels into 4.	In the modernized system, when one channel is placed in maintenance bypass, the divisions will automatically implement a reduction in voting requirements occurs (e.g., 2oo4 reduced to two-out-of-three (2oo3) voting) within each division. If another channel fails, the divisions will further reduce the voting requirements (e.g., 2oo4 reduced to 2oo3 for maintenance bypass, then reduced to 2oo2 on failure of another channel). If insufficient channels remain in service (e.g., one or two channels of the original four, no channels for a 1oo2 voting), the PPS will scram or actuate both divisions. Similar actions will occur if there are only two channels providing data to multiple divisions, voting either 1oo2 or 2oo2. If one of the channels is in maintenance bypass, the divisions will drop to 1oo1 voting. If the remaining channel fails, the division will actuate. For the case where 4oo4 voting will be used, while one channel is in maintenance bypass, a four-channel function with multiple divisions will continue to operate, with a reduction in voting requirements (e.g., 4oo4 reduced to 3oo3). If another channel fails, the division will further reduce the voting requirements (e.g., 4oo4 reduced to 3oo3 for maintenance bypass, and then reduced to 2oo2 on failure of another channel). In 4oo4 voting, if one channel or no channels remain, the PPS will actuate.	New architecture as proposed at left accepted.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
5. Channel checks are manual operations and require two hours of effort every shift.	We should be able to replace the manual channel checks with automation on the non-safety DCS platform. The current assumption in the CBA is that the function called "channel checks" will be eliminated from the Tech. Specs, by leveraging platform capabilities described in this line item. There will be no need for printing or signing reports. The non-safety related comparison and alarming will remain, with the understanding that the data will be placed in a long-term historian, along with alarms. This is consistent with the Vogtle Units 3/4 LAR and the forthcoming WCAP which eliminates Channel Checks as a surveillance entirely.	Provide the channel-specific PPS and DAS data to non-safety DCS and write non-safety related application software to compare each of the channels and alarm on persistent mismatches outside the calibration acceptance bands of each type of input (e.g., wide range reactor pressure, narrow range reactor water level). The project team will establish data lists as part of system design. Exelon to decide how this will be accomplished in the existing (or new) non-safety related data network.	Reduces workload. Digital data capture facilitates this capability. Resolution accepted.
6. The regulatory requirement exists that instruments and controls are available in the control room to allow the operator to shut down and maintain the reactor in a cold shutdown condition (or lesser state).	The glass cockpit envisioned eliminates, to the extent practicable, separate meters, recorders, indicator lamps, and manual controls. While the glass cockpit would like to eliminate all these features, there are regulatory requirements for sufficient indication and control for maintaining situational awareness and controlling the plant with a failed safety system, which would eliminate video displays and soft controls.	We see no regulatory or technical reason that DKTs cannot be credited for PAMS. There is no requirement for diversity in RG 1.97 Rev. 2. In a future modernization, non-safety related parameters can be displayed on the DCS. As required, the DKTs have access to the modernized control system data. The D3 Analysis may require additional actuation capabilities through a DAS function operating in the non-safety related DCS.	Resolution accepted.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
6(a).	Minimal dedicated indications and hardwired controls must be identified and required locations sited. What is the minimum required physical switches required by regulation? What is the bounding requirement?	The FSAR Chapter 7 and Regulation require the following manual actuations, which shall not be dependent on the digital equipment to implement. • RPS Trip – will be provided to disable power to the rod control actuation groups • RRCS Trip – will be provided in a separate project that initiates the ATWS portion of the DAS • Turbine Trip – is provided by separate logic, not included in the PPS scope • APRM Bypass – is provided by the existing Nuclear Instrumentation and will not be affected by PPS replacement. D3 analysis will confirm that the minimum required physical switches have been identified.	See item #30 below.
