October 30, 2024

TP-LIC-LET-0356
Project Number 99902100

U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
ATTN: Document Control Desk

Subject: Transmittal of TerraPower, LLC Topical Report, "Instrumentation and Control Architecture and Design Basis Topical Report," Revision 2

References:

1. Transmittal of TerraPower, LLC Topical Report, "Instrumentation and Control Architecture and Design Basis Topical Report," Revision 1, March 7, 2024 (Accession No. ML24068A186)
2. TerraPower, LLC – Audit Plan for Topical Report "Instrumentation and Control Architecture and Design Basis Topical Report," Revision 1, June 24, 2024 (Accession No. ML24163A003)

This letter transmits the TerraPower, LLC (TerraPower) "Instrumentation and Control Architecture and Design Basis Topical Report", NAT-4950 Revision 2 (enclosed). The report contains an overview of the instrumentation and control (I&C) architecture and design basis for the Natrium® Plant[1] and a description of the methodology used to address common-cause failure (CCF) that is consistent with NRC SRM-SECY-22-0076, Staff Requirement-SECY-22-0076- Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems (ADAMS Accession No. ML23145A181). The revised report is provided to replace the information contained in Reference 1 with supplemental detail to address questions discussed during the NRC audit of the architecture and design basis (Reference 2) and includes other editorial revisions.

[1] Natrium is a TerraPower and GE-Hitachi technology.

TerraPower requests that the NRC provide a safety evaluation report (SER) on the Natrium I&C architecture and design basis.

The report contains proprietary information and as such, it is requested that Enclosure 3 be withheld from public disclosure in accordance with 10 CFR 2.390, "Public inspections, exemptions, requests for withholding." An affidavit certifying the basis for the request to withhold Enclosure 3 from public disclosure is included as Enclosure 1. Enclosure 3 also contains export controlled information (ECI) which can be disclosed to Foreign Nationals only in accordance with the requirements of 15 CFR 730 and 10 CFR 810, as applicable. Proprietary and ECI materials have been redacted from the report provided in Enclosure 2; redacted information is identified using [[ ]]$^{(a)(4)}$, [[ ]]^{ECI}, or [[ ]]$^{(a)(4),\ ECI}$.

This letter and enclosures make no new or revised regulatory commitments.

If you have any questions regarding this submittal, please contact Ian Gifford at igifford@terrapower.com or Nick Kellenberger at nkellenberger@terrapower.com.

Sincerely,

George Wilson

George Wilson
Vice President, Regulatory Affairs
TerraPower, LLC

Enclosures:
1. TerraPower, LLC Affidavit and Request for Withholding from Public Disclosure (10 CFR 2.390(a)(4))
2. TerraPower, LLC Topical Report, "Instrumentation and Control Architecture and Design Basis Topical Report," Revision 2 – Non-Proprietary (Public)
3. TerraPower, LLC, Topical Report, "Instrumentation and Control Architecture and Design Basis Topical Report," Revision 2 – Proprietary (Non-Public)

cc: Mallecia Sutton, NRC
Josh Borromeo, NRC
Nathan Howard, DOE
Jeff Ciocco, DOE

ENCLOSURE 1

TerraPower, LLC Affidavit and Request for Withholding from Public Disclosure (10 CFR 2.390(a)(4))

Enclosure 1
TerraPower, LLC Affidavit and Request for Withholding from Public Disclosure
(10 CFR 2.390(a)(4))

I, George Wilson, hereby state:

1. I am the Vice President, Regulatory Affairs and I have been authorized by TerraPower, LLC (TerraPower) to review information sought to be withheld from public disclosure in connection with the development, testing, licensing, and deployment of the Natrium® reactor and its associated fuel, structures, systems, and components, and to apply for its withholding from public disclosure on behalf of TerraPower.

2. The information sought to be withheld, in its entirety, is contained in Enclosure 3, which accompanies this Affidavit.

3. I am making this request for withholding, and executing this Affidavit as required by 10 CFR 2.390(b)(1).

4. I have personal knowledge of the criteria and procedures utilized by TerraPower in designating information as a trade secret, privileged, or as confidential commercial or financial information that would be protected from public disclosure under 10 CFR 2.390(a)(4).

5. The information contained in Enclosure 3 accompanying this Affidavit contains non-public details of the TerraPower regulatory and developmental strategies intended to support NRC staff review.

6. Pursuant to 10 CFR 2.390(b)(4), the following is furnished for consideration by the Commission in determining whether the information in Enclosure 3 should be withheld:

    a. The information has been held in confidence by TerraPower.

    b. The information is of a type customarily held in confidence by TerraPower and not customarily disclosed to the public. TerraPower has a rational basis for determining the types of information that it customarily holds in confidence and, in that connection, utilizes a system to determine when and whether to hold certain types of information in confidence. The application and substance of that system constitute TerraPower policy and provide the rational basis required.

    c. The information is being transmitted to the Commission in confidence and, under the provisions of 10 CFR 2.390, it is received in confidence by the Commission.

    d. This information is not available in public sources.

    e. TerraPower asserts that public disclosure of this non-public information is likely to cause substantial harm to the competitive position of TerraPower, because it would enhance the ability of competitors to provide similar products and services by reducing their expenditure of resources using similar project methods, equipment, testing approach, contractors, or licensing approaches.

I declare under penalty of perjury that the foregoing is true and correct.
Executed on: October 30, 2024

George Wilson
_____

George Wilson
Vice President, Regulatory Affairs
TerraPower, LLC

ENCLOSURE 2

TerraPower, LLC
"Instrumentation and Control Architecture and Design Basis Topical Report" Revision 2

Non-Proprietary (Public)

Document Title: Instrumentation & Control Architecture and Design Basis Topical Report				
Natrium Document No.: NAT-4950	**Rev. No.:** 2	**Page:** 1 of 48	**Doc Type:** RPRT	**Target Quality Level:** N/A
Alternate Document No.: N/A	**Alt. Rev.:** N/A	**Originating Organization:** TP / Engineering (ENG)		**Quality Level:** N/A
Natrium MSL ID: N/A	**Status:** Released			**Open Items?** N/A
Approval				
Approval signatures are captured and maintained electronically; see Electronic Approval Records in EDMS. Signatures or Facsimile of Electronic Approval Record attached to document.				

Not Confidential
Verify Current Revision

REVISION HISTORY

Revision No.	Affected Section(s)	Description of Change(s)
0	All	Initial release
1	4.1.1, 4.6.8, 6.2.2, Table 4-1, Table 6-1, Figure 5-1, Figure 6-1, Figure 6-5	- Updated ESF examples (Section 6.2.2) - Added note for AST (Table 4-1) - Added PSP Current Sensor (Table 6-1) - Type D variables changed from NSRTS to NST (Sections 4.1.1, 4.6.8, Figures 5-1 and 6-1 - Simplified RMS diagram (Figure 6-5)
2	3, 4, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.2, 4.4, 7.4.1, Figure 6-1	Incorporated changes based upon the NRC audit of the Topical Report. Updated Figure 6-1 to remove PAM Type D from RPS Div A (consistent with Rev 1 and the text)

Not Confidential
Verify Current Revision

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Acronyms and Abbreviations

Acronym / Abbreviation	Description
ADAMS	NRC Agencywide Documents Access and Management System
AMC	Auxiliary Monitoring and Control System
AOO	Anticipated Operational Occurrence (see NEI 18-04)
ARM	Area Radiation Monitoring
AST	Anticipatory Automatic Seismic Trip System
BDBE	Beyond Design Basis Event (see NEI 18-04)
CCF	Common Cause Failure
CDA	Critical Digital Assets
CPA	Construction Permit Application
CPS	Combined Plant Stack
CRA	Control Rod Assembly
CRD	Control Rod Drive System
CTC	Coolant Temperature Monitoring and Control System
DBA	Design Basis Accidents (see NEI 18-04)
DBE	Design Basis Event (see NEI 18-04)
DCS	Distributed Control System
DID	Defense-in-Depth
DRG	NRC Design Review Guide
DRMS	Digital Radiation Monitoring System
ERFB	Emergency Response Facility Backup
ERFP	Emergency Response Facility Primary
ERM	Effluent Radiation Monitor
ESF	Engineered Safety Features
F-C	Frequency-Consequence (see NEI 18-04)
FHC	Fuel Handling Supervisory Control System
FHCR	Fuel Handling Control Room
HFE	Human Factors Engineering
HMI	Human Machine Interface
HR	Heat Removal
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Controls
IAEA	International Atomic Energy Agency
IEEE	Institute of Electrical and Electronics Engineers
ISP	Intermediate Sodium Pump
LBE	Licensing Basis Events (see NEI 18-04)

LMP	Licensing Modernization Project
LWR	Light-Water-Reactor
MCR	Main Control Room
NEI	Nuclear Energy Institute
NI	Nuclear Island
NIC	Nuclear Island Control System
NRC	Nuclear Regulatory Commission
NSRST	Non-safety-related with Special Treatment
NST	Non-safety-related with no treatment
PAM	Post-Accident Monitoring
PDH	Plant Data Highway
PIE	Postulated Initiating Event
PMC	Plant Monitoring and Control System
PRA	Probabilistic Risk Assessment
PRM	Process Radiation Monitoring
PSAI	Plant-Specific Action Items
PSP	Primary Sodium Pump
RC	Reactivity Control
RE	Radiation Monitor
RIS	Reactor Instrumentation System
RMC	Rod Monitoring and Control System
RMS	Radiation Monitoring System
RPS	Reactor Protection System
RR	Radionuclide Retention
RSC	Remote Shutdown Complex
RSF	Required Safety Function
RTB	Reactor Trip Breaker
RWG	Gaseous Radwaste Processing System
RWL	Liquid Radwaste Processing System
RWS	Solid Radwaste Processing System
SCADA	Supervisory, Control and Data Acquisition
SCG	Sodium Cover Gas Systems
SOV	Solenoid Operated Valve
SPDS	Safety Parameter Display System
SR	Safety-Related
SSC	Structures, Systems, and Components
ST	Shunt trip
SVDU	Special Video Display Unit
ToR	Topical Report

UMC	Utility Monitoring and Control System
UV	Under Voltage
VDU	Visual Display Unit

1 PURPOSE

The purpose of the Natrium®[1] Instrumentation and Control (I&C) Architecture and Design Basis Topical Report (ToR) is to describe the overall architecture and associated design basis including compliance with Institute of Electrical and Electronics Engineers (IEEE) Std 603, and the process for:

- I&C relationship to plant-level lines of defense (Section 4.2, I&C Relationship to Plant-Level Lines of Defense).
- Structure, system, and component (SSC) classification (Section 4.3, Safety Classification Process)
- I&C functions basis and allocation to individual systems (Section 4.4, Function Allocation to I&C Systems).
- I&C functions basis and allocation to individual systems

The ToR also describes the following:

- I&C Integrated network (Section 5, Instrumentation and Control Integrated Network)
- Individual I&C systems (Section 6, Instrumentation and Control Systems)
- Application of fundamental design principles, simplicity, and diversity and defense-in-depth (DID) (Section 7, Fundamental I&C Design Principles, Simplicity, and Security).
- Secure I&C (Section 7.8, Secure I&C)

This ToR demonstrates that the Natrium I&C architecture meets applicable regulatory requirements and SRM-SECY-22-0076.

2 SCOPE

The Natrium I&C Architecture Topical Report addresses the I&C systems architecture and associated design basis information with a focus on the safety-related (SR) I&C systems, interfaces, and communication paths.

