



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

**TERRAPOWER, LLC – DRAFT SAFETY EVALUATION OF TOPICAL REPORT NAT-4950,
“INSTRUMENTATION AND CONTROL ARCHITECTURE AND DESIGN BASIS TOPICAL
REPORT”, REVISION 2 (EPID L-2024-TOP-0006)**

SPONSOR AND SUBMITTAL INFORMATION

Sponsor: TerraPower, LLC
Sponsor Address: 15800 Northup Way, Bellevue, WA 98008
Project No.: 99902100
Submittal Date: March 7, 2024

Submittal Agencywide Documents Access and Management System (ADAMS) Accession Nos.: ML24068A186; ML24305A009

Brief Description of the Topical Report: By letter dated March 7, 2024, TerraPower, LLC (TerraPower) submitted Topical Report (TR) NAT-4950 Revision 1, “Instrumentation & Control Architecture and Design Basis Topical Report,” (ML24068A186) to the U.S. Nuclear Regulatory Commission (NRC) staff. By email dated April 15, 2024 (ML24101A204), the NRC staff informed TerraPower that the TR provided sufficient information for the NRC staff to begin its detailed technical review. On June 24, 2024, the NRC staff transmitted an audit plan to TerraPower (ML24163A003) and subsequently conducted an audit of materials related to the TR from July 8, 2024, to September 30, 2024. The audit summary report was issued on March 7, 2025 (ML25015A128). On October 30, 2024, TerraPower submitted a revision of the TR (ML24305A009) to clarify portions of the TR as discussed in the audit summary.

The Instrumentation and Control (I&C) Architecture and Design Basis TR describes the overall architecture and associated design basis including (1) compliance with Institute of Electrical and Electronics Engineers (IEEE) Std 603, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, and (2) the process for I&C relationship to plant-level lines of defense, structure, system, and component (SSC) classification, and I&C functions basis and allocation to individual systems. The TR also describes the I&C integrated network, individual I&C systems, application of fundamental design principles, and secure I&C.

REGULATORY EVALUATION

1. Regulatory Requirements

Under the provisions of *Title 10 of the Code of Federal Regulations* (10 CFR) Part 50, “Domestic Licensing of Production and Utilization Facilities,” and 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants,” applicants for a construction permit (CP), operating license, standard design certification, combined license, standard design approval, or manufacturing license must submit Principal Design Criteria (PDC) for the proposed facility. PDCs establish the necessary design, fabrication, construction, testing, and performance design criteria for SSCs important to safety to provide reasonable assurance that the TerraPower Sodium design could be operated without undue risk to the health and safety of the public.

10 CFR 50.55a(h), “Protection and safety systems,” incorporates the 1991 version of IEEE Std. 603, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” by reference, including the correction sheet dated January 30, 1995. IEEE Std. 603-1991 establishes minimum functional design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems.

10 CFR 73.54, “Protection of digital computer and communication systems and networks,” requires, in part, that NRC licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks.

10 CFR Part 50, appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,” establishes quality assurance requirements for the design, fabrication, construction, testing, and operation of the SSCs of a facility.

2. Regulatory Guidance

SRM-SECY-22-0076, “Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems,” (ML23145A176) approved the NRC staff’s recommendation in SECY-22-0076, “Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems,” (ML22193A290) with edits and provided direction to the NRC staff on risk-informing assessment of potential common-cause failures (CCFs) in safety related digital I&C systems.

Regulatory Guide (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,” Revision 0, (ML20091L698), provides the NRC staff’s guidance regarding using a technology-inclusive, risk-informed, and performance-based methodology to inform the licensing basis and content of applications for non-light-water reactors (non-LWRs). It endorses, with clarifications, Nuclear Energy Institute (NEI) 18-04, “Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development,” Revision 1, (ML19241A472), as one acceptable method for informing the licensing basis and determining

the appropriate scope and level of detail for parts of applications for licenses, certifications, and approvals for non-LWRs.

NEI 18-04 presents a technology-inclusive, risk-informed, and performance-based process for selection of licensing basis events (LBEs), classification of SSCs and associated special treatments and programmatic controls, and determination of defense-in-depth (DID) adequacy for non-LWRs. It provides applicants one acceptable method for informing the licensing basis and content of applications regarding the forementioned topics above.