6(b).	Remote shutdown panels (RSP) are distributed throughout the Limerick Plant.	During detailed design of the modification, ensure that the modification does not disable any function performed by the remote shutdown panel. Determine, during detailed design, how much of the RSP must be tested to confirm RSP still works.	RSP is not in scope and not part of this project. RSP functionality will be unchanged and not affected by this modernization, which will be a guiding principle for detailed design.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
7. Evaluation of the RPS voting scheme is required. GE transitioned to 2oo4 for the ABWR, similar to the voting scheme used by the other PWR NSSS vendors.	In the RPS (and potentially in other systems), the 1oo2 voting scheme has several issues, not the least of which are the false half scrams, where only one channel determines that a scram is required, and the failure to scram when only two channels in one division vote to scram.	Change the voting scheme to 2oo4 in the RPS divisions for the actuations. Change nothing past the field output terminations, leaving the requirement for both SOVs to open to dump air (i.e., retaining the in-field confirmation). Field equipment wiring and field equipment "voting" is unchanged.	Resolution accepted. Also, see item #4(d) above.
8. We need to determine the methods to be used to address the different voting schemes in N4S and ECCS.	N4S has 2oo2 taken once for MSIVs, 1oo2 taken once for certain valves, 1oo1 for other valves. Could we apply a new scheme for all valves within scope? Would that violate any current design requirements? We first need to define what N4S is, the scope we will tackle, and then consider voting. The goal is to produce a scheme that is at least as reliable as the existing system. We do not intend to change field wiring.	See Response to #4(d) above and LAR Framework Sections 3.3.1 and 3.3.4. Retain the N4S architecture where an individual channel/division isolates the inboard and another channel/division isolates the outboard valve, retaining the existing assignments to electrical divisions. Maintain the current ECCS architecture. This is driven by the constraint to not add additional field equipment.	Where possible, implement 2oo4 logic, otherwise, maintain current design. Do not add more field inputs in an attempt to "improve" voting schemes.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
9. Determine whether requiring both RPS divisions to scram is reasonable and meets the single-failure criterion.	In the RPS (and potentially in other systems), the 1oo2 taken twice voting scheme has several issues. The current design requires both RPS divisions to actuate to generate the scram. The RPS does provide both solenoid valves on the control rod drive mechanisms and solenoid valves on the air headers, either of which can cause the scram. If either does not actuate, then either manual operator action or the automatic action in the RRCS is responsible for the scram. This is the currently licensed design.	Consider the current RPS design and determine what should be done to implement the single-failure criterion within channels and divisions. Single-failure tolerant discrete outputs added to the PPS for outputs that scram, isolate, or actuate, which provides what we conclude is sufficient to meet the existing expectations for other nuclear systems with 4 divisions in current designs systems. Voting logic is discussed in other decision rows. As part of detailed design, consider channel-level, division-level, and train-level single-point vulnerability studies.	Maintain existing licensed trips functions. Improve trip logic consistent with #7 above to provide intended trips and minimize erroneous trips. Match original functions, using existing field sensing and actuations, keeping the in-field configurations.
10. Data and status communication must be as reliable as possible.	There are several issues identified in DI&C-ISG-04, Section 1, (specifically Item 12) that can be resolved using the information and requirements provided in that section.	Implement guidance in DI&C-ISG-04 Rev. 1 Section 1, “Interdivisional Communications,” with specific emphasis on the “black channel” communications requirements listed in DI&C-ISG-04 Section 1, Item 12. Addressed in functional requirements baseline documents and LAR Framework Document Sections 3.3.5 and 3.4.1	Expect vendor topical reports to address this. Final result must be captured in FR and LAR Framework.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
11. Video displays in the main control room need to be defined.	The distributed DKT switch-based concept offers several advantages since operators can move display functions easily to various locations in the control room.	The LAR Framework proposes a method to ensure that the SRO cannot be “at the controls” with Human System Interfaces (HSI) that have command and control capabilities. Using the switched DKT approach for the primary HSI enables an incremental approach to a modern control room. This approach supports the movement of functions within the control room by switching the display to a different DKT Interface or repurposing individual DKTs as needed, rather than cutting and patching steel control room cabinets to physically remove and reinstall HSIs in other locations. Other approaches are equally acceptable, as long as the incremental capabilities of the switched DKT approach are incorporated. The DKT capabilities will have to be commercial-grade dedicated. Either the selected safety system vendor can perform the dedication, or a trusted third-party dedicator can perform the dedication.	The LWRS and MPR staff conclude that the DKT switch capabilities are desirable. At a minimum this feature should be designed for future integration.