The scope of the report also includes:

- The industry standards and regulatory guidance related to I&C architecture.
- The NRC SRM-SECY-22-0076 (ADAMS Accession No. ML23145A181), Staff Requirement -SECY-22-0076 - Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems [1].
- Fundamental I&C design principles from the Nuclear Regulatory Commission (NRC) Design Review Guide (DRG): Instrumentation and Control for Non-Light-Water Reactor (Non-LWR) Reviews (ADAMS Accession No. ML21011A140) [2].

1 Natrium is a TerraPower and GE-Hitachi technology.

- The I&C functionality, safety classification, and plant-level functional requirements that are based on a risk-informed approach and application of diversity and DID principles consistent with the industry guidance Nuclear Energy Institute (NEI) 18-04, Risk-Informed Performance- Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development [3].

3 BACKGROUND

In recent years, the industry and the NRC started incorporating risk-informed decision-making into plant process and programs (e.g., maintenance and fire protection). Subsequently, NEI, under the umbrella of the Licensing Modernization Project (LMP), issued NEI 18-04, Revision 1, “Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development.” NEI 18-04 was subsequently endorsed by the NRC in Regulatory Guide 1.233 [4].

In lieu of the traditional safety classification of the systems and the digital D3 assessment, the Natrium power plant, uses NEI 18-04 to define the necessary DID at the plant level (including the I&C systems), SSC classification based on risk assessments, DID considerations, and expert panel reviews. The NEI 18-04 methodology is risk-informed and the outcome of the processes include identification of performance requirements.

In addition, the NRC issued SRM-SECY-22-0076 in 2023 to expand the policy in SECY-93-087 [5] to allow the use of risk-informed insights for digital systems D3 assessments. The SRM-SECY-22-0076 approach can be implemented using the NEI 18-04 methodology and the guidance in the DRG. In addition, the NRC DRG acknowledges use of the guidance described in NEI 18-04 for selecting and analyzing Licensing Basis Events (LBEs), classifying SSCs, and assessing DID that differs from traditional licensing approaches and terminology for LWRs. In addition, due to simplicity and inherent passive safety features of the Natrium power plant, there is less reliance on safety functions compared with traditional LWRs.

This ToR is primarily based on the NEI-18-04 methodology, the NRC DRG (2021 version), IEEE 603- 2018 [6], and the Commission guidance in SRM-SECY-22-0076.

4 INSTRUMENTATION AND CONTROL SYSTEMS OVERVIEW

The I&C includes systems that are classified as SR, non-safety-related with special treatment (NSRST), and non-safety-related with no special treatment (NST) as described in NEI 18-04. Important aspects of Natrium I&C architecture include:

- The Reactor Protection System (RPS) combines reactor scram and Engineered Safety Features (ESF) functions (ESF functions are very limited as compared to LWRs).
- Use of an NSRST power supply.
- Use of a digital protection system technology platform that addresses common cause failure (CCF) vulnerabilities using internal diversity features.
- Inclusion of cyber security features in the I&C architecture and system design.
- Simplicity of the RPS

There are five defense lines (DLs) described in Section 4.2. DL2, DL3, DL4 and DL5 functions rely on I&C systems. The RPS consisting of reactor scram and ESF is a SR system and credited in the DID Defense Line (DL3). DL3 relies on the SR I&C systems (RPS, XIS, RIS) functionality. The DID assessment is performed at the plant level including considerations for CCF.

The Curtiss-Wright RadICS platform used for the RPS has been accepted for use in SR I&C system applications by the NRC [7]. The RPS incorporates features of the approved RadICS platform to address CCF. As such, a diverse system is not needed to address CCF of the RPS actuation system; however, the plant level DID assessment assumes availability of manual reactor scram by RPS at Defense Line 4 (DL4), and certain NSRST and NST I&C functions provided by the Nuclear Island Control System (NIC).

I&C functions are defined by the plant-level DID assessment and assigned to I&C sub-systems. Simplicity is considered during I&C systems design and function allocation. Simplicity considerations include minimizing interactions between the SR and non-safety-related (NSRST and NST) systems (i.e., no priority module included in the design) and absence of inter-channel communications within the RPS (except for voting).

The NIC is classified as NSRST and primarily performs the NSRST and NST control functions. The NIC platform is selected to meet the project performance goals. Redundancy of NIC components and network, combined with special treatments, ensures the required reliability. Standalone systems that interface with NIC include, but are not limited to, the Radiation Monitoring System (RMS) and the local controllers included with fuel handling equipment that interface with the Fuel Handling Supervisory Control System (FHC).

The SR I&C systems do not require a Class 1E power supply to perform their required safety functions (RSFs). The power supply to the SR systems is classified as NSRST.

As required by NEI 18-04, NSRST systems (e.g., NIC) are subject to special treatment that includes requirements for reliability. The licensee or applicant referencing this ToR will provide special treatment details and the reliability targets.

The Natrium I&C includes cyber security features in the design to allow the plant to readily implement 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks [8], cyber security requirements and controls.

The preliminary outcome of the DID process (e.g., I&C functions list and DLs) is provided in this report to support overall understanding of the I&C architecture, systems, safety classification, and function allocation. The licensee or applicant referencing this ToR will provide the final version of the information noted as preliminary.

4.1 I&C Architecture Design Bases

The following sections provide I&C architecture compliance with regulatory requirements and conformance with regulatory guidance, industry codes, and standards used for development of the architecture. Additional requirements and guidance documents may be applicable to the individual I&C systems and will be described by the licensee or applicant referencing this ToR.

4.1.1 Code of Federal Regulations

The Natrium I&C architecture meets the following regulatory requirements, as applicable:

- 10 CFR 50.34(a)(3)(i), Principal Design Criteria for the facility.

The Natrium power plant adheres to the Natrium Principal Design Criteria. Refer to the Topical Report, “Principal Design Criteria for the Natrium Advanced Reactor,” (ADAMS Accession No. ML23024A281) [9].

- 10 CFR 50 Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.

TerraPower QA Program Description (QAPD), TP-QA-PD-0001 [10], implements the 10 CFR 50 Appendix B requirements.

- 10 CFR 50.55a, Codes and Standards.

The Natrium I&C use IEEE Std 603-2018 instead of IEEE Std 603-1991 [11] cited in 10 CFR 50.55(a)(h). However, the RadICS platform used for the RPS conforms with IEEE Std 603-1991. IEEE Std 603-2018 Clause 5.16, CCF, is addressed by the implementation of the risk-informed performance-based approach described in NEI 18-04 and SECY-22- 0076.

TerraPower has performed a comparison of the 1991 and 2018 versions of IEEE Std 603 and concludes that the 2018 version of IEEE Std 603 meets or exceeds the requirements of the version incorporated into 10 CFR 50.55a(h). Therefore, TerraPower can adopt IEEE Std 603-2018 for use without the need for an approved alternative and still demonstrate compliance with IEEE Std 603-1991.

- 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks.

The Natrium I&C architecture uses deterministic one-way communications devices or firewalls for communications with systems in lower security defensive levels to meet the cyber security defensive strategy. Licensee or applicant referencing this ToR will submit a separate cyber security plan as required by regulation.

4.1.2 Regulatory Guidance

The following section provides I&C architecture conformance with regulatory guidance used for the development of the architecture. In some cases, the RadICS platform adheres to earlier versions of the RGs or Codes and Standards.

Table 4-1: Regulatory Guidance

RG / DRG	Rev/Year	Title	Exceptions and Clarifications
1.53	2/2003	Application of the Single-Failure Criterion to Safety Systems	Natrium I&C uses IEEE 379-2014, IEEE 603-2018, and IEEE 7-4.3.2-2016
1.62	1/2010	Manual Initiation of Protective Actions	Manual initiation of scram and ESF functions is classified as NSRST

Not Confidential
Verify Current Revision

RG / DRG	Rev/Year	Title	Exceptions and Clarifications
1.75	3/2005	Physical Independence of Electric Systems	Natrium I&C uses IEEE 384-2018, and IEEE 603-2018 (RadICS uses IEEE 384-1992)
1.97	5/2019	Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants	Natrium I&C does not utilize SR power for Type B and C variables. Instead, Natrium I&C will ensure that reliable power with sufficient backup is provided for Post- Accident Monitoring (PAM) functions.
1.233	0/2020	Guidance for a Technologically Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors	
1.152	4/2023 & 3/2011	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants	RadICS uses RG 1.152 Revision 3
1.153	1/1996	Criteria for Safety Systems	Natrium I&C uses IEEE 603-2018 (RadICS uses IEEE 603-1991)
DRG	2021	Design Review Guide (DRG): Instrumentation and Controls for Non-Light-Water Reactor (Non-LWR) Reviews	The DRG is used as a guide for development of Natrium I&C architecture and this ToR

4.1.3 Industry Codes and Standards

The following section provides I&C architecture conformance with industry standards used for the development of the architecture.

Table 4-2: Industry Codes and Standards

Standard	Rev/ Year	Title	Natrium I&C Exceptions and Clarifications	RG Endorsement
ASME NQA- 1	2015	Quality Assurance Requirements for Nuclear Facility Applications	See TP QAPD TP-QA-PD-0001 (latest revision), TerraPower QA Program Description	10CFR50.55a, Codes and Standards and RG 1.28 Revision 5, Quality Assurance Program Criteria - Design and Construction
IEEE 379	2014	IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems	RadICS references IEEE 379-2000	
IEEE 384	2018	IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits		Not Endorsed. RadICS platform uses IEEE 384-1992 endorsed by RG 1.75 Revision 3, Criteria for Physical Independence of Electrical Safety Systems
IEEE 497	2016	IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations	Natrium I&C uses an NSRST power source (Type B, C, F variables requiring reliable power supply are NSRST). The risk-informed approach will be used as deemed necessary to meet the intent of IEEE 497.	RG 1.97 Revision 5, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants

Standard	Rev/ Year	Title	Natrium I&C Exceptions and Clarifications	RG Endorsement
IEEE 603	2018	IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations	Natrium I&C uses an NSRST power source. RadICS platform is based on 1991 version. CCF and DID for Natrium I&C is based on NEI 18- 04.	Not Endorsed: Latest versions currently incorporated in 50.55a(a)(2) is IEEE Std 603-1991
IEEE 7-4.3.2	2016	IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations	RadICS conforms to IEEE 7-4.3.2-2003 as endorsed by RG 1.152 Revision 3	RG 1.152 Revision 4

4.1.4 Guidance and Reports

The following section provides additional guidance and reports that were considered in the development of the I&C architecture as described in this report.

Table 4-3: NEI Guidance

Document / Report	Rev / Date	Title	Natrium I&C Exceptions and Clarifications	RG Endorsement
NEI 08-09	6/2010	Cyber Security Plan for Nuclear Power Reactors	Natrium is planning to use NEI 08-09 and Addendums	N/A
NEI 18-04	1/2019	Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light-Water Reactor Licensing Basis Development		RG 1.233

Not Confidential
Verify Current Revision

Document / Report	Rev / Date	Title	Natrium I&C Exceptions and Clarifications	RG Endorsement
SRM-SECY-22-0076	2023	Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems		N/A

4.2 I&C Relationship to Plant-Level Lines of Defense

I&C diversity and defense-in-depth is based on the overall plant PRA and DID analysis and leverages the RPS platform internal diversity that addresses CCF. Functions performed by the I&C systems are credited in different defense lines. DL3 safety functions are implemented in SR systems including the RPS. The DL2 and DL4 functions are performed by passive systems and NSRST and NST controls.

The defense-in-depth strategy evaluation outlines how the LBEs challenge each layer of DID, the functions and systems that respond to the challenges, and the state at which the event ends. The evaluation shows that no single layer, function, or feature is specifically relied upon to mitigate the postulated initiating event (PIE).

