TERRAPOWER, LLC – AUDIT PLAN FOR TOPICAL REPORT "INSTRUMENTATION AND CONTROL ARCHITECTURE AND DESIGN BASIS TOPICAL REPORT," REVISION 1 (CAC / EPID NO.00431 / L-2024-TOP-0006)

Applicant:	TerraPower, LLC
Applicant Address:	15800 Northup Way, Bellevue, WA 98008
Plant Name:	Natrium
Project No.:	99902100

Background:

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" (Agencywide Documents Access and Management System (ADAMS) Accession No. ML24068A186) to the U.S. Nuclear Regulatory Commission (NRC) staff. The TR describes TerraPower's overall architecture related to Instrumentation and Control (I&C). It also addresses the associated design basis and the process for I&C's relationship to lines of defense, structure, system, and component (SSC) classification, and I&C functions basis and allocation to individual systems. On April 15, 2024, the NRC staff found that the material presented in the TR provides technical information in sufficient detail to enable the NRC staff to conduct a detailed technical review (ML24101A204).

TerraPower has requested the NRC staff's review and approval of the I&C architecture and design basis methodology as presented in the subject TR for potential use by future applicants, where applicable. In addition to the regulatory approach highlighted below in "Regulatory Audit Basis", the applicant's licensing methodology related to I&C architecture and design basis follows industry standards and regulatory guidance related to I&C architecture and also I&C functionality, safety classification, and plant-level functional requirements are based on a risk-informed approach and application of diversity and defense in depth (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," Revision 1 (ML19241A472).

Purpose:

The purpose of the audit is for the NRC staff to gain a more detailed understanding of TerraPower's I&C architecture and design basis methodology, which is referenced in the construction permit application for the proposed Kemmerer Power Station Unit 1 site near Kemmerer, Wyoming. This audit and corresponding topical report are also being developed for future applicants seeking to utilize this topical report. An additional purpose of the audit is to identify any information that will require docketing to support the NRC staff's safety evaluation of the subject TR. Therefore, the NRC staff is requesting access to TerraPower documents associated with the I&C architecture and design basis as discussed in the TR. The NRC staff will summarize its observations in an audit report to be provided to TerraPower, as discussed below.

Regulatory Audit Basis:

The basis for this audit includes:

Under the provisions of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities," applicants for a construction permit and operating license must submit Principal Design Criteria (PDCs) 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 a facility referencing this topical report could be operated without undue risk to the health and safety of the public.

10 CFR 50.55a(h), incorporates the 1991 version of Institute of Electrical and Electronics Engineers (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 U.S. 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, manufacture, construction, and operation of those structures, systems, and components.

Regulatory Guidance

SRM-SECY-22-0076, "Staff Requirement – SECY-22-0076 – Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems," (ML23145A181) dated May 25, 2023, 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.

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, NEI 18-04 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 determination of 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 Control 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.

Regulatory Audit Methodology:

The regulatory audit will follow the guidance in Nuclear Reactor Regulation Office Instruction LIC-111, "Regulatory Audits," Revision 1 (ML19226A274), and focus on information provided by TerraPower in the electronic reading room.

Information and Other Material Necessary for the Regulatory Audit:

Specific audit information needs and questions include but are not limited to the following:

1. Explain how TerraPower plans to address 'preliminary information' provided/discussed in the topical report. Describe the scope of the topical report in this context.

An example is contained within section 4.2, "I&C Relationship to Plant-Level Lines of Defense," which states that "This topical report provides preliminary list of functions assigned to the Reactor Protection System (RPS) (see Section 6.2). The licensee or applicant referencing this topical report will provide the list of functions, defense lines, classifications, and assignment to the I&C systems based on the DID analysis and [probabilistic risk assessment (PRA)] process described in this section and Section 4.3."

- 2. Sections 1.0 and 2.0, "Purpose" and "Scope," state that this topical report identifies I&C relationship to plant-level lines of defense, safety classification, and function allocation to I&C systems. Since plant-level lines of defense information has not yet been reviewed and approved by the NRC staff, the design basis for I&C systems can't be finalized. Similar to question 1, please discuss how TerraPower proposes to address impacts to the I&C system design basis while the plant-level design bases are undergoing the iterative design process.
- 3. Section 3.0, "Background," states: "In recent years, the industry and the NRC started incorporating risk-based decision-making into plant process and programs (e.g., maintenance and fire protection)."

The expression "risk-based" is not consistent with the NRC's approach, which is rather "risk-informed." The Commission, in SRM-SECY-98-144, "White Paper on Risk-Informed and Performance-Based Regulation," (ML003753601) states that "… the Commission does not endorse an approach that is "risk-based"; however, this does not invalidate the use of probabilistic calculations to demonstrate compliance with certain criteria, such as dose limits." Consistent with the Commission policy, the industry and the NRC have been increasingly developing and using the risk-informed (and performance-based) approaches to the regulation of nuclear reactors. This expression "risk-based" is repeated in the topical report. Was the use of the term "risk-based" a typographical error?