11(a). Video displays in the main control room need to be defined.	DKTs need to exist to support soft controls for the RO.	The LAR Framework concludes that a primary display should be provided for each channel. Since there are usually two channels in division, one of the channel displays should also serve the division to which the channel is attached. In the N4S, there are some subdivided divisions, which would be assigned to the channel to which the subdivided division is attached. To meet the single-failure criterion, a redundant DKT is required for each of the channel/division DKTs. If the switched DKT concept is used, the requirement for redundant DKTs is satisfied by the other control room DKTs.	The switched DKT concept is incorporated in the LAR Framework and the PPS functional requirements. Further exploration of the concept will occur during detailed design, which includes Human Factors Engineering.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
12. Video displays in the main control room need to be defined.	If the DKT concept is adopted, we need to consider the DI&C-ISG-04 regulatory issues with using non-safety related displays to issue commands to safety functions, considering that non-safety displays issuing commands to safety systems become multidivisional displays and the general guidance of DI&C-ISG-04 Section 3 applies, as does the detailed guidance in Sections 3.1 and 3.2.	The safety-related DKT switch architecture is described in the LAR Framework Document Section 3.3.5 and 3.4.5. This addresses the DI&C-ISG-04 regulatory issues with using non-safety related displays to issue commands to safety functions, A pair of safety-related DKT Switches (Division A and Division B, divisionally powered) was chosen. Continuous visibility licensing discussion provided in LAR Framework Sections 3.1.2 and 3.3.5. The detailed design process must evaluate the installed system cyber security and SDOE at the DKT vendor. From a CCF view, the software in the DKT will need to be evaluated for CCF.	With precedent established, Exelon licensing is not opposed. Details with regard to cyber, CCF, and continuously visible vs. continuously available data display need to be established.
13. Video displays in the main control room need to be defined.	If all displays are on the DKT Switch network, commands from the video displays are limited, and it will be difficult to convince the regulator that faults and failure in the DKT Switch and non-safety related video displays are unlikely (i.e., common-cause failure).	The LAR Framework demonstrates that the safety-related DKT architecture is not a multidivisional display as envisioned in DI&C-ISG-04 Section 3. The preference is for all displays to be serviced by the DKT Switch architecture.	With precedent established, Exelon licensing is not opposed. Details with regard to cyber, CCF, and continuously visible vs. continuously available data display need to be established.
14. Video displays and LAR.	The LAR Framework needs to contain a sufficiently complete version of the systems. It has been suggested that the video and video network not be included in the LAR Framework and implemented in a separate 10 CFR 50.59 evaluation. It is not clear whether the NRC will have issues with this split.	The HMI methodology needs to be presented as part of the safety-related upgrade effort, including how the modernization ultimately supports a largely glass control room concept. The concept needs to be licensable, sufficiently described, and consistent with DI&C-ISG-04. The DKT switch concept is captured in the LAR Framework Document, Sections 3.3.5 and 3.4.5.	With precedent established, Exelon licensing is not opposed. Details with regard to cyber, CCF, and continuously visible vs. continuously available data display need to be established.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
15. ECCS consists of many subsystems.	It is not yet clear what subsystems are considered part of the current ECCS scope. How are closed loop flow control, closed loop speed control, and overspeed protection accomplished for HPCI and RCIC? Should the Flow Indicating Controllers (FICs) for these systems be included within the scope of the proposed modification? Should HPCI and RCIC pressure control also be included as part of the digital modernization to support Emergency Operating Procedure execution? Is RCIC in scope because of its physical proximity? What other items fall into this category? The safeguards switchgear (4.16 kV) bus instrumentation is currently part of the ECCS LGS Technical Specifications. Determine whether these functions are in the scope of this modification or should bus protection and EDG load sequencing be addressed in a separate modification.	ECCS subsystems are captured in the functional requirements baseline documents and the LAR Framework Document. The systems are HPCI, RHR in LPCI mode, ADS, and Core Spray. The engineered safety features initiate RCIC. The HPCI and RCIC controls are currently part of this scope. Diesel initiation is also part of the Core Spray scope. The systems are: • ECCS – proper • HPCI • ADS • Core Spray (diesel relay logic included) • RHR/LPCI • RCIC • RHR – Remaining The scope was later augmented to automate significant parts of the manual RHR configuration, to reduce the potential for human performance errors, as documented in LAR Framework Section 3.4.4.	Systems agreed upon and scope incorporated in LAR and functional requirements baseline documents.