There are five layers of defense discussed in Table 5-2 of NEI 18-04 including the following and illustrated in Figure 4-1, Defense Line Concept:

1. Prevent off-normal operation and Anticipated Operational Occurrences (AOOs).
2. Control abnormal operation, detect failures, and prevent Design Basis Events (DBEs).
3. Control DBEs within the analyzed design basis conditions and prevent Beyond Design Basis Events (BDBEs).
4. Control severe plant conditions and mitigate consequences of BDBEs.
5. Deploy adequate offsite protective actions and prevent adverse impact on public health and safety.

For the Natrium project, a Postulated Initiating Event (PIE) is defined as an event capable of leading to AOOs or accident conditions.

PIEs and Initiating Events are generally similar in the sense that they involve a failure of some normal operating function. However, a PIE may not actually result in an Initiating Event if it does not result in a reactor trip. For that reason, a PIE may nominally appear as a "plant transient precursor" but with additional complications or failures that same PIE may lead to an LBE.

Within the topical report AOO, DBE, and BDBE are used to refer to the frequency of the PIE regardless of whether or not it actually causes a reactor trip. It is not associated with the initiator of a given AOO, DBE, or BDBE (except for the PIE itself with the uncomplicated plant response to the PIE).

For the Natrium power plant, the above layers are expanded on in detail to include the following:

The five DLs for the design provide protection against unacceptable releases of radiation. The DLs include programmatic elements, design features, and design functions. The first and fifth DLs include programmatic elements and design features, while the second, third, and fourth DLs include design functions.

The first DL (DL1) reduces the potential for PIEs to occur and for failures to occur in subsequent defense lines. This is achieved through application of programmatic elements and design features. The programmatic elements assure that quality, reliability, and conservatism are present in the design, construction, and operation of the plant. Design features reduce the likelihood of initiating events and help assure that equipment performing DL functions can be counted on to operate reliably.

The second, third, and fourth DLs (DL2, DL3, and DL4) include the design functions necessary to ensure performance of the fundamental safety functions, and therefore prevent PIEs from leading to unacceptable radioactive releases. A DL function of I&C includes both sensing of a signal to determine the need for the function (i.e., indication), if required, and actuation to complete the function.

The fifth defense line (DL5) involves offsite emergency preparedness to protect the public in case a substantial radioactive release occurs or is imminent.

Among DLs 2, 3, and 4, two independent and diverse (to the extent practical) defense lines can mitigate any AOO PIE.

Among DLs 2, 3, and 4, two independent and diverse (to the extent practical) defense lines can mitigate any DBE PIE other than PIEs caused by a CCF in another defense line, unless the PRA concludes that the frequency of the PIE combined with the additional failure is less than 5E-07 per plant year.

Among DLs 2, 3, and 4, at least one defense line can mitigate any DBE PIE caused by a CCF in DL2 or DL4, with the mitigation means being independent from the effects of the initiating CCF.

CCFs in DL3 and any BDBE PIEs can be mitigated by unaffected functions in any defense line.

Severe accidents with a frequency greater than 5E-07 per plant year can be mitigated by DL4 functions that are independent (to the extent practical) from DLs 2 and 3, and the DL4 functions used to back up DLs 2 and 3 and mitigate BDBE PIEs.

The DID evaluations utilize the layers list above in addition to utilizing the guidance listed in NEI 18-04 Tables 5-2 to 5-4. The following steps outlined in NEI 18-04 are used for evaluating LBEs for DID adequacy:

1. Confirm that plant capabilities for DID are deployed to prevent and mitigate each LBE at each layer of defense challenged by the LBE.
2. Confirm that a balance between event prevention and mitigation is reflected in the layers of defense for risk-significant LBEs.
3. Identify the reliability/availability missions of SSCs that perform prevention and mitigation functions along each LBE and confirm that these missions can be accomplished. A reliability/availability mission is the set of requirements related to the performance, reliability, and availability of an SSC

function that adequately ensures the accomplishment of its task, as defined by the PRA or deterministic analysis.

4. Confirm that adequate technical bases for classifying SSCs as SR or non-safety-related and risk-significant exist and their capabilities to execute the RSFs are defined.
5. Confirm that the effectiveness of physical and functional barriers to retain radionuclides in preventing or limiting release is established.
6. Review the technical bases for important characteristics of the LBEs with focus on the most risk-significant LBEs, and LBEs with relatively higher consequences. The technical bases for relatively high-frequency LBEs that are found to have little, or no release or radiological consequences is also a focus of the review.
7. Confirm that risk-significant sources of uncertainty in both the frequency and consequence estimates that need to be addressed via programmatic and plant capability DID measures have been adequately addressed.

The defense line functions are included as means of accomplishing the fundamental safety functions. Since there is typically some type of sense and actuation to perform these functions, there are generally PRA basic events associated with these DLs. DL1 is related to programs and design features that do not directly accomplish a safety function.

In this context "design features" have to do with design constraints or the existences of programs or features that prevent an initiating event in the first place, that increase the reliability of the functions that need to be performed during an event or limit the consequence of an event. Design features do not just mean "an SSC is a design feature". Generally, the DL1 features are not directly included in the PRA with basic events and have no credible failure modes during an event. DL2, DL3, and DL4 are generally associated with PRA basic events but may also be associated with DID functions not directly considered in the PRA.

The plant capability DID is addressed through design efforts, PRA, and qualitative reviews. This guidance addresses the qualitative review. The design effort identifies the defense levels and the fault list with the defense levels identified for each LBE. The PRA evaluates the quantitative risk. Table 4-1 provides a breakdown of the plant capability DID and what effort will address each portion.

Table 4-4: Layer Guidelines

Layer	Layer Guideline		Overall Guidelines	
	Quantitative	**Qualitative**	**Quantitative**	**Qualitative**
1) Prevent off-normal operations and AOOs	Maintain frequency of plant transients within designed cycles; meet owner requirements for plant reliability and availability		Meet F-C target for all LBEs and cumulative risk metric targets with sufficient margins (NEI 18-04PRA Analysis to be performed)	No single design or operational feature, no matter how robust, is exclusively relied upon to satisfy the five layers of defense
2) Control abnormal operation, detect failures, and prevent DBEs	Maintain frequency of all DBEs < 10^{-2} /plant year	Minimize frequency of challenges to SR SSCs		
3) Control DBEs within the analyzed design basis conditions and prevent BDBEs	Maintain frequency of all BDBEs < 10^{-4} /plant year	No single design or operational feature relied upon to meet quantitative objectives for all DBEs		
4) Control severe plant conditions and mitigate consequences of BDBEs	Maintain individual risks from all LBEs < QHOs with sufficient margins	No single barrier or plant feature relied upon to limit releases in achieving quantitative objectives for all BDBEs		
5) Deploy adequate offsite protective actions and prevent adverse impact on public health and safety				

Not Confidential
Verify Current Revision

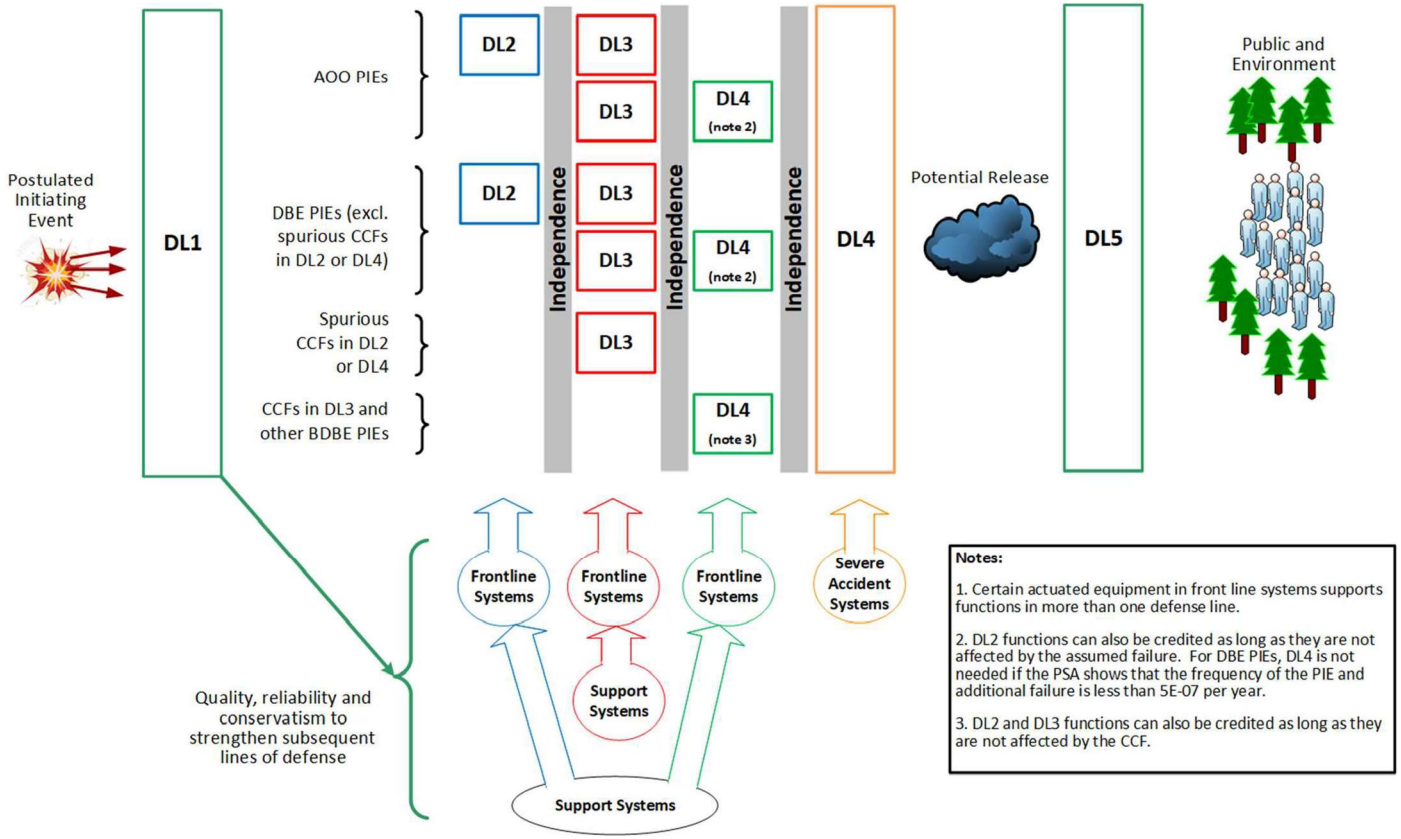


Figure 4-1: Defense Line Concept

This ToR provides preliminary list of functions assigned to the RPS (see Section 6.2). The licensee or applicant referencing this ToR will provide the list of functions, defense lines, classifications, and assignment to the I&C systems based on the DID analysis and PRA process described in this section and Section 4.3.

4.3 Safety Classification Process

The plant-level SSC classification process is consistent with the guidance of NEI 18-04 and is applied to the plant systems, including the I&C systems. The plant-level SSC classification is performed at a level of detail commensurate with the design and safety strategy using the mature defense lines strategy, events list, and the initial risk-information gained through the implementation of the NEI 18-04 process. The three classification levels of SR, NSRST, and NST and the designation of SSCs as risk-significant and safety-significant are consistent with NEI 18- 04.

The Natrium power plant utilizes an integrated digital-based I&C design. The I&C architecture is arranged to support a plant-level DID framework using the safety analysis framework from NEI 18-04 that results in system classification based on the importance of the system safety functions.