Design Review Guide (DRG): "Instrumentation and Controls for Non-Light-Water Reactor (Non-LWR) Reviews," (ML21011A140). This document provides guidance for the NRC staff to use in reviewing the I&C portions of applications for advanced non-LWRs within the bounds of existing regulations.

RG 1.253, "Guidance for a Technology-Inclusive Content of Application Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors," Revision 0 (ML23269A222). This document was published after the Topical Report was submitted however it provides guidance for a technology-inclusive methodology to inform the licensing basis and content of applications for non-light-water reactors.

TECHNICAL EVALUATION

Consistent with the purpose of the TR, the NRC staff focused its review regarding the proposed Sodium I&C systems on the overall architecture and associated design basis. The TR is based on preliminary I&C systems design. In addition, the NEI 18-04 process, including the probabilistic risk assessment (PRA), is an iterative process and has not yet been fully implemented for the proposed Sodium design. Therefore, the NRC staff's review emphasis was on whether the I&C system architecture and associated design basis described in the TR can be used to support the compliance with the relevant regulatory requirements and the conformance with SRM-SECY-22-0076 for the prospective Sodium reactor licensing applications under 10 CFR Parts 50 or 52 regarding its I&C design.

TerraPower states that this TR is primarily based on the NEI 18-04 methodology, the DRG, IEEE Std 603-2018, and the Commission's direction in SRM-SECY-22-0076. The NRC staff used the DRG as the primary review guidance for the TR.

1. Evaluation of Instrumentation and Control Systems Overview (Section 4 of the TR)

I&C Architecture Design Bases

Section 4.1, "I&C Architecture Design Bases", of the TR provides an overview of the design bases for the I&C architecture for the Sodium design. For the design bases, this section of the TR provides the regulatory requirements, regulatory guidance, and industry codes and standards TerraPower used for development of the architecture. The TR notes that 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 TR.

As discussed in the DRG for I&C, the NRC staff's review approach for an I&C design starts with the evaluation of the proposed overall I&C architecture. The overall I&C architecture and systems design should demonstrate the reliability and robustness of the proposed I&C design. Certain regulatory requirements provide provisions or design constraints that directly or

indirectly influence the I&C architecture. The NRC staff concludes that the regulatory requirements, regulatory guidance, and industry codes and standards listed in the TR are important and influence the I&C architecture based on past review experiences.

In particular, 10 CFR 50.55a(h) incorporates by reference IEEE Std 603-1991 with the 1995 correction sheet, which includes technical requirements such as single failure criterion, independence, and control of access that directly influence the I&C system architecture. Similarly, the Natrium PDCs also include design criteria for safety-significant I&C systems that influence the I&C system architecture. The proposed Natrium power plant follows the PDCs discussed in the TR "Principal Design Criteria for the Natrium Advanced Reactor" (ML24283A066).

In addition, the TR discusses conformance with applicable regulatory guidance, industry standards, and additional guidance used or considered for the development of the architecture.

The NRC staff concludes that the design bases for the proposed Natrium I&C systems architecture are reasonable and an I&C systems architecture developed based on these design bases can lead to a reliable and robust I&C systems design.

As noted in the TR, additional requirements and guidance documents may be applicable to the individual I&C systems and will be described by a licensee or applicant referencing this TR.

Use of IEEE Std 603-2018 Instead of IEEE Std 603-1991

The TR states that the Natrium I&C uses IEEE Std 603-2018 instead of IEEE Std 603-1991 referenced in 10 CFR 50.55a(h). The NRC staff has neither endorsed IEEE Std 603-2018 nor incorporated it by reference into 10 CFR 50.55(a)(h). During the regulatory audit, the NRC staff questioned the potential need for an alternative request under 10 CFR 50.55a(z), or an exemption request under 10 CFR 50.12, "Specific Exemptions," in order to use the version of the IEEE Std different from that incorporated by reference in 50.55a(h). The TR states that TerraPower performed a comparison of the 1991 and 2018 versions of IEEE Std 603 and found that the latter meets or exceeds the requirements of the former incorporated into 10 CFR 50.55a(h). During the regulatory audit, the NRC staff reviewed the comparison file in the electronic reading room and found that the 2018 version is very similar to the 1991 version but there are some differences. Without a formal and systematic review by the NRC of the 2018 version as part of the 10 CFR 50.55a(h) rulemaking to incorporate it by reference, or potentially a revision to RG 1.153, "Criteria for Safety Systems," Revision 1 (ML003740022) to endorse it, it is premature to conclude that the 2018 version meets or exceeds the requirements of the 1991 version incorporated into 10 CFR 50.55a(h). Based on a question and ensuing discussions during the regulatory audit on this subject, TerraPower revised the TR to include a clarification on the use of the 2018 version regarding the compliance with IEEE Std 603-1991 as incorporated by reference in 10 CFR 50.55a(h).