16. N4S interacts many subsystems.	It is not yet clear what functions are considered part of the current N4S scope. N4S is required to execute a number of functions, which are organized by system (Function 1 [a-f] affects main steam, Function 2 affects RHR [shutdown cooling mode], Function 3 affects reactor water cleanup, etc.). We assume all functions will be in scope.	Clearly define and document the N4S subsystems that are in this project's scope. Functions identified and incorporated in LAR Framework Section 3.2.2 and functional requirements baseline documents.	N4S subsystems have been agreed to.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
16(a).	With the decision to implement the RPS and only that portion of N4S that is implemented in the RPS/N4S cabinets as Project 1 and the remainder of the N4S and ECCS as Project 2 define a clear interface that will provide a bridging strategy between Project 1 and the next outage where Project 2 is installed. The interface is likely to require discrete outputs from the digital PPS to the remaining N4S and ECCS, which would be installed in Project 1 and removed in Project 2.	To be determined by Exelon and their selected vendor during the conforming of the PPS Functional Requirements Baseline Document and the LAR Framework Document to the vendor's prequalified platform design.	Feasibility of implementation as described in the problem statement will be best determined through collaboration between Exelon and their selected vendor.
17. RRCS is classified as a safety system, with four channels and two divisions.	Modify the RRCS design to a highly reliable, non-safety related design. Keep the four sets of inputs but combine channel and division functions into a single level of application software, running in a single (redundant) processor.	Clearly define the RRCS design as implemented on the non-safety DCS as a redundant, 2oo4 division voting scheme for trips. Ensure that the trip outputs are single-failure proof. 2oo4 would allow for maintenance online.	Engineering team agrees with the resolution at left.
17(a).	RRCS current functionality includes logic to run back all the feed pumps. This "feature" is not required in regulatory space (10 CFR 50.62). This "feature" has the potential to cause unintended operational upset.	Remove this function from RRCS based on Operating Experience review and 10 CFR 50.62.	Engineering team agrees with the resolution at left.
18. The training materials for the RPS list a set of jumpers to remove to trip on any single nuclear instrumentation trip.	Does this single input trip still need to exist in the final design, or can/should this "startup" related trip be eliminated from the design? Is there any currently envisioned use for this function? Are shorting links still the most appropriate method for instantiating this trip?	Exelon has determined that the plant no longer performs this test, so the modernization project should not include this noncoincident trip. Exelon personnel indicate that strongest rod-out determinations are made analytically, eliminating the need for the function disabled by the shorting links for empirical strongest rod-out testing. Therefore, do not incorporate this functionality in the replacement system.	Engineering team agrees with the resolution at left. Eliminates cost to implement.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
19. Certain plant systems should never actuate unless required (e.g., automatic depressurization, standby liquid control [SLC]).	Outputs controlling the ADS and SLC (and potentially other equally potent systems) need to be designed to avoid the potential for a single hardware component failure to open valves, start pumps, or actuate squib valves.	One design consideration was to evaluate the ECCS and N4S systems individually to ensure that single hardware failures do not result in actuations. The LAR Framework and the functional requirements baseline documents require all outputs that cause scrams or actuations to be single-failure tolerant and diagnosed.	Current functionality needs to be mimicked in the new system with the single-failure criterion applied to each discrete output that causes scram, isolation, or actuation.