NEI 18-04 describes the methodology for selection of LBE; safety classification of SSCs and associated risk-informed special treatments; and determination of DID adequacy for non-LWRs.

Table 4-2 shows the classification of the functions assigned to each I&C system based on the plant-level SSC classification. System classification is based on the highest safety classification of the functions allocated to the system.

Table 4-5: Instrumentation and Control System Classification

System Name	Abbreviation	Safety Classification of System (some functions allocated to the system maybe of lower classification)
Auxiliary Monitoring and Control System	AMC	NSRST
Anticipatory Automatic Seismic Trip System	AST	NSRST*
Coolant Temperature Monitoring and Control System	CTC	NSRST
Fuel Handling Supervisory Control System	FHC	NST
Plant Monitoring and Control System	PMC	NST
Reactor Instrumentation System	RIS	SR
Rod Monitoring and Control System	RMC	NST
Radiation Monitoring System	RMS	NSRST
Reactor Protection System	RPS	SR
Seismic Monitoring System	SMS	NST
Utility Monitoring and Control System	UMC	NSRST
Nuclear Instrumentation System	XIS	SR

*The licensee or applicant referencing this ToR will provide the AST architecture including interface with RTBs.

4.4 Function Allocation to I&C Systems

The plant and I&C functions are determined using the plant risk and DID analysis based on NEI 18-04. The process is iterative. During the preliminary design and requirements phase of the project, a baseline is established. The plant DID analysis and safety classification are updated based on design considerations through the design development process. The design control and change process is described in the TerraPower Quality Assurance Program Description (QAPD), TP-QA-PD-0001. The list of functions and classification of the SSCs will be finalized at the end of the design phase using the NEI 18- 04 process and subject to the change control process.

Additional requirements are applied to I&C due to regulatory and stakeholder requirements. System functions are allocated to the various I&C systems based on the safety classification and nature of the function using an approved process. The following are the considerations for function allocations to the I&C systems:

- Safety classification
- Monitoring, controls, and actuations
- Operational efficiency
- Manual operator action
- PAM
- Simplicity
- Technical constraints
- Expert judgement

5 INSTRUMENTATION AND CONTROL INTEGRATED NETWORK

The following sections described the overall I&C architecture and communications.

5.1 Overall Architecture

The overall I&C architecture is shown in Figure 5-1, Overall I&C Architecture Diagram, (see Figure 5-2, Overall I&C Architecture Diagram Legend, for the legend). The NIC is described in Section 6.7, Nuclear Island Control System.

[[

]](a)(4), ECI

Figure 5-1: Overall I&C Architecture Diagram

Not Confidential
Verify Current Revision

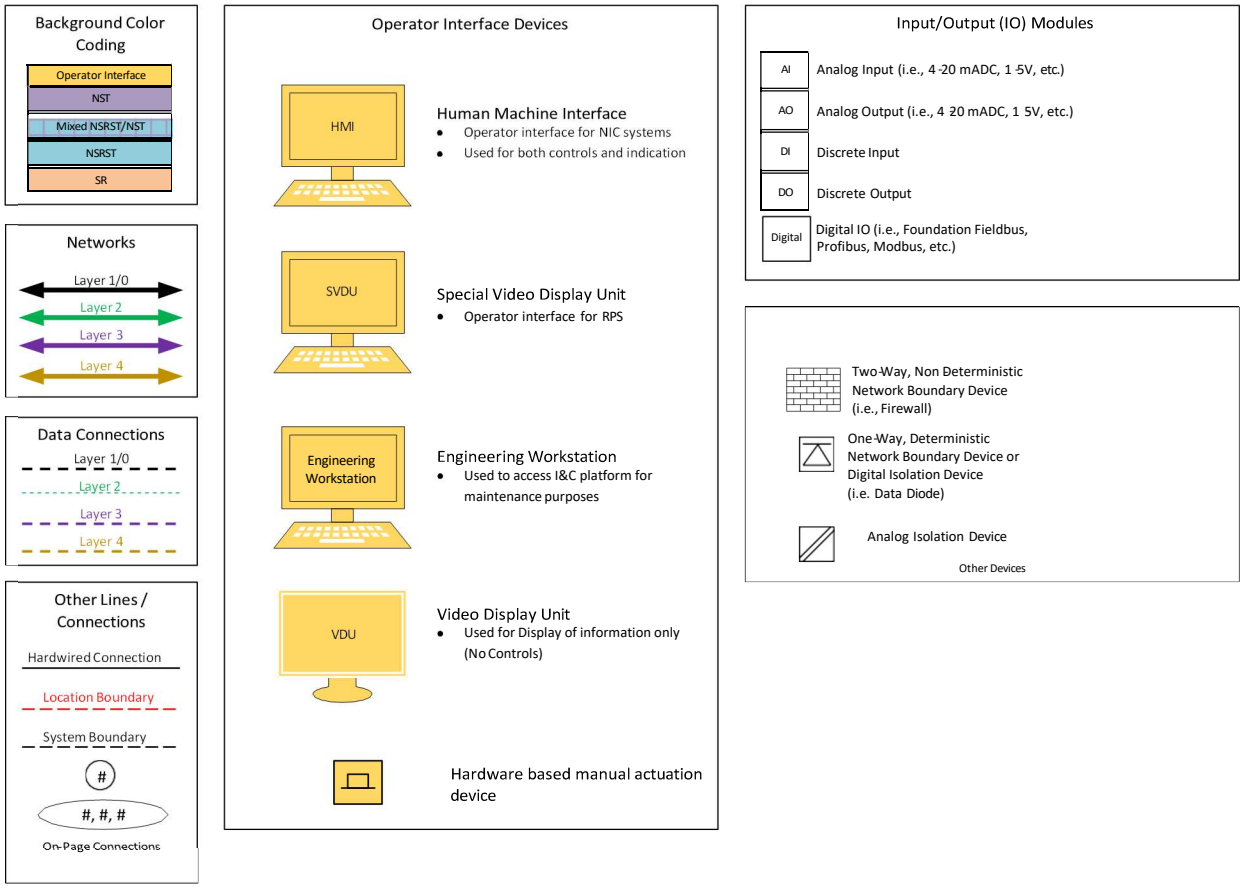


Figure 5-2: Overall I&C Architecture Diagram Legend

5.2 Distributed Control System (DCS)

The backbone of the NIC is implemented on a DCS that provides a means for gathering information from field sensors, executing both manual and automatic logic, interfacing to field actuators, and providing a means of human interface between this equipment and operators. Additionally, the NIC includes controls that are executed outside of the DCS by vendor supplied control systems (i.e., skids). Vendor supplied control systems will include interfaces for communication with the DCS.

5.3 Monitoring and Indication

The Natrium I&C provides for monitoring the plant at various locations including the main control room (MCR), the Fuel Handling Control Room (FHCR), and the Remote Shutdown Complex (RSC). Figure 5-1, Overall I&C Architecture Diagram, shows the MCR and outside the MCR boundary. The RPS divisional A and B Special Video Display Units (SVDUs) in MCR and RSC are qualified to display NSRST PAM variables. Any NIC VDU can be configured to include these variables.

5.4 Communications

Hardwired connection of signals is used to ensure reliability commensurate with SR, NSRST, and NST requirements and include direct, non-multiplexed, transmission of signals. Bus connections are used to achieve space saving and efficient communication between non-safety-related equipment (NSRST and NST). Bus connection refers to the exchange of multiplexed information (e.g., fieldbus communication using standard protocols such as Fieldbus, Modbus, Profinet, and Profibus). Copper or optical fiber may be used for both hardwired and bus connections. Data communication between I&C systems is described below:

- There are no data bus communications from the NSRST and NST systems to the SR systems.
- Communication from SR I&C systems to the NSRST and NST systems is via isolated hardwire or through data diode and gateways (both are one-way communication).
- The SR I&C does not have inter-divisional communications with exception of the RPS coincidence voting. RPS utilizes RadICS platform communication protocols and methods as described in the RadICS platform topical report.

6 INSTRUMENTATION AND CONTROL SYSTEMS

The Natrium I&C systems are described in this section with a focus on SR I&C systems and interfaces. Other systems are described to show interfaces and to support presentation of the overall architecture. The interfaces to individual plant systems shown on the figures and described in the following sections are also preliminary. The updated list of systems, classifications, and interfaces will be provided by the licensee or applicant referencing this ToR.

6.1 Equipment Location

The I&C equipment locations are such that they are protected from internal and external hazards and are qualified for operational and accident conditions, as applicable. The licensee or applicant referencing this ToR will provide specifics of equipment locations.

6.2 Reactor Protection System

The RPS is a SR I&C system consisting primarily of electronics and electrical equipment cabinets in the Nuclear Control Building substructure, as well as operator interface devices in the MCR and RSC.

The primary function of the RPS is to, with precision and reliability, accept input signals from plant instrumentation, apply required logic, and automatically generate output signals to initiate SR functions, scram and ESF, when required by plant conditions. The RPS also serves to display critical information to operators in the control room and in the remote shutdown facility during normal and postulated post-accident conditions.

The RPS monitors the plant conditions and performs the automatic SR functions that are needed to bring the plant to a safe state if a design basis accident occurs (i.e., DL3 protective functions). The RPS also provides the operators with the capability to monitor the plant conditions during normal operations, during and after plant transients, as well as postulated accidents. The RPS is a highly reliable and dependable system with four redundant divisions included in the configuration. Figure 6-1 shows a block diagram of the RPS.

Each RPS cabinet has redundant power supplies for its electronics. The RPS is functionally independent of NSRST and NST systems, thereby ensuring that the failure of one or more of those systems does not prevent the RPS from performing its safety functions.

[[

]](a)(4), ECI

Figure 6-1: RPS Block Diagram

6.2.1 Reactor Scram

A scram occurs when the RPS initiates a sudden shutdown of the reactor through rapid insertion of the control rods. The scram is provided in support of RSFs related to Reactivity Control (RC) during design basis accidents (DBAs).

The RPS initiates a scram automatically when plant conditions exceed established setpoints to prevent reaching analytical limits set in the safety analysis. The RPS initiates automatic scram when conditions such as the following are sensed.

- High High Neutron Flux
- High High Hot Pool Temperature
- High High Primary Sodium Level
- High High Power-to-Flow Ratio
- High High Cold Pool Temperature

- High High Positive Neutron Flux Rate
- High High Negative Neutron Flux Rate
- Low Low Primary Sodium Level
- Low Power, High Neutron Flux
- Loss of Primary Sodium Flow
- Loss of Power to RPS

The RPS also provides the ability for operators to initiate a manual scram from the MCR, although this manual scram capability is not credited in the safety analysis.

During normal operations, each control rod assembly (CRA) is held at a controlled position above or within the core by pressurized argon. The argon pressure at each CRA is maintained by three solenoid operated valves (SOVs) at each CRA which are normally energized. De- energizing at least 2-out-of-3 SOVs at a given CRA will vent the pressurized argon, releasing that CRA and allowing it to fall into the core via gravity. A reactor scram signal de-energizes all controls rod solenoids.

Figure 6-2, RTB Arrangement, shows the RTB arrangement. Each RPS division controls two RTB assemblies, each of which has three poles, corresponding to the three solenoids at each CRA. The RTB assemblies are arranged in a 2-out-of-4 configuration so that failure of any single breaker, either open or closed, will neither cause loss of safety function nor spurious reactor scram. The CRA releases when power is removed from any 2-out-of-3 associated solenoids, therefore failure of any single breaker pole does not affect CRA operation.