Based on the above, the NRC staff concludes that an applicant or licensee referencing the TR, based on the use of IEEE Std 603-2018, should describe the conformance of their I&C systems design to IEEE Std 603-1991. This is consistent with the guidance in section X.3, Mapping to Regulations and Guidance, of the DRG and will support the NRC staff's review of the design regarding its compliance with 10 CFR 50.55a(h), which incorporates the 1991 version of the standard. The NRC staff also notes that the RadICS platform, used for the safety-related Reactor Protection System (RPS), conforms 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. A licensee or applicant referencing this TR will submit a separate cyber security plan as required by regulation.

I&C Relationship to Plant-Level Lines of Defense

Section 4.2, "I&C Relationship to Plant-Level Lines of Defense," of the TR discusses how the I&C systems and their functions are related to the plant-level lines of defense. TerraPower follows the risk-informed and performance-based methodology in NEI 18-04, which includes the process for evaluating the adequacy of DID using risk insights from the PRA. The DID 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 in the TR shows that no single layer, function, or feature is specifically relied upon to mitigate the postulated initiating event. The TR describes the concept of defense lines 1 through 5 in figure 4-1, "Defense Line Concept," and discusses the details on how the defense lines are used in combination with the DID approach discussed in Chapter 5, "Evaluation of Defense-in-Depth Adequacy," of NEI 18-04.

The I&C systems are an integral part of the overall plant, and the plant-level DID adequacy evaluation under the NEI 18-04 methodology should appropriately consider the I&C systems. The NRC staff concludes that the defense lines concept in the TR is a reasonable way of evaluating the DID adequacy because the concept is consistent with the guidance in section X.2.2.1, "Defense-in-Depth Measures," of the DRG regarding DID measures for I&C and TerraPower follows the NEI 18-04 methodology for the overall plant.

However, the NRC staff notes that the I&C design for this TR is preliminary and that the NEI 18-04 methodology has also been not fully implemented. The TR states in section 4.2 that "The licensee or applicant referencing this [TR] 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 [Safety Classification Process]." An applicant for a CP under 10 CFR Part 50 should be able to reference this TR if the application is based on a preliminary design (i.e., not seeking a finality determination from the NRC) and following RG 1.253, "Guidance for a Technology-Inclusive Content of Application Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors," Revision 0 (ML23269A222).

Safety Classification Process

Section 4.3 of the TR discusses the SSC classification process and the classification of I&C systems. The I&C systems are classified as Safety-Related (SR), Non-Safety-Related with Special Treatment (NSRST), or Non-Safety-Related with No Special Treatment (NST) based on the plant-level SSC classification process consistent with the guidance of NEI 18-04. The TR states that 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. Table 4-5, "Instrumentation and Control System Classification," of the TR lists individual I&C systems and their classifications. The proposed Natrium power plant's integrated digital-based I&C design is

based on the I&C architecture, discussed in section 5, "Instrumentation and Control Integrated Network," of the TR, that supports a plant-level DID framework using the NEI 18-04 methodology that leads to system classification based on the significance of the system safety functions. The NRC staff concludes that the I&C systems classification process is reasonable because the process reflects the guidance in NEI 18-04 regarding SSC classification. The NRC staff also concludes that the classification of the I&C systems in Table 4-5 is reasonable based on the description of the I&C systems and their safety functions in section 6, "Instrumentation and Control Systems," of the TR.

However, the NRC staff notes that the I&C systems design for this TR is considered preliminary and that the NEI 18-04 methodology has also been not fully implemented. The TR states in section 4.2 that "The licensee or applicant referencing this TR 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."