20. The fail-safe RPS outputs need to ensure that all RPS failures, including Software CCF, always result in the outputs going to the fail-safe state.	Failures that result in not initiating a half-scram block the ability of the RPS to initiate a scram.	Faults and failures in the selected vendor's RPS equipment must result in fail-safe actuation. The LAR Framework and the functional requirements baseline documents require all outputs that cause scrams or actuations to be single-failure tolerant.	Engineering team agrees with the resolution at left.
21. ATWS outputs will continue to be energized to trip or actuate.	Failures that result in not energizing the RRCS outputs would block the ability of the RRCS to perform any scram and shutdown actions.	Verify that the selected vendor's RRCS equipment has no single hardware failure modes that would result in failure to actuate. Verify that the selected vendor's RRCS equipment has no failure modes that would result in false actuation. 11(a). Verification of both of these requirements should consider the single-failure criterion. The LAR Framework and the functional requirements baseline documents require all outputs that cause scrams or actuations to be single-failure tolerant.	Engineering team agrees with the resolution at left.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
22. Normally, engineering safety features are assumed to be fail-as-is.	The N4S and ECCS outputs are level mode signals, so failure of N4S or ECCS hardware/software to the off state could result in turning off containment isolation in N4S functions or turning off running components in ECCS systems. N4S fails differently, depending on the function/group. Certain groups fail-safe and isolate. Groups related to HPCI and RCIC fail as-is (e.g., a power loss to the logic would not result in a half isolation for the steam supply valves).	Confirm that N4S and ECCS actions are licensed as fail-safe, fail-as-is, or fail-to-actuate, based on the safety function and the existing licensing basis, due to things such as logic or communication errors. The LAR Framework and the functional requirements baseline documents require all outputs that cause scrams or actuations to be single-failure tolerant. There are some ESF outputs that are energized to actuate, and others are deenergize to actuate. Current functionality will be duplicated in the new system. Incorporate in the LAR Framework and functional requirements baseline documents.	Current functionality needs to be duplicated in the new system.
23. The trending function of safety-related recorders is not safety-related. Determine if trending of safety-related data is a function of the non-safety system.	Determine the safety function of the recorders. If each recorder's safety function is to indicate values with non-safety related means of archiving data, the non-safety data network/DCS can implement the trending function. If the recorder's safety function is safety-related trending, the safety system is required to implement the trending function, which increases complexity, cost, and licensing risk.	Determine whether indication or trending is the part of the safety recorder licensing requirements. RG 1.97 Rev. 2 was reviewed, and no requirement was found for trending. If trending is required, trending of safety-related data can be provided by the non-safety related DCS, which has all PPS data in the DCS data historian.	There is no regulatory requirement for trending. As part of detailed design, determine if the license committed to data retention.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
24. Historical retention of plant data.	Strip chart recorder paper is the data document of record for historical retention at many plants. Using the electronic history from the data historian should replace this process, with electronic copies of the data preserved as historical records.	The licensing basis does not require historical retention of strip chart data. All data is transferred to the DCS and retained. Administrative procedure changes will be included in the Engineering Change package to support this transition. Data is provided to the DCS, and the DCS can, in future, be used to provide trending. No trending incorporated in the PPS.	As part of detailed design, determine what happens to recorder flash cards. As part of detailed design, examine record retention procedure with records management.
25. Instrumentation loop modifications.	Modification of instrumentation loops requires revisions to loop budget calculations, requires continuity testing, and could require drawings to be revised. The aggregate cost of such modifications is prohibitive.	As a rule, instrumentation loops will not be modified as part of this modernization so that loop calculations do not need to be reperformed. Exceptions may be required.	Engineering team agrees with the resolution at left.