Each RTB assembly is equipped with an undervoltage (UV) trip as well as a shunt trip (ST) design feature. The undervoltage design feature will open the breaker when control power to the breaker is removed either by RPS or by power loss, thus providing a failsafe trip. For additional reliability and diversity, a ST design feature is also included which opens the breaker when control power is applied by automatic reactor trip signal. The shunt trip is also used for manual trip and is available for future remote trip function if needed (NSRST function).

[[

]](a)(4), ECI

Figure 6-2: RTB Arrangement

For diversity in support of DID, the RPS also initiates a control rod drive system (CRD) Driveline Scram Follow function to mechanically drive control rods in when any automatic or manual scram occurs, regardless of CRA release success. The CRD Driveline Scram Follow demand output signals are independent of the RTB trip demand output signals from RPS.

6.2.2 Engineered Safety Features

ESFs are provided in support of RSFs related to providing Heat Removal (HR) during postulated accidents.

The RPS initiates ESFs automatically when conditions such as the following are sensed:

- PSP Trip on High Cold Pool Temperature with Reactor Scram and Low Neutron Flux
- ISP Trip on High Cold Pool Temperature with Reactor Scram and Low Neutron Flux
- ISP Trip on High Primary Sodium Level with Reactor Scram and Low Neutron Flux
- SPS Pump Trip on Low Primary Sodium Level

The RPS also provides the capability to manually initiate each ESF from the main control room, although these manual ESF capabilities are not credited in the safety analysis.

ESFs all involve tripping pumps. Each pump that must be tripped as part of an ESF is controlled by two electrical breakers which are part of the same system as the pump. These pump breakers are arranged in series such that tripping either breaker will stop the pump, thus achieving the safe state.

Each ESF pump breaker is equipped with an undervoltage release trip as well as a shunt trip mechanism. The undervoltage release will open the breaker when control power to the breaker is removed either by RPS or by loss of control power. Loss of incoming power to RPS results in removal

of control power to the associated ESF breakers, thus providing a failsafe design. For additional reliability and diversity, a shunt trip feature is also included which opens the breaker when control power is applied to the ST coil. Figure 6-3 shows the ESF breaker arrangement.

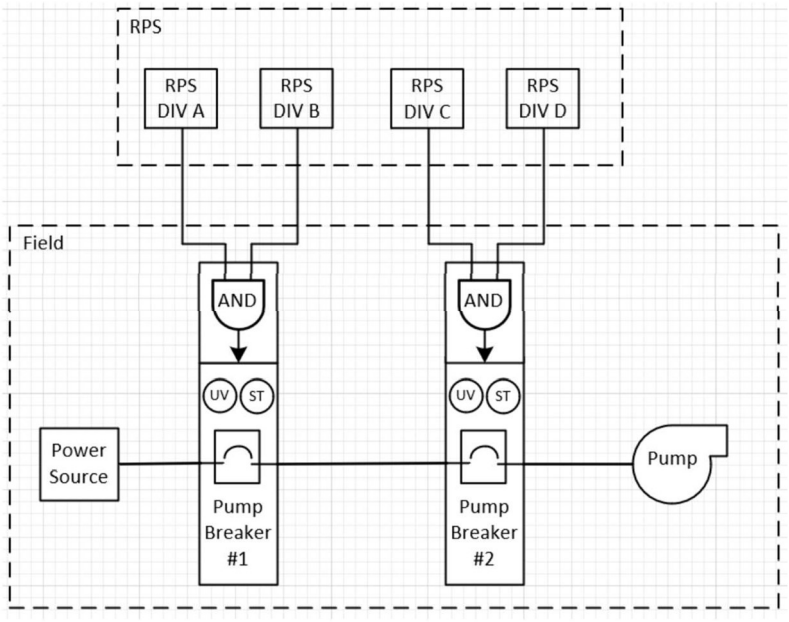


Figure 6-3: ESF Breaker Block Diagram (Typical)

The ESF control scheme is designed such that failure of any RPS division, in either the high or low direction, will neither cause loss of the safety function nor spurious pump trip. The RPS design includes the capability (not shown in Figure 6-3) to temporarily force the ESF output of any RPS division into the safe state manually such that there is no reduction in safety if a single RPS division is out of service for testing or maintenance.

6.3 Nuclear Instrumentation System

The Nuclear Instrumentation System (XIS) provides instrumentation to sense neutron flux leakage from the core during fuel movement, reactor startup, power operations, shutdown, and accident conditions. The XIS system amplifies and conditions the instrument signals as required and provides corresponding input signals to the RPS and the NIC for use in protective, control, and monitoring functions.

The XIS is located in dedicated cabinets in the Nuclear Island (NI). The XIS is comprised of four redundant divisions, each of which includes a division-specific flux detector and signal conditioning. Each XIS division is separate and independent from the other XIS divisions. The XIS sensors are located at different quadrants of the reactor. The four ex-core fission chambers are placed inside of detector guide tubes that are located on the outside perimeter of Core Barrel Structure (CBS) Outer Barrel. XIS provides flux signals to RPS in support of SR protective functions, and the four XIS divisions correspond to the four RPS divisions. Each XIS division interfaces with the corresponding RPS division only, thus maintaining divisional independence. All XIS signals sent to RPS are made available to the Plant Data Bus via the RPS Data Gateway.

The XIS also provides signals to the NIC in support of control functions. NIC systems, such as Rod Monitoring and Control (RMC) and Coolant Temperature Control (CTC), which use the XIS signals in control schemes are provided with isolated, hardwired signals from XIS.

Each XIS division also provides isolated, hardwired signals to Audible Count Rate (ACR) monitoring devices in the MCR and in the FHCR for use during refueling and startup operations. Figure 6-4 shows the overall XIS block diagram, interfaces with NIC, and isolations between SR and non-safety-related (NSRST and NST) systems.

Not Confidential
Verify Current Revision

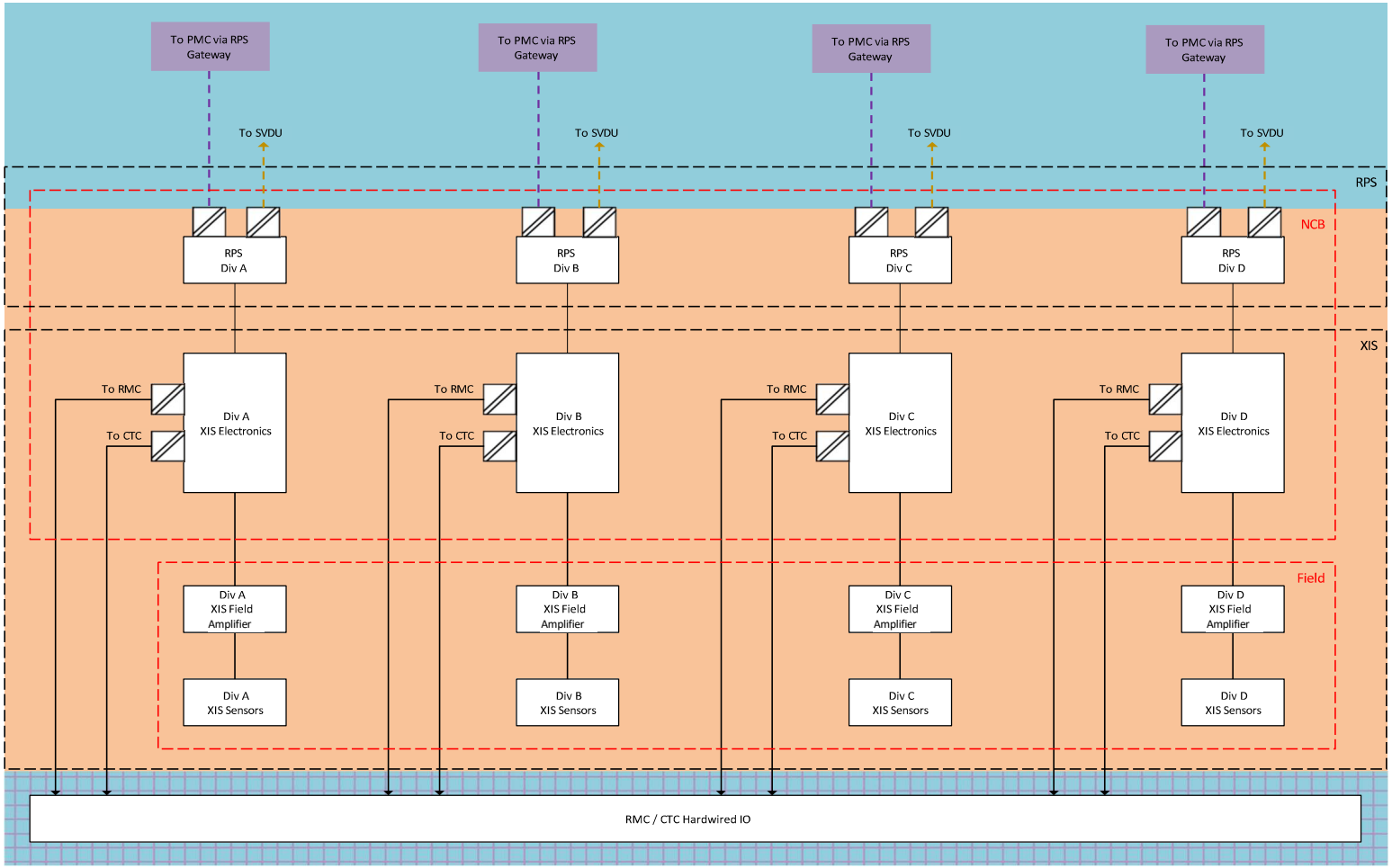


Figure 6-4: XIS Block Diagram

Note 1 - Sensors and Hardwired inputs/outputs (I/O) to NIC will be NSRST or NST as required by the functions supported by the sensors.
Note 2 - The block diagram is not meant to show exact connections between various devices.
Note 3 - The exact number of devices is not shown on this block diagram.

6.4 Reactor Instrumentation System

The Reactor Instrumentation System (RIS) provides instrumentation to detect selected parameters in or near the reactor vessel and transmits corresponding signals to the RPS and the NIC for use in protective, control, accident monitoring, and surveillance functions.

The RIS is a collection of individual RIS instrument channels, where a channel is defined as a single sensor and its associated cabling and signal amplification electronics (if required). An individual RIS instrument channel may support one or multiple functions which are classified as SR, NSRST, or NST. Table 6-1 provides safety classification and number of RIS channels.

Table 6-1: Preliminary RIS Variable Summary

Variable	Number of Channels /Sensors	Safety Class
Primary Sodium Hot Pool Temperature	4	SR
Primary Sodium Hot Pool Level	4	SR
Core Exit Temperatures	15 Sensors	NSRST
Reactor Vessel/Guard Vessel Liquid Sodium Detection	3 Sensors	NSRST
Cold Pool Temperature	4	SR
Reactor Head Temperature	3 Sensors	NST
Primary Sodium Pump Shaft Speed*	4	SR
Primary Sodium Pump Current Sensor*	4	SR

*Primary Sodium Flow will be interpreted from Primary Sodium Pump shaft speed, current and other variables.