The TR also has a footnote regarding the NSRST Anticipatory Automatic Seismic Trip System (AST) that states "The licensee or applicant referencing this TR will provide the AST architecture including interface with RTBs [Reactor Trip Breakers]." Therefore, the NRC staff's review of the TR did not include the AST architecture.

Function Allocation to I&C Systems

Section 4.4, "Function Allocation to I&C Systems," of the TR discusses the process for the I&C systems function allocation. The process is iterative through the design development process and consistent with the NEI 18-04 methodology. The design control and change process is described in TP-QA-PD-0001, Revision 14-A TerraPower Quality Assurance Program Description (QAPD), (ML23213A199). The list of functions and classification of the SSCs are finalized at the end of the design phase using the NEI 18-04 methodology and subject to the change control process. The TR notes that additional requirements are applied to I&C due to regulatory and stakeholder requirements.

The NRC staff concludes that the process for the I&C systems function allocation is reasonable because the process reflects the guidance in NEI 18-04 regarding identification of safety functions for SSCs.

2. Evaluation of I&C Integrated Network and I&C Systems (Sections 5, 6 & 7 of the TR)

Section 5 of the TR discusses the overall I&C architecture of the proposed TerraPower Sodium reactor and section 6 of the TR describes the Sodium I&C systems that make up the integrated Sodium I&C architecture network. I&C architecture for the Sodium plant primarily consists of nuclear island control system (NIC) implemented on a distributed control system (DCS) platform, and RPS implemented using RadICS platform. TR figure 5-1, "Overall I&C Architecture Diagram," depicts the architecture design is consistent with five layers of defense discussed in table 5-2, "Guidelines for Establishing the Adequacy of Overall Plant Capability Defense-in-Depth," of NEI 18-04 and illustrated in TR figure 4-1, "Defense Line Concept." I&C design functions in relationship to plant level lines of defense for the defense Lines 2, 3, and 4 I&C are clearly defined in section 4.2 of the TR. Communication paths between all components of the architecture are clearly shown and identified in TR figure 5-1. Fundamental I&C design principles of independence and redundancy for the safety-related RPS are evaluated below. Applicable fundamental I&C design principles for the safety-related RPS platform (defense Line 3) are described in the 2016-RPC003-TR-001, "RadICS Topical Report," Revision 2, P-A

(ML20202A030).

Section 6.2, "Reactor Protection System", of the TR discusses the RPS design. The primary function of the RPS is to automatically initiate safety-related functions, scram, and engineered safety features (ESF). Section 6.3, "Nuclear Instrumentation System," and figure 6-4, "XIS Block Diagram," of the TR discuss the nuclear instrumentation system (XIS) that provides neutron flux signals to RPS and NIC for protective, control, and monitoring functions. The RPS initiates automatic scram at following process parameters:

- 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

A reactor scram signal de-energizes all control rod solenoids allowing the control rod assemblies to fall into the reactor core via gravity. Provisions for operator initiated manual scram are provided in the main control room. This operator manual action is not credited in the preliminary safety analysis report.

The RPS is designed to initiate ESF functions to support Required Safety Functions (RSF) related to heat removal during postulated accidents. The RPS automatically initiates ESF functions at following process parameters:

- Primary Sodium Pump (PSP) Trip on High Cold Pool Temperature with Reactor Scram and Low Neutron Flux
- Intermediate Sodium Pump (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
- Sodium Processing System (SPS) Pump Trip on Low Primary Sodium Level

The NRC staff confirmed that the RadICS platform has the capacity to handle the number of functions assigned to each channel for the proposed Sodium RPS design.