26. PPS Nomenclature Changes.	Detailed system nomenclature for the new Plant Protection System needs to be established for this modification. New system nomenclature should be maintained where possible and when changes need to be explained.	Channels (bi-stable analog trip unit replacements) will be referred to as Channel A, B, C, and D, with instruments designed as “A” tied to Channel A only, “B” tied to Channel B, “C” tied to Channel C, and “D” tied to Channel D. Divisions (voters and logic) will be referred to as Divisions 1, 2, 3, and 4, to ensure differentiation. Division 1 will be powered from Electrical Bus A, Division 2 from Electrical Bus B, Division 3 from Electrical Bus C, and Division 4 from Electrical Bus D. All four channels and divisions retain their existing field power supply separations.	Engineering team agrees with the resolution at left.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
27. RPS Channel Bypass and Fail Logic.	The design team expects to install a maintenance bypass switch in the control room, which will allow the watchstanding operator to bypass only one RPS/N4S/ECCS channel and eliminate the potential for maintenance or calibration activities on that bypassed channel to cause a plant scram. Design considerations should include minimizing issues with separation. As an example, the bypass switch could be based on fiber optic sensing (since the switch feeds both electrical divisions) and designed to make it mechanically impossible to interrupt the fiber optic sensing for more than one channel at a time.	Maintenance bypass is a common feature on a 2oo4 voting protection system. Maintenance bypass for channels is incorporated in the LAR Framework and in the safety-related functional requirements baseline documents.	Engineering team agrees with the resolution at left. Licensing risk is low.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
28. RPS Channel Bypass and Fail Logic.	Normally, with all channels online and no channels in maintenance bypass, the RPS votes two-out-of-four (2oo4). Each RPS division reads the channel maintenance bypass selector switch and determines if the operator is requesting to bypass a channel. Each division independently makes this determination and provides the status to the external channel check. If the divisions are making different decisions, the channel check software alarms. If the other three channels are operable, the division allows the bypass (if the requested channel is inoperable, the division allows the bypass). If one channel is in maintenance bypass, the RPS votes two-out-of-three (2oo3). On detection of the failure of any channel, the divisions treat that channel as bypassed and do not allow maintenance bypass for any other channel. If a channel is maintenance bypass and another channel fails, the divisions transition to 1oo2 voting. If more than two channels fail, the divisions conservatively trip.	With the addition of maintenance bypass, a clearly stated set of requirements must exist for changing the voting scheme in bypass and in the presence of channel failure. While it is possible to set the bypassed channel to vote to trip or actuate, that condition seems overly conservative. The proposed path seems appropriately conservative but not excessive. If three or four channels have failed, something has gone drastically wrong and the conservative approach is to trip the plant. The LAR Framework and functional requirements baseline documents provide detailed descriptions of voting and the way voting changes with channel failure and channel bypass.	Engineering team agrees with the resolution at left. Licensing risk is low.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
29. Manual Trip and Reset Pushbuttons.	The existing architecture treats the manual pushbuttons as just another trip signal in the chain. When going to a modern RPS, the manual trips have to be relocated such that no software common cause failure can inhibit the operator's ability to trip the plant. The existing manual scram buttons are just another set of contacts in the relay logic for each channel and initiate a plant scram through both the primary and backup SOVs. In the existing system, pressing A1 or A2 initiates a half-scram in Division A and then pressing either B1 or B2 initiates a half-scram in Division B, which results in a plant trip.	Eliminate two of the four scram buttons based on precedent. Each button causes a half-scram. The buttons are duplicated as soft controls. In the extremely unlikely event that one button fails during a software common cause failure of the RPS, RRCS will provide an alternate means to scram. Divisional software reads and implements the reset pushbuttons functions in software. Divisional software implements the required timers. For an automatic scram, the Divisions start the reset timer as part of the logic. If the operator initiates a manual scram, the Divisions use the on/off state of the power applied to the groups of trip solenoid valves to initiate the reset timer, where any four of the four group trips associated with that division results in initiating the trip seal-in and the reset timer.	Engineering team agrees with the resolution at left.