Figure 5-1, Overall I&C Architecture Diagram, shows the RIS inputs to RPS and NIC. The RIS meets IEEE Std. 603-2018 and IEEE 384-2018 [12] and the following requirements:

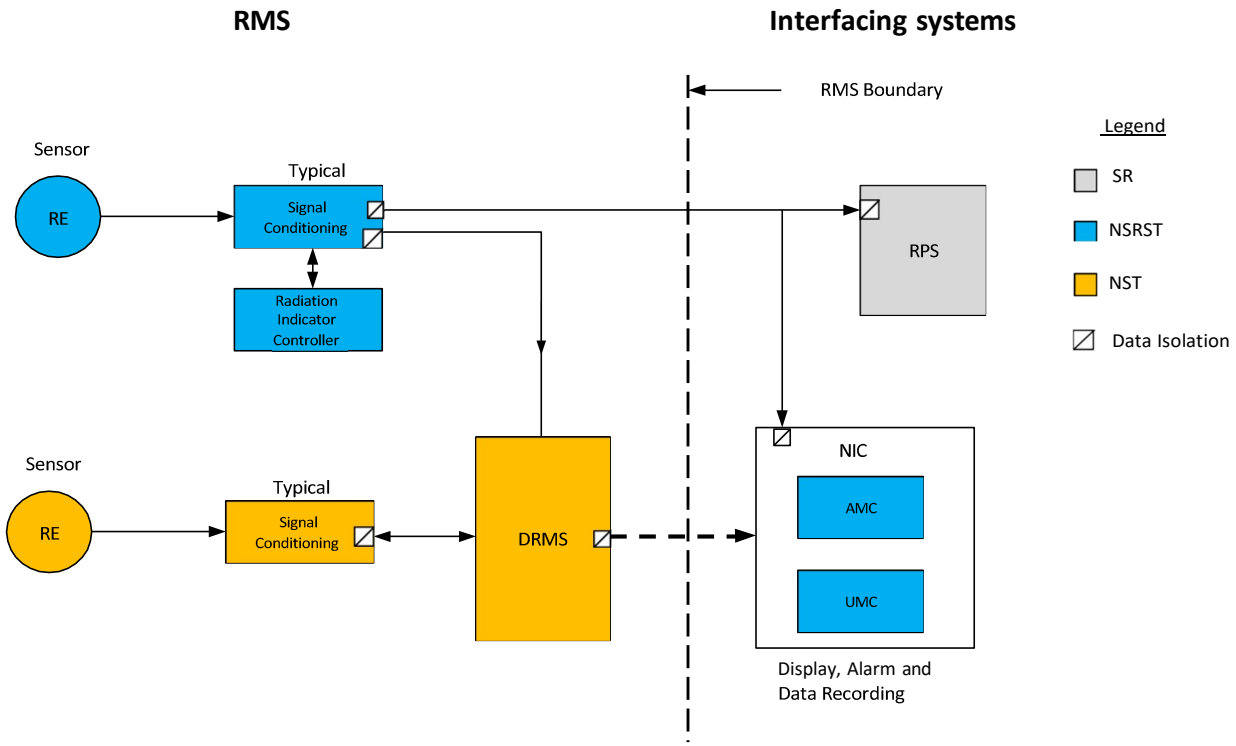
- Independence between redundant RIS channels
- Independence between the SR and non-safety-related (NSRST and NST) equipment
- Isolation between the SR and non-safety-related (NSRST and NST) equipment
- Quality assurance requirements
- Special treatment based on classification (e.g., codes and standards, RGs, programs). The licensee or applicant referencing this ToR will identify the specific special treatments.

6.5 Radiation Monitoring System

The RMS is a digital system with NSRST and NST functions that provides radiation detection for systems, buildings, and release pathways throughout the plant. The RMS continuously monitors radiation and sampling analysis of selected radioactive processes, as well as monitoring for the selected release points where radioactive effluents leave the site boundary.

All monitors provide activity, monitor health, control, and status information to the Digital Radiation Monitoring System (DRMS) central computer system located in the MCR. The DRMS provides a direct digital connection to the I&C AMC for plant display and control of the RMS, which consists of three main monitoring groups:

- Area Radiation Monitoring (ARM) located throughout the NI buildings. The ARM provides PAM (DL5-PAM2) signals to the I&C AMC and the PAM (DL5-PAM1) to the RPS.
- Process Radiation Monitoring (PRM) located on various systems within the NI. The PRMs provides PAM (DL5-PAM2) signals to the I&C AMC and the PAM (DL5-PAM1) to the RPS.
- Effluent Radiation Monitoring (ERM) located on the Combined Plant Stack (CPS). The ERM provides PAM (DL5-PAM2) signals to the I&C AMC.



Note -This interface diagram is intended to show the interfaces between RMS and I&C Systems and is not meant to show the different types of connections and radiation monitors or quantity of monitors.

Figure 6-5: RMS Block Diagram

6.6 Seismic Monitoring System

The Seismic Monitoring System (SMS) is an NST system. The SMS monitors the vibratory ground motion and resultant vibratory responses of representative structures so that plant personnel can take prompt action to assess the effects of an earthquake. The SMS provides time-history acceleration data on the seismic response in the free-field, containment structure, and other structures.

The SMS is made up of two main types of components: acceleration sensors and a recorder. The acceleration sensors are the instruments capable of sensing absolute acceleration and provide a signal to the recorder. The recorder is an instrument that is capable of recording and storing data from the acceleration sensors.

The SMS provides an alarm to the NIC if the SMS detects that the seismic threshold is reached for any channel.

6.7 Nuclear Island Control System

The NIC is a group of I&C sub-systems that perform NST and NSRST control and monitoring functions. The NIC is implemented on a DCS platform that provides a means for gathering information from field sensors, executing both manual and automatic logic, interfacing with field actuators, and providing a means of interface between that equipment and operators. Additionally, the NIC includes controls that are executed outside of the DCS by vendor supplied control systems (e.g., vendor skids) that include interfaces for communication with the DCS. The following subsystems are considered part of the NIC as shown in Figure 5-1:

- Plant Monitoring and Control System (PMC)
- Rod Monitoring and Control System (RMC)
- Coolant Temperature Control System (CTC)
- Utility Monitoring Control System (UMC)
- Auxiliary Monitoring and Control System (AMC)
- Fuel Handling Supervisory Control System (FHC)

NIC controls or interacts with some safety equipment during the normal operations (DL1) and in response to AOOs (DL2) and BDBEs (DL4). These NIC functions are classified as NSRST and NST and include the CRD Driveline Scram Follow, PSP and ISP trips, and SPS isolation. The I&C system does not include a priority module. To confirm NSRST and NST systems do not create a hazard, a hazard analysis will be performed to confirm a) NIC faults are not propagated to the SR equipment, and b) NIC controls and faults do not impede initiation of protective actions or prohibit completion of RSFs.

The NIC system block diagram is shown in Figure 5-1.

6.7.1 Plant Monitoring and Control System

The monitoring and controlling of the NI are accomplished using plant controllers, networks, and Human Machine Interfaces (HMI), which are necessary to operate the plant during normal operations, including commissioning, maintenance, refueling and accident conditions. The PMC has bi-directional communication to other NIC subsystems via the Plant Data Highway (PDH), see Figure 5-1. There is only one-way communication via gateway from the RPS to the NIC. The PDH uses a redundant ethernet network to provide fast and secure communication to the PMC and other connected systems. The HMI bus provides a separate network from the PDH to support intensive data display functions

between the VDUs and historian servers. The plant intranet network is isolated from the PMC by a data diode.

Data transferred on the PDH includes time stamp information. Data from the plant systems flows to the historian for logging. The operator workstations are connected to the HMI bus along with alarm annunciator and other information support devices (e.g., printers, scanners). Operators can monitor plant data and control plant equipment through the HMI in all operating modes. The PMC does not have ability to perform automatic control. However, other NIC subsystems provide controls for plant equipment and the PMC has the necessary user interface to perform manual control through NIC sub-systems controllers.

The PMC includes the following features:

- Process Visualization
- Control and Operation
- Trending and Historical Data
- Procedural Support
- Security and Access Control
- Application Servers

The PMC system block diagram is shown in Figure 5-1.

The PMC network supports common services such as alarming, displaying, and recording. There are various PMC supporting units such as VDU, HMI, Safety Parameter Display System (SPDS) HMI, Engineering Workstation, Network Bridge, Application Servers, Cyber Security Infrastructure, and Database Server.

6.7.2 Rod Monitoring and Control System

The RMC provides the hardware and software to monitor and control the sub-systems and sub-components of the CRD. The RMC is integrated with the PMC to provide information to be displayed on the HMI monitors. The RMC is classified as NST. The RMC interfaces with the CRD, CTC, FHC, NI Ancillary Electrical System (NEA), NI Auxiliary Electrical Systems (NES), RIS and XIS.

The RMC is a subsystem of the NIC. Figure 5-1 shows the RMC system block diagram. The RMC performs the following functions through the manipulation of the CRD:

- Monitoring Functions
- Indication Functions
- Alarm Functions
- Power Runback
- Normal Insertion and Withdrawal

- Rod Withdrawal Inhibit
- Driving the uncoupled control rod drive mechanism drivelines to their fully withdrawn positions from the core
- Providing the necessary interlocks to the FHC system to support refueling operation
- Startup testing

6.7.3 Coolant Temperature Control System

The CTC provides the hardware and software to monitor and control those plant systems that are associated with primary and intermediate heat transport. The CTC is used to perform both NST and NSRST functions. The CTC is integrated with the PMC to provide information to be displayed on the plant HMIs. Figure 5-1 shows the CTC block diagram. The CTC monitors and controls the following components of the plant systems:

- The Primary Sodium Pump Adjustable Speed Drives (ASDs) of the Primary Heat Transport System
- The Intermediate Sodium Pump ASDs of the Intermediate Heat Transport System
- The Intermediate Air Cooling System, including control of the dampers, heating system, and blowers
- The NI Salt System isolation, vent, and salt drain valves
- The Energy Island Salt System Cold Salt Transfer Pump ASDs, Cold Salt Transfer Pump minimum flow control valves, Cold Salt Transfer Pump output flow control valves, the vent valves, and gravity drain monitoring and control
- Control rod movement coordination with the RMC system, including the initiation and management of the Run Back function, and the Constant Power Control regulation functions. CTC determines when to move Secondary Control Rods and RMC determines which rods to move.

6.7.4 Utility Monitoring and Control System

The UMC provides the hardware and software to monitor and control various utility systems. The UMC is made up of multiple interconnected components that are distributed throughout the process. The UMC is a subsystem of the NIC. Figure 5-1 shows the block diagram of the UMC.

The UMC system receives inputs from sensors, perform logic operations, and activates outputs to control and adjust the process. The UMC is integrated with the PMC to provide real-time monitoring and control. The UMC performs NSRST and NST functions and interfaces with various plant systems, such as NI Air and Gas Distribution Systems, NI Fire Protection Systems, NI Water Systems, and NI HVAC Systems.

6.7.5 Auxiliary Monitoring and Control System

The AMC provides the hardware and software to monitor and control the plant systems that are associated with the NI auxiliary systems. The AMC is integrated with the PMC to provide information to be displayed on the plant HMIs. The AMC is a subsystem of NIC. The AMC block diagram is shown in Figure 5-1.

The AMC is used to perform both NST and NSRST functions. The AMC interfaces with various plant systems, such as Sodium Processing Systems, Gaseous Radwaste Processing System, Liquid Radwaste Processing System, Sodium Cover Gas Systems, Solid Radwaste Processing System, and RMS.

6.7.6 Fuel Handling Control System

The FHC provides the hardware and software to monitor and control the fuel handling systems. The FHC is integrated with the PMC to provide information to be displayed on the plant HMIs and VDUs. The FHC is used to perform NST functions. Figure 5-1 shows the FHC block diagram. A portion of the FHC will be executed on FHC Supervisory, Control, and Data Acquisition (SCADA) that is not part of the DCS as shown on the overall I&C architecture, Figure 5-1.