Section 6.7, "Nuclear Island Control System," and figure 5-1 of the TR describe the NIC, which is a group of I&C sub-systems that perform NST and NSRST control and monitoring functions. The NIC also controls vendor supplied skid mounted components via communication interfaces with the DCS. The following subsystems are considered part of the NIC:

- 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)

3. RPS Redundancy

Section 7.3, “Redundancy,” figure 5-1, and figure 6-1, “RPS Block Diagram,” of the TR demonstrates RPS design’s conformance to the fundamental I&C design principle of redundancy. Redundancy in the RPS design consisting of four separate and independent divisions of sensors and logic solvers assures that single failure in the RPS will not prevent performance of any RSF. The RPS design presented in the TR meets the single failure criterion of IEEE Std 603-1991, section 5.1, “Single-failure criterion.” Redundancy design capabilities of the RadICS platform that is used for the Natrium RPS architecture is evaluated in the NRC staff-approved RadICS TR, 2016-RPC003-TR-001 for meeting the requirement of IEEE Std 603-1991, section 5.1. Based on its review using the DRG, the NRC staff concludes that there is adequate redundancy in the RPS design such that a single failure would not result in loss of any RSF, and the RPS design meets the relevant requirements of IEEE Std 603-1991.

4. Natrium I&C System Independence

Section 5.4, “Communications,” section 7.1, “Independence,” figure 5-1, and figure 6-1 of the TR demonstrate the RPS design’s conformance to the fundamental I&C design principle of independence, such that a failure in NSRST or NST I&C systems does not result in loss of any RSF. Safety-related isolation devices, shown as part of the RPS, are used between the SR RPS and NSRST/NST NIC components. Section 7.1 states that the RPS maintains independence, including physical separation and electrical isolation, between redundant RPS divisions in accordance with IEEE Std 603-1991, section 5.6, IEEE Std 384, and RG 1.75, “Criteria for Independence of Electrical Safety Systems,” Revision 3, (ML043630448). There is no data communication from NSRST/NST I&C systems to SR I&C systems. One-way data communication from SR I&C systems to NSRST/NST I&C systems is via isolated hardware or through data diode and gateways. One-way RPS inter-divisional communication for coincidence voting is performed using RadICS platform communication protocols and methods described in the RadICS platform TR. Based on its review using the DRG, the NRC staff concludes that physical and electrical separation in the Natrium I&C architecture, as described in the TR and RadICS platform inter-divisional data communication independence evaluated in the NRC staff-approved RadICS TR, 2016-RPC003-TR-001, meet the independence requirements of IEEE Std 603-1991, and a failure in NSRST or NST I&C systems would not result in loss of any RSF.

5. Diversity

Conformance with Commission Expectations Regarding Common Cause Failures in SRM-SECY-22-0076

Section 7.4.1, “SECY-22-0076,” of the TR addresses the four-point expanded policy in SRM-SECY-22-0076 for staff review of applications involving digital I&C systems. In summary, TerraPower implements the policy using the NEI 18-04 methodology. The DID adequacy evaluation under the methodology is at a plant-level and encompasses the I&C system DID. The NRC staff concludes that the overall approach to address the four points of SRM-SECY-22-0076 is reasonable because it is consistent with RG 1.233 and the DRG regarding DID adequacy evaluation that includes potential I&C system CCF vulnerabilities.

Regarding Point 3 of the SRM, the TR includes some details and preliminary results. Using the defense-line approach, discussed in section 4.2 of the TR, TerraPower states that the Natrium

design features are adequate to address CCF. The design features include the RPS internal diversity (discussed in the RadICS TR safety evaluation report) and diverse Sodium Processing System Pump, Primary Sodium Pump, and Intermediate Sodium Pump shutdown and trip. The NEI 18-04 evaluation of the Natrium design shows that the event sequences involving the CCF of the RPS or that of other I&C systems with the RPS working are below 1E-4 per plant year. Based on that, the TR states that, if needed, the diverse system to mitigate CCF can thus be non-safety-related (e.g., NSRST SSCs). With the CCF of the RPS being the primary concern, TerraPower evaluates and demonstrates the DID adequacy for the event sequences involving the RPS CCF using the defense-line approach discussed in section 4.2 of the TR. The NRC staff concludes that TerraPower's approach to address Point 3 of the SRM is reasonable because it is consistent with the SRM and follows RG 1.233. In addition, the NRC staff concludes that the preliminary results indicate the potential CCF, as evaluated as part of the event sequence assessment under the NEI 18-04 methodology, can be reasonably prevented or mitigated or is not risk-significant.

The NRC staff evaluated the diversity of the RadICS platform during the review of the associated platform generic TR and noted in its safety evaluation (SE) that the platform includes diversity features, such as internal diversity using different digital technologies, that could mitigate the potential CCF vulnerabilities; however, the NRC staff concluded in the SE that a plant-specific evaluation must be performed at the time of application development and imposed a plant-specific action item (i.e., PSAI 7.9) for applicants or licensees referencing the platform TR.