29(a).	We have to consider the system behavior differences between the manual scram push buttons and moving the Reactor Mode switch from Run.	Incorporate the differences in the safety-related functional requirements baseline documents.	Engineering team agrees with the resolution at left.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
30. System Controls.	Many of the existing N4S and ECCS control switches are wired directly to the field-actuated components in addition to automatic control signals routed from the logic circuitry. Should this modification address the interface of control switches with field-actuated devices (e.g., breakers) or should it only address the automatic control circuitry interface with the field-actuated device? All control wiring for N4S and ECCS are located in two or three panels in MCR. Most of these should be something that can be revised with minimal impact.	Manual control switches will be limited to: (1) Those required to have direct interface to field devices (e.g., scram, turbine trip) (2) Those that provide spatially dedicated system level actuations for plant operational events (3) Others that are required or desired by operations (e.g., ADS Inhibit switches, SLCS Inhibit switches). For (2) and (3) above, these switches will provide digital inputs to the PPS, except the SLCS Inhibit switches, which are input to ATWS. The N4S and ECCS portions of the DAS design are not affected by this decision.	Engineering team agrees with the resolution at left.
30(a).	Manual control inputs could be routed through the new platforms as part of the digital modernization. The platform would then serve as the interface for all manual and automatic control of the field-actuated equipment. However, the scope of physical modifications associated with this option may be very large depending on the existing control wiring arrangements. This may also create problems with software common cause failure and preventing manual operations that are required by Operations procedures to respond to various casualties, so not all manual controls will be able to be routed through the logic solver.	The decision is to ensure that those manual controls that have to function in the presence of software common cause failure will not be routed through the logic. All other manual controls not covered by #6 or #30 above are replaced by soft controls.	Engineering team agrees with the resolution at left.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
31. Annunciator System.	The Plant Protection System supports the function to have outputs to the existing alarm annunciator system.	Proposed solution is to use 1E to non-1E one-way fiber optic communication links from the PPS to the DCS, which provide isolation and separation between the PPS and the DCS. The DCS provides discrete outputs to drive the existing annunciator system. This will allow further modernization for an alarm presentation system in the future. For SOE and first-out, relay outputs will be provided in the PPS that provide safety to non-safety related isolation. SOE data points will also be provided on the communication links to the DCS.	Engineering team agrees with the resolution at left.
32. Manual SCRAM Switches / Manual Actuation Switches.	Status input of the switches as inputs of the Plant Protection System. Monitor the state of the switches in the 1E platform.	Monitor the state of the remaining manual scram and actuation switches associated with the PPS to provide the required functionality within the PPS (e.g., 10 second reset lockout after scram initiated). Manual switches will have direct (or relay isolated, if necessary for power levels) means of disconnecting the power for the RPS scram solenoids.	Direct connection to scram solenoid. In series with PPS output. PPS to monitor status. See #30 above.
33. Perform automatic reactor level and pressure control during casualties for both HPCI and RCIC.	Current system does not provide level and pressure control.	Requires the addition of controls of turbine for pumps. Current system is manual, with an operator setting the flow rate through FICs. Eliminate the HPCI and RCIC FICs. Function of the FICs shall be migrated to PPS. Augmented control shall support flow, reactor pressure, and reactor water level control schemes, to support casualty control. Since the DAS function is likely to include RHR and RCIC, ensure that the function is included in the DAS. Ensure that a reliable method of switching between PPS and DAS analog outputs exist, if the HPCI and/or RCIC controls are required in the DAS function of the DCS.	Engineering team agrees with the resolution at left.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
33(b).	With a DAS, priority logic must be provided that is not subject to the PPS postulated software common cause failure.	Provide an appropriate Equipment Interface Module (EIM in the LAR Framework, safety-related functional requirements baseline document, and NSR functional requirements baseline document terminology) that provides the priority logic and discrete outputs necessary to control the plant equipment.	Engineering team agrees with the resolution at left.