6.8 Post-Accident Monitoring

Post-accident monitoring is provided in the event of an accident per RG 1.97 Revision 5 and IEEE Std 497-2016. Since the Natrium I&C systems already include provisions for providing display of information, the existing hardware for these systems are leveraged to meet PAM requirements. Natrium I&C does not have any Type A PAM variables since there are no specific safety functions that require manual action during DBAs. The NSRST Type B, C, and F variable are processed in RPS (signals are isolated if needed) and displayed on SVDUs. The NST Type E variables inputs are provided to the PMC for display via the SPDS. The RPS includes SVDU screens in the RSC and the MCR, and the PMC includes screens on various HMIs and VDUs as shown in Figure 5-1.

7 FUNDAMENTAL I&C DESIGN PRINCIPLES, SIMPLICITY, AND SECURITY

Section 7 describes the Natrium I&C adherence to the I&C fundamental design principles, simplicity, and security, as described in the DRG for I&C of non-LWRs.

7.1 Independence

The RPS maintains independence, including physical separation and electrical isolation, between redundant RPS divisions in accordance with IEEE Std 603, Section 5.6, IEEE Std 384, and RG 1.75. In addition, SR RPS equipment physical separation and electrical isolation is maintained from NSRST and NST equipment such that a failure in NSRST and NST equipment cannot cause a loss of safety function.

7.2 Communications and Logical Independence

In accordance with DI&C-ISG-04 [13], for digital portions of the RPS, data communication between SR divisions or between SR and non-safety-related (NSRST and NST) systems does not inhibit the performance of safety functions. In accordance with IEEE Std 7-4.3.2 [14], Section 5.6, for digital portions of the RPS, NSRST and NST software which resides on the same computer, or shares resources with SR software, does not inhibit the performance of safety functions.

See the RadICS platform topical report for additional information on communications and independence.

See Section 5.4 for additional information on communications.

7.3 Redundancy

The RPS meets the single failure criterion of IEEE Std 603, Section 5.1. The RPS is designed such that no single failure results in loss of an RSF. This includes potential single failures of supporting systems, such as power and environmental controls, which could result in loss of an RPS safety function.

The RPS has four redundant divisions, each of which accepts input signals from corresponding divisions of measurement instruments and systems (e.g., XIS, RIS, etc.). Each division:

- Converts analog input signals to digital and applies signal conditioning, calculations, and permissive or block logic, as required
- Compares variables to the setpoints to determine if the RPS division will generate a divisional scram or ESF actuation vote
- Communicates divisional scram and ESF actuation vote status with the other RPS divisions
- Counts votes from all divisions, and when sufficient total votes exist (e.g., 2 out of 4) issues scram, ESF actuation, or both signal(s) as required
- Communicates with division-specific SVDU in the MCR and RSC

The RPS meets the redundancy requirements of IEEE Std 603, Section 8.3, for redundant power supply. The RPS utilizes redundant power sources such that there is no loss of safety function while a power source is bypassed for maintenance.

7.4 Diversity

As stated in Section 4, Instrumentation and Control Systems Overview, the overall plant DID is based on NEI 18-04. The Commission has approved the staff SECY-22-0076 (ADAMS Accession No. ML22164B003) in SRM-SECY-22-0076 (ML23145A181). The SECY letter expanded the current policy on potential CCF in I&C systems to include the use of risk-informed approaches. The NRC DRG also supports a regulatory framework that is risk-informed and performance-based, per NEI 18- 04 and RG 1.233. Based on the above, the I&C D3 analysis is encompassed by the overall plant DID analysis, as described in Section 4.2, I&C Relationship to Plant-Level Lines of Defense.

The following provides results of the PRA DID analysis and use of the RadICS platform to address RPS CCF. The NRC evaluated the diversity of the RadICS platform used for the RPS and concluded that the applicant's or licensee's D3 analysis should either (1) demonstrate adequate diversity exists to mitigate plant vulnerabilities without the need for a diverse actuation system, or (2) determine the need for a diverse actuation system to provide adequate mitigation against plant vulnerabilities. Additionally, the NRC concluded the RadICS platform cannot be confirmed to meet all the NRC staff positions within BTP 7-19 because a system level D3 assessment requires availability of a system- specific design. Therefore, a plant-specific evaluation must be performed at the time of application development (PSAI 7.9).

The RadICS Platform Safety Evaluation Report (SER) PSAI 7.9 is addressed by the Natrium I&C design, allocation of functions, safety classification and diversity and defense in-depth based on PRA and the plant DID analysis. These analyses are consistent with the SRM-SECY-22-0076 methodology. The analysis requires implementation of diverse NST and NSRST functions at DL4 including diverse Sodium Processing System (SPS) Pump, Primary Sodium Pump (PSP) and Intermediate Sodium Pump (ISP) shutdown and trip. In addition, the RPS design implements the RadICS fail safe modes as indicated in PSAI 7.9. Note that other RadICS PSAIs will be addressed by the licensee or applicant referring this ToR.

Common cause failures are included in the PRA fault tree models for components that perform an active function for the system response to event mitigation including CCF of the safety-related protection system (i.e. RPS) and CCF of the non-safety control system (i.e. NIC).

Common cause failures for most events are modelled using the Alpha Factor method when specific details about the components are not known. The Alpha Factor method is not used for the RPS digital platform based on the diversity assessment of the RadICS digital I&C platform documented in the RadICS platform topical report. For those components, the following assumptions are made:

- It is assumed that the processing and bistable logic blocks of RPS will include both a complex programmable logic device (CPLD) and a field programmable gate array (FPGA). Further, it is assumed that these are different pieces of hardware (diverse) and use different internal software coding.
- Although the CPLDs and FPGAs are considered different pieces of hardware and use different programming, simultaneous CCF of both sets of equipment is considered. CCF between the two sets of equipment accounts for issues caused by potentially common software specifications and environmental conditions. Each of the four processing and bistable logic blocks of RPS will include both a CPLD and a FPGA. These devices are evaluated separately from their associated bistable for CCF. It is assumed that CCF among all four CPLDs could occur with a probability of 1E-04 per plant year. Similarly, it is assumed that CCF of all four FPGAs could occur with a probability of 1E-04 per plant year. Additionally, CCF between the CPLDs and FPGAs is assumed to occur with a failure probability of 5E-06 per plant year.

The analysis of the RPS platform diversity identified the effects of postulated failures. The internal diversity ensures postulated failures are identified and appropriate alarms are activated. Upon detection of a significant fault, the RadICS platform assures that the outputs associated with a logic module achieve a predefined safe position (e.g., output modules are de-energized.). The RPS is designed such that de-energized outputs result in actuation of the scram and ESF safety functions (safe state). Inconsequential failures of the RadICS platform are alarmed and have no impact on plant safety.

Hardwired manual actuation of scram and all ESFs that bypasses the RPS digital I&C platform is provided in the design for DID.

7.4.1 SECY-22-0076

The following addresses the SRM-SECY-22-0076 that approved the staff recommendation with some changes:

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

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

Natrium I&C implementation: An assessment of the defense-in-depth and diversity is performed consistent with NEI 18-04. The assessment considers risk significance of the RPS. SSC safety classification concluded that RPS is SR.

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

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

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

Natrium I&C implementation: The DID assessment is performed using a risk-informed approach and is consistent with RG 1.233.

3. The defense-in-depth and diversity assessment must demonstrate that a postulated CCF can be reasonably prevented or mitigated or is not risk-significant.

The applicant must demonstrate the adequacy of any design techniques, prevention measures, or mitigation measures, other than diversity, that are credited in the assessment. The level of technical justification demonstrating the adequacy of these techniques or measures, other than diversity, to address potential CCFs must be commensurate with the risk significance of each postulated CCF.

A diverse means that performs either the same function or a different function is acceptable to address a postulated CCF, provided that the assessment includes a documented basis showing that the diverse means is unlikely to be subject to the same CCF. The diverse means may be performed by a system that is not safety-related if the system is of sufficient quality to reliably perform the necessary function under the associated event conditions. Either automatic or manual actuation within an acceptable timeframe is an acceptable means of diverse actuation.

If a postulated CCF is risk-significant and the assessment does not demonstrate the adequacy of other design techniques, prevention measures, or mitigation measures, then a diverse means must be provided.

Natrium I&C implementation: The DID assessment establishes the defense lines and shows that design features are adequate to address CCF. The RadICS platform topical report described the

internal diversity as approved by the NRC. The PRA DID analysis shows the RPS, with inherent internal diversity, sufficiently decreases the CCF risk beyond the DBE region such that the RPS CCF event can be further mitigated through DL4 functions.

The consideration of CCF in the PRA shows that no PIE combined with RPS failure is above 1E-4 per year and thus wouldn't require another SR system. Other CCFs are considered but are also not greater than the 1E-4 per year to cause need for another SR system. An example is the alternate pump trip that overcomes failure of the ESF to trip the reactor pumps (whether it is by way of RPS CCF or breaker CCF).

The RPS CCF event is the major event of concern. CCFs of other systems are mitigated through actuation of the RPS.

See Section 4.2, I&C Relationship to Plant-Level Lines of Defense, for implementation of defense lines.

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

Natrium I&C implementation: The risk-informed critical safety functions and monitoring of parameters that support the safety functions are identified through the application of NEI 18-04. The critical safety functions are the Required Safety Functions, as defined in NEI 18-04.

The DL4 functions provide defense in-depth and diversity to address BDBEs, including RPS CCF. The following are examples of diverse manual controls provided in DL4 based on the preliminary PRA and the plant DID assessment. The licensee or applicant referencing this ToR will provide the complete listing:

- Manual reactor scram
- Manual shutdown on cover gas leakage
- Manual shutdown for unexpected conditions, on failed fuel detection exceeding normal operational limits, and on cover gas leakage

Instrumentation, indications, and manual controls are provided to allow operators to monitor the plant status, control the plant, and verify the completion of actions during normal operations and accident conditions, and monitor parameters post-accident as required by PAM implementation.

7.4.2 Sensor Diversity

The RIS, XIS and PHT provide inputs to the RPS for monitoring and actuation. Most Class 1E sensors are analog and not subject the Software CCF of a programmable digital device. However, if redundant sensors are selected that contain a programmable digital device, then one of the following methods will be used to address Software CCF.

- 100% testing of the sensors, or

- An assessment of CCF to show low likelihood of failure, and incorporation of mitigative actions, if needed (e.g., use of different type or model to provide diversity)

The Natrium power plant design shares some sensors among various functions that may reside in different defense lines. An analysis will be performed (e.g., hazard analysis) to confirm that shared sensors do not reduce effectiveness of the DID strategy, do not contradict PRA assumptions, and maintain functional independence. Any issues identified by the analysis will be mitigated or properly justified.

7.5 System Integrity

Consistent with IEEE Std 603 clause 5.5, and IEEE Std 7-4.3.2 clause 5.5, the RPS is designed to perform its safety functions under the full range of applicable conditions enumerated in the design basis, includes test and calibration features, fault detection, and self-diagnostics. The RadICS Platform predictability and repeatability design features are described in Sections 6.3, 6.4, 6.8, and 6.10 of the RadICS platform topical report.

Digital portions of the RPS (i.e., RadICS) complies with the requirements of IEEE Std 7-4.3.2- 2003, Section 5.5.1, including:

- No loss of safety function is experienced when the system is subjected to I/O failures, roundoff problems, improper recovery actions, input power fluctuations, multiple signal changes, and environmental stressors.
- Single failure of RPS components does not preclude the RPS from being placed in a safe condition.
- Safety function capability is resumed automatically after system restart.