Regarding Point 4 of the SRM, TerraPower defines the risk-informed critical safety functions to be the RSFs defined in NEI 18-04. An RSF is a PRA Safety Function that is required to be fulfilled to maintain the consequence of one or more DBEs or the frequency of one or more high-consequence BDBEs inside the F-C Target. The NRC staff concludes that the definition within the context of Point 4 of the SRM is reasonable because RSFs are a subset of PSFs modeled in PRA that are critical to maintain the consequence of important event sequences inside the frequency-consequence target in NEI 18-04. TerraPower provides examples of diverse manual controls in the TR but states that licensees or applicants referencing the TR will provide the complete listing. The TR also notes that the post-accident monitoring (PAM) instrumentation requirements as part of the Point 4 discussion. Section 6.8, "Post-Accident Monitoring," of the TR states that 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 and the I&C system does not have any Type A PAM variables since there are no specific safety functions that require manual action during DBAs.

Section 7.4.2, "Sensor Diversity," of the TR addresses sensor diversity and states that most Class 1E sensors that provide input to RPS are analog and not subject to software CCF. However, if redundant sensors are selected that contain a programmable digital device, then applicants or licensees referencing this TR are required to use one of the following methods 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 proposed Natrium power plant design shares some sensors among various functions that may reside in different defense lines. An applicant or a licensee referencing this TR is required to perform an analysis (e.g., hazard analysis) as part of the NEI 18-04 methodology

implementation 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.

6. System Integrity & Deterministic Performance

Section 7.5, "System Integrity," of the TR describes how the RPS design conforms to the fundamental I&C design principle of deterministic behavior. The TR references the RadICS TR, which has been previously evaluated by the NRC staff, for the predictability and repeatability of design features of the platform consistent with IEEE Std 603-1991 clause 5.5, and IEEE Std 7-4.3.2 clause 5.5. Hence the digital portions of the Sodium RPS design exhibit the following system integrity capabilities:

- 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.

Section 7.5.1, "Deterministic," of the TR further states that the RadICS modules perform their intended function in accordance with predefined times and do not use interrupts; as such, the system operates deterministically. In the SE for the RadICS TR, the NRC staff has reviewed and accepted the deterministic behavior of the RadICS system. Based on this deterministic behavior of the RadICS platform, the selected maximum response time of the system will not change and is predictable. The response times are verifiable during the factory acceptance testing. Applicants or licensees referencing this TR must assure that the assumed response times for RSFs in the safety analysis account for the overall I&C system response time, including the RPS digital portions (RadICS platform) and the input sensors.

Consistent with RadICS TR and the IEEE Std 603-1991 clause 5.2, the RSFs once initiated automatically or manually by the RPS, the intended sequence of protective actions of the execute features will continue until completion.

7. Simplicity

Section X.1.2, "Architecture Assessment Review Criteria," of the DRG states that the overall I&C architecture and architecture of individual systems should be simplified to the extent practical, and simplicity should be a cross-cutting concept that supports the fundamental I&C design principles for developing I&C systems with high reliability. Compared to simple systems and architectures, it is more difficult to demonstrate that complex I&C systems and architectures conform to fundamental I&C design principles such as independence; however, it is difficult to define and control simplicity and complexity. But from a safety perspective, the simpler design options are those that accomplish the safety function and address potential hazards while exhibiting the following properties: (1) the I&C system architecture design is as simple as practical; (2) any added complexity provides a safety benefit; and (3) any added complexity does not diminish the design's conformance to the fundamental I&C design principles. As such, designs that incorporate this concept will facilitate the NRC staff's efficient I&C architecture evaluation.

Consistent with concepts of simplicity discussed in the DRG, the Sodium I&C architecture

presented in the TR exhibits the simplicity properties identified in the DRG. Independence and separation of the safety-related RPS from the NSRST/NST NIC, and no data communications from NIC to RPS and between independent RPS channels demonstrates adequately simple I&C architecture that allow for efficient evaluation by the NRC staff.