34. Interface for non-1E system response for reactor SCRAM or RPS Actuation.	Current System has auxiliary contacts going to non-1E systems.	Maintain an isolation device that provides a discrete signal to non-1E systems to maintain current design functions (e.g., Feedwater run back on SCRAM). This feature could be migrated to the PPS digital data interface to the non-1E platform if this provides satisfactory time response. Response times for this interface shall be evaluated. Note that the example implementation provided above (Feedwater) is not currently implemented on DCS. Therefore, a discrete output for similar conditions is required. An increased I/O density is required. Additionally, the vendor shall provide an isolation device for 1E to non-1E isolation. Ensure data is provided via one-way data link for future integration and consideration on DCS.	Engineering team agrees with the resolution at left.
35. Nuclear Instrumentation output is currently bypassed by the NIs in Tech Specs.	Nuclear Instrumentation output is currently bypassed by the NIs in Tech Specs. Currently, RPS channels are not allowed to bypass NI inputs to RPS.	Bypass should be maintained in NIs. RPS Channel Bypass may be accomplished due to the NI output going to all four channels to maintain 2oo4 vote scheme. This avoids a half-scram condition on an NI voter failure. The LAR Framework and FR documents include the existing design. The LAR Framework also includes the TS actions to reflect this state.	Engineering team agrees with the resolution at left.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
36. Field component feedback (i.e., valve status, pump, motor status, etc.) on DKT.	Currently, lamps show component status in MCR. To support the movement from physical indicator to glass display, feedbacks shall be inputs to the safety platform and made available for presentation on DKTs.	All feedback shall be inputs to the safety platform. The safety platform shall also transmit the status to the DCS to maintain current functionality or enhance current functionality using a DCS vs. plant computer. Desired end state to move to a glasstop control room where safety-related component status is displayed on the DKT's. Interim state may have to maintain existing HMIs on the vertical control board. Describe desired end state to vendor in requirements.	Engineering team agrees with the resolution at left.
37. Reactor Mode Switch.	The Reactor Mode Switch is difficult to move, based on the large number of switches in this multideck switch. The project should plan to minimize the number of mode switch contacts, making the switch easier for the RO to operate.	While there is a potential to integrate replacing the existing switch decks on the Reactor Mode Switch with logic in the PPS, this has not been evaluated for licensing, especially for software common cause failure in the PPS having effects on other safety-related and non-safety related users of the existing contacts. This is currently not included in either the LAR Framework or the safety-related functional requirements baseline documents.	Exelon engineering and licensing to work with selected vendor to develop plan to migrate outputs as necessary.
38. NI Cross connect to RPS and align channel inputs.	The current design uses GE NUMAC voters to combine the discrete outputs of the Average Power and Oscillation Power Range Neutron Monitors (APRM and OPRM respectively). The Intermediate Range Neutron Monitors (IRMs) are provided as separate inputs, two IRMs to each channel. The NI voters include bypass capabilities and provide one redundant vote to the RPS that integrates all neutron monitoring information. As a result, the RPS only knows that some element of the neutron monitoring has voted to trip.	Exelon plans to upgrade to a Wide Range Neutron Monitor, which would replace the Source (SRM) and IRMs. There would still be eight monitors, which would drive the existing eight inputs that were driven by the IRMs. The APRM/OPRM voters remain unchanged. Since the SRMs trips have been permanently bypassed by Exelon, the SRMs will not be included in the PPS design.	Engineering team agrees with the resolution at left.

Issue	Problem Statement	Resolution	Engineering Team Disposition (Decision and Why)
39. Existing Electrical Power Monitors (EPMs).	The existing EPMs for each RPS division currently disconnect power from the complete RPS division. Disconnecting power from the PPS logic solvers is inappropriate and not required. With power disconnected, the RPS channels and divisions will all report failed, which is incorrect and would result solely from the EPM "protecting" the logic solvers.	The EPMs must be rewired (if retained) to disconnect, and thus protect, only the solenoid power. There is no reason, with the current design, to disconnect power from any portion of the PPS.	Detailed design will address this issue, but power to the logic solvers cannot be disconnected.