7.5.1 Deterministic

The RadICS modules perform their intended function in accordance with predefined times and do not use interrupts; as such, the system operates deterministically. The NRC has reviewed and accepted the deterministic behavior of the RadICS system in the RadICS platform topical report safety evaluation report [7]. Since the system behavior is deterministic, the maximum response time of the system will not change and is predictable. The response times are verified during the factory acceptance testing.

Consistent with IEEE Std 603-1991 clause 5.2, the RPS is designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features will continue until completion.

7.6 Simplicity

After the minimum required reliability is achieved, simplicity in the design, construction, startup, and operation of the overall Natrium I&C system is considered over other design attributes. This approach reduces project risks associated with complex digital I&C systems.

There are no data communications between the independent channels and divisions of the protection system except for voting.

7.7 Reliable I&C

The design applies a diverse combination of design features to perform the required safety functions across layers of defense to meet the DID adequacy and address single failure and CCF.

Safety I&C systems are designed such that no single failure will result in loss of a required safety function. This includes potential single failures of supporting systems, such as power and environmental controls, which could result in loss of a safety function. Single failure design features meet the requirements of IEEE Std 603, Section 5.1 and IEEE Std 379 [15].

The I&C systems meet the reliability goals established by the PRA. The reliability of the systems is demonstrated qualitatively and quantitatively.

7.7.1 Quantitative Reliability

PRA and DID assume a reliability target for the SR systems to meet the plant-level Frequency-Consequence (F-C) target as described in NEI 18-04. Reliability of the RPS is demonstrated for the hardware during the detailed design phase.

Reliability of other components such as sensors and breakers are based on the industry established reliability and confirmed through procurement. The NSRST systems meet the special treatments determined by implementation of the NEI 18-04 process. The licensee or applicant referencing this ToR will define the special treatments.

7.7.2 Qualitative Reliability

The reliability of the safety application software, if any, and the software used for the development of the safety digital devices is demonstrated qualitatively. The goal of software reliability is to demonstrate that the software is robust and fault free. The following measures and features ensure that I&C systems (and software) perform the intended functional requirements reliably under the defined plant conditions:

- Implementation of I&C design criteria
- Application of industry codes and standards
- Equipment qualification
- Verification and validation
- Surveillances and inspections
- Failure and condition monitoring

- Maintenance Rule implementation
- RPS failsafe design
- Self-diagnostics
- Mitigation of common cause failure
- Hazard analysis
- Design control
- Electronic Design development process
- System development process
- Testing (e.g., design, factory acceptance, site acceptance, periodic testing)
- Quality assurance program
- Corrective action program
- Operation and maintenance programs

7.8 Secure Instrumentation and Control

A description of secure I&C development and operation environment controls applied to each I&C safety system and cyber security implementation during the development phase is provided in this section.

7.8.1 Secure Development Environment

The RPS meets the guidelines of Regulatory Guide, 1.152 [16], Criteria for use of Computers in Safety Systems of Nuclear Power Plants, for secure development. Physical, logical, and programmatic controls are provided during the digital safety system electronic design development, manufacturing, and testing of the system. A vulnerability assessment is performed for the development environment to identify security vulnerabilities and to implement mitigative measures and controls for the identified vulnerabilities.

The controls for the secure development environment (SDE) include, but are not limited to:

- Physical access controls to the development system, the plant units, test units, software, and components. Only approved personnel are allowed to access and make changes to the system.
- Isolation of the development system from the internet and corporate and development networks. The controls include one-way communications to the networks outside the development environment.
- Software is scanned for viruses and malware where applicable.
- The safety system electronic design verification and validation (V&V) and requirements traceability also provides an additional layer of protection by identifying electronic design features that are not traced to requirements and documenting unneeded functionality.

7.8.2 Secure Operational Environment

The licensee or applicant referencing this ToR develop processes and programs for establishing a secure operational environment. The safety-related I&C systems includes the following design features to facilitate development of the secure operations environment:

- Communications isolation: one-way communication through approved data diode between SR and non-safety-related (NSRST and NST) systems and networks.
- Access controls
- The safety system cabinets are provided with access control keys to limit access to authorized personnel.
- Changes to the setpoints and adjustable parameters are controlled by two physical controls (i.e., keyswitch and password)
- The safety system cabinets are provided with door alarms.
- Appropriate logs are provided for access control (e.g., cabinet and door) and post-event investigations.
- Other access controls are to be defined by the licensee or applicant referencing this ToR.

7.8.3 Cyber Security

10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks, requires licensees to develop cyber security plans and programs to protect critical digital assets, including digital safety systems, from malicious cyber-attacks. Subsequently, the NRC found use of NEI 08-09 [17], "Cyber Security Plan for Nuclear Power Reactors," acceptable for meeting 10 CFR 73.54. The licensee or applicant referencing this ToR provide the description of the cyber security program to meet 10 CFR 73.54. To support cyber security implementation by the licensees and applicants, and as additional measure for secure digital safety systems, the Natrium I&C architecture implements the following cyber security defensive levels, features, and controls. Also, note the plant DID and defensive layers using NEI 18-04 is different and independent of the cyber security DID and defense lines.

7.8.4 Cyber Defense-in-Depth Protective Strategies

Defense-in-depth protective strategies are implemented, documented, and maintained to ensure the capability to detect, delay, respond to, and recover from cyber-attacks on CDAs. The defensive strategy describes the defensive security architecture, identifies the protective controls associated within each security defensive level, implements cyber security controls in accordance with the cyber security plan, employs the cyber security Defense-in-Depth measures described in NEI 08-09, and maintains the cyber security program.

This defensive architecture provides for cyber security defensive levels separated by security boundaries devices, such as firewalls and unidirectional data diodes, at which digital communications are monitored and restricted. Systems requiring the greatest degree of security are located within the greatest number and strength of boundaries. The criteria below are utilized in the defensive architecture.

The Natrium I&C defensive model is deployed using a network architecture portrayed by a series of increasing logical isolation levels, consisting of three cyber security defensive levels of isolation: Level 4, Level 3, and Level 2, with Level 4 providing the highest level of isolation. Level 2 refers to the corporate business network. Level 1 and Level 0 are defined, respectively, as the business network interface to the internet and the internet itself.

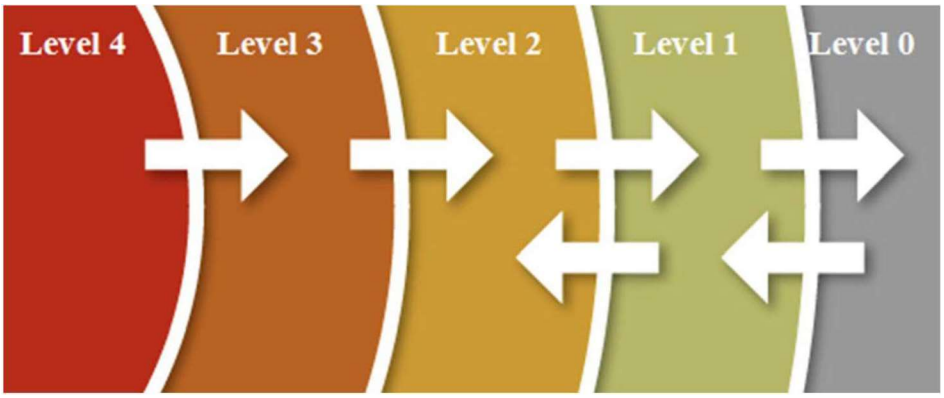


Figure 7-1: Natrium I&C Defensive Model

Figure 5-1 shows the one-way communications (data diodes) and high-level overview of the cyber security infrastructure.

Isolation between the different levels is provided by isolated (air gapped) systems, deterministic, and non-deterministic devices defined as follows:

- Deterministic Device: A deterministic device is a device that limits information flow to one direction (e.g., data diode or equivalent). This device does not allow information of any kind, including handshaking protocols, to transverse directly from networks, systems, or CDAs existing at a lower isolation level to a higher isolation level.
- Non-deterministic Device: A non-deterministic device is a device that implements a rule set to control and monitor communication across isolation levels (e.g., firewall and network-based intrusion detection system). This device is configured to implement the Information Flow Enforcement cyber security control in NEI 08-09, Revision 6 (Addendum 1), Appendix D, Section 1.4, and the rule set characteristics for non- deterministic information flow enforcement described in the Defense-In-Depth cyber security control in NEI 08-09, Revision 6 (Addendum 1), Appendix E, Section 6.

[[

]]$^{(a)(4), ECI}$

[[

]](a)(4), ECI

7.9 Human Factors Engineering

Human Factors Engineering (HFE) is implemented using the guidance of NUREG-0700, “Human-System Interface Design Review Guidelines,” and NUREG-0711, “Human Factors Engineering Program Review Model”. TerraPower has submitted a separate Topical Report for the HFE Program Plan and Methodologies [18] to the NRC for approval.

8 SUMMARY AND CONCLUSIONS

The Natrium I&C architecture is based on the plant-level risk and DID analysis which considers CCF. The architecture is developed using insights from the risk assessment performed in accordance with NEI 18-04 and SRM-SECY-22-0076. The control and monitoring functions resulting from the plant risk and DID assessment are assigned to I&C systems. One of the top goals of the architecture is simplicity. The resulting architecture meets the requirements of 10 CFR 50 for protection instrumentation by adhering to the NRC guidance documents and industry codes and standards, as applicable, and with noted exceptions. This ensures the architecture meets the fundamental I&C design principles (i.e., independence, redundancy, diversity in support of DID, and deterministic behavior).

The I&C conforms to the guidance of IEEE Std 603-2018, IEEE Std 7-4.3.2-2016, IEEE Std 384-2018 and the NRC DI&C-ISG-04 (Note: RadICS platform conforms to earlier revision of IEEE Standards).

9 REFERENCES

1. NRC SRM-SECY-22-0076 (ADAMS Accession No. ML23145A181), Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems
2. NRC Design Review Guide: Instrumentation and Controls for Non-Light-Water Reactor (Non-LWR) Reviews, February 2021 (ADAMS Accession No. ML21011A140)
3. Nuclear Energy Institute, NEI Technical Report 18-04, Revision 1, August 2019, Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light-Water Reactor Licensing Basis Development
4. Regulatory Guide 1.233, Revision 0, Guidance for a Technology Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors
5. NRC SECY-93-087 - Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs
6. IEEE Std 603-2018, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
7. RadICS Topical Report, 2016-RPC003-TR-001, Revision 2, P-A (ADAMS Accession No. ML20202A030)
8. 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks
9. TerraPower Letter to U.S. Nuclear Regulatory Commission, TP-LIC-LET-0052, Submittal of TerraPower Topical Report, “Principal Design Criteria for the Natrium Advanced Reactor” (ADAMS Accession No. ML23024A281), dated January 24, 2023
10. TerraPower Quality Assurance Program Description, TP-QA-PD-0001, Revision 14
11. IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
12. IEEE Std 384-2018, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits
13. DI&C-ISG-04, Task Working Group #4: Highly-Integrated Control Rooms- Communications Issues (HICRc), Revision 0
14. IEEE Std 7-4.3.2-2016, IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations
15. IEEE Std 379-2014, IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems
16. Regulatory Guide 1.152, Revisions 3 & 4, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
17. Nuclear Energy Institute, NEI Report 08-09, Revision 6 and Addendums, Cyber Security Plan for Nuclear Power Reactors

Not Confidential
Verify Current Revision

18. TerraPower Letter to U.S. Nuclear Regulatory Commission, TP-LIC-LET-0069, Submittal of TerraPower Topical Report, “TerraPower Human Factors Engineering Program Plan and Methodologies Topical Report” (ADAMS Accession No. ML23116A226), dated April 26, 2023

END OF DOCUMENT