8. Reliable I&C

Section 7.7, "Reliable I&C," of the TR outlines some of the design features that contribute to reliable safety-related I&C systems, such as meeting the single failure design criteria in accordance with requirements of IEEE Std 603, section 5.1 and IEEE Std 379, "IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems." The Natrium TR claims that the I&C systems meet the reliability goals established by the PRA. The reliability of the systems is demonstrated qualitatively and quantitatively in the TR.

The NRC staff concludes that the qualitative reliability arguments made in the TR are reasonable for reliability of the safety application software, and the software used for the development of the safety digital devices. The goal of software reliability is to demonstrate that the software is robust and fault free. To ensure that I&C systems (and software) perform the intended functional requirements reliably under the defined plant conditions, the TR section 7.7.2, "Qualitative Reliability," lists measures and features for digital system development, which the NRC staff concludes are acceptable because they include a comprehensive set of design, process, programmatic, and operational activities that should lead to a reliable I&C system.

For the quantitative reliability of the I&C system, TR section 7.7.1, "Quantitative Reliability," states that 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 TR is required to define the quantitative reliability targets and special treatments for the I&C systems as part of the NEI 18-04 methodology implementation.

9. Secure Instrument and Control

The NRC staff reviewed the TR as it relates to the requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks," which is also known as the Cyber Rule. In 2009, the Cyber Rule was published and consists exclusively of performance-based requirements (74 FR 13926). Below are major highlights of these requirements:

- a) Submit a Cybersecurity Plan (CSP) and an implementation schedule which satisfies rule requirements for approval.
- b) Protect digital computer, systems, and networks associated with Safety, Security, and Emergency Preparedness (SSEP) functions against cyber-attacks. More specifically, SSEP relates to Safety-related functions, important-to-safety functions, Security functions, emergency preparedness functions, and support systems.
- c) Maintain DID strategies, capability to detect, respond to, and recover from cyberattacks.
- d) Ensure that SSEP functions are not adversely impacted due to cyberattacks.
- e) Ensure personnel are trained.

10 CFR 73.54 does not require specific cybersecurity design features; however, by reviewing

the performance-based requirements, applicants may determine cybersecurity design features they may wish to incorporate during the design stage of development.

TerraPower in its TR committed to the following cybersecurity design features:

- a) A licensee or applicant referencing this TR will submit a separate CSP as required by regulation.
- b) To include cybersecurity features in the design to allow the plant to readily implement the Cyber Rule requirements and controls.
- c) To establish a secure, I&C development and operation environment and to develop processes and programs for establishing a secure operational environment.
- d) To establish cybersecurity DID protective strategies.

The NRC staff in consideration of the above commitments makes no specific findings relative to the TR in relation to the Cyber Rule requirements in 10 CFR 73.54.

LIMITATIONS AND CONDITIONS

The NRC staff identified the following limitations and conditions applicable to any licensee or applicant referencing this TR:

1. Applicants or licensees referencing this TR will need to address the areas which are not evaluated by the TR with respect to I&C architecture and design basis. As an example, section 4.3 of the TR states that an applicant or licensee referencing the TR “will provide the AST architecture including interface with RTBs.” An applicant or licensee referencing the TR must submit documentation and justify that the activities have been completed to a state that is appropriate for the intended licensing application.
2. Because this TR is based on a preliminary design and partial implementation of the Licensing Modernization Project (LMP), an applicant or licensee referencing this TR must utilize the NEI 18-04 methodology as the I&C system design matures and provide justifications for areas that deviate from the TR.
3. Applicants or licensees referencing this TR outside the context of an LMP-based approach must describe how the TR remains applicable outside of an LMP-based context and, as appropriate, supplement the TR as needed.
4. Because this TR relies on the NRC staff-approved RadICS TR 2016-RPC003-TR-001, Revision 2, P-A, an applicant or licensee referencing this TR must fully address that applicable generic open items and plant-specific action items in the RadICS TR and provide justifications for items that are not applicable.

CONCLUSION

The NRC staff has completed its review of TR NAT-4950, Revision 2. The NRC staff concludes that, subject to the limitations and conditions discussed above, the I&C systems architecture and associated design basis in the TR can be used to support the prospective Sodium reactor licensing applications under 10 CFR Parts 50 or 52 regarding their I&C design and its compliance with the applicable regulatory requirements and SRM-SECY-22-0076. This conclusion is based on the technical evaluation above where the NRC staff determined that the I&C systems architecture and associated basis is generally consistent with the guidance in the

DRG, RG 1.233, and SRM-SECY-22-0076.

Project Managers: Roel Brusselmans, NRR
 Stephanie Devlin-Gill, NRR
 Mallecia Sutton, NRR

Principal Contributors: Dinesh Tenaja, NRR
 Ian Jung, NRR
 Joseph Ashcraft, NRR
 Calvin Cheung, NRR
 Ralph Costello, NSIR

Date: 3/24/2025

References

- U.S. Nuclear Regulatory Commission, Regulatory Guide 1.233, “Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors,” dated June 2020, (ML20091L698)
- Nuclear Energy Institute 18-04, “Risk-Informed Performance-Based Technology-Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development,” Revision 1, dated August 2019, (ML19241A472)
- U.S. Nuclear Regulatory Commission, Regulatory Guide 1.253, “Guidance for a Technology-Inclusive Content of Application Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Advanced Reactors,” (ML23269A222)
- NEI 21-07, Revision 1, “Technology Inclusive Guidance for Non-Light Water Reactors Safety Analysis Report Content for Applicants Using the NEI 18-04 Methodology,” dated February 2022, (ML22060A190)
- U.S. Nuclear Regulatory Commission, Design Review Guide (DRG): Instrumentation and Controls for Non-Light Water Reactor (Non LWR) Reviews,” Washington DC, dated February 26, 2021, (ML21011A140)
- U.S. Nuclear Regulatory Commission, “Staff Requirements—SECY-22-0076—Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems,” dated May 25, 2023, (ML23145A181 and ML23145A182)
- U.S. Nuclear Regulatory Commission, SECY-22-0076, “Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems,” dated August 10, 2022, (ML22193A290)
- U.S. Nuclear Regulatory Commission, Supplement to SECY-22-0076, ‘Expansion of Current Policy on Potential Common Cause Failures in Digital Instrumentation and Control Systems,’” dated January 23, 2023, (ML22357A037)
- U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities,” U.S. Nuclear Regulatory Commission, Washington, DC
- RadICS Topical Report, 2016-RPC003-TR-001, Revision 2, P-A, (ML20202A030)
- TerraPower Topical Report, “Principal Design Criteria for the Sodium Advanced Reactor” NATD-LIC-RPRT-0002-A, Revision 1, dated October 8, 2024, (ML24283A066)
- TerraPower “Quality Assurance Program Description,” TP-QA-PD-0001-A, Revision 14, (ML22266A286)
- IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

- IEEE Std 603-2018, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

SUBJECT: TERRAPOWER, LLC – DRAFT SAFETY EVALUATION OF TOPICAL REPORT
NAT-4950, “INSTRUMENTATION AND CONTROL ARCHITECTURE AND
DESIGN BASIS TOPICAL REPORT,” REVISION 1 (EPID L-2023-TOP-0055)
DATED: MARCH 24, 2025

DISTRIBUTION:

PUBLIC
RidsOgcMailCenter Resource
RidsNrrDanu Resource
RidsNrrDanuUal1 Resource
DGreene, NRR
SDevlin-Gill, NRR
RBrusselmans, NRR
JBorromeo, NRR
MSutton, NRR
DAtkinson, NRR
RAnzalone, NRR
IJung, NRR
CCheung, NRR
DTaneja, NRR

ADAMS Accession Nos.:

Pkg: ML25036A028

Email: ML25036A035

Enclosure (Public): ML25036A030

NRR-043

OFFICE	NRR/DEX/EICB:TR	NRR/DEX/EICB:BC	NRR/DANU/UAL1:PM
NAME	DTaneja	FSacko	RBrusselmans
DATE	2/3/2025	2/3/2025	2/5/2025
OFFICE	NRR/DANU/UAL1:LA	OGC:NLO	NRR/DANU/UAL1:BC
NAME	DGreene	JEzell	JBorromeo
DATE	2/13/2025	3/5/2025	3/24/2025
OFFICE	NRR/DANU/UAL1:PM		
NAME	RBrusselmans		
DATE	3/24/2025		

OFFICIAL RECORD COPY