4. Section 3.0, "Background," states: "The SRM-SECY-22-0076 approach is consistent with NEI 18-04."

As discussed in SECY-23-0092, "Annual Update on Activities to Modernize the U.S. Nuclear Regulatory Commission's Digital Instrumentation and Controls Regulatory Infrastructure and License Amendment Requests," (ML23228A226) the Staff Requirements Manual's (SRM) language does not clearly connect to NEI 18-04 and the "DRG: Instrumentation and Control for Non-LWR Reviews" e.g., "critical safety function." Thus, the topical report's statement above is not considered accurate and should be rephrased. One option is to use the following statement instead:

"The SRM-SECY-22-0076 approach can be implemented using the NEI 18-04 methodology and the guidance in DRG."

5. Section 4, "Instrumentation and Control Systems Overview," states on Page 9 of 43 that "The preliminary outcome of the DID process (e.g., I&C functions list and DLs [Defense Lines]) 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 topical report will provide the final version of the information noted as preliminary."

a. Clarify the statement in section 4.0 which states that due to the RadICS platform, a diverse system is not needed to address Common Cause Failure (CCF). RadICS states under Branch Technical Position (BTP) BTP 7-19, "Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure Due to Latent Design Defects in Digital Safety Systems" (ML20339A647) that a plant specific design (plant specific action item (PSAI) 7.9) should meet or support criteria of BTP 7-19. Section 7.4, "Diversity" of the topical report also discusses that PSAI 7.9 should be performed at application development.

b. Please provide additional information on how the power supply is highly reliable. Is the information supporting highly reliable demonstrated in this topical report or elsewhere?

c. Please explain the basis for stating the design meets required reliability: "Redundancy of NIC [Nuclear Island Control System] components and network, combined with special treatments, ensures the required reliability."

 Section 4.1.1, "Code of Federal Regulations," states that "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."

The NRC staff has neither endorsed IEEE Std 603-2018 nor incorporated by reference into 10 CFR 50.55(a)(h). The TR does not fully discuss the justification for its use instead of IEEE Std 603-2018. TerraPower should discuss this approach further and explain why there is no need for an exemption request, or an alternative request under 10 CFR 50.55a(z).

 For section 4.1.2, "Regulatory Guidance," it appears that the overall architecture and design basis is informed by the risk-informed and performance-based process in NEI 18-04, as endorsed by RG 1.233. For example, the topical report discusses the plant-level DID and layers of defense using the NEI 18-04 methodology that are closely related to the development of the I&C architecture and design basis. Should RG 1.233 be included in this section for completeness?

- For section 4.1.2, "Regulatory Guidance," with 10 CFR 73.54 listed under section 4.1.1, should Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," Revision 1 (ML22258A204) be listed in this section? Consistent with the security-bydesign concept, the I&C architecture development should consider cyber security early and often.
- 9. For section 4.1.2, "Regulatory Guidance," it is not clear to the NRC staff what is the intended scope of the regulatory guidance documents listed in this section. Based on the title of the topical report, which includes the I&C architecture and design basis, it can be interpreted that comprehensive regulatory guidance needs to be included for the I&C design in the topical report. There are several regulatory guidance documents that are not included in the topical report that are expected to be part of the overall I&C design basis. Examples include those that are associated with environmental qualification of I&C equipment (e.g., RG 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Revision 2 (ML19175A044), the software life cycle development (e.g., RGs 1.169 1.173), and setpoints (i.e., RG 1.105, "Setpoints for Safety Related Instrumentation," Revision 4 (ML20330A329)). Additional information or clarification is needed on the scope of the regulatory guidance listed in this section.
- 10. Section 4.1.3, "Industry Codes and Standards," states that "Natrium I&C uses highly reliable NSRST (Non-Safety Related with Special Treatment) power source (Type B, C, F variables requiring reliable power supply are NSRST)" when discussing IEEE Std 497-2016, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," endorsed by RG 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," Revision 5 (ML18136A762). Type F has to do with indication of fuel damage and its effects.

Type F variables are those that provide primary information to accident management personnel to indicate fuel damage and the effects of fuel damage. How does TerraPower define fuel damage and what are the possible parameters projected to be qualified as Type F variables?

- 11. It is not clear to the NRC staff what the intended scope of the industry codes and standards listed in section 4.1.3, "Industry Codes and Standards." Depending on the scope, the list of industry codes and standards may need to be adjusted.
- 12. Section 4.1.3, "Industry Codes and Standards," does not include the industry documents that are discussed within the topical report. Examples include NEI 18-04, which is extensively used, and NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6 (ML101180437). Should these be listed in this section for clarity and completeness?
- 13. In section 4.1, "I&C Architecture Design Bases," the TR does not list SRM-SECY-22-0076 although it is mentioned under section 4.1.2 as part of the 10 CFR 50.55a, "Codes and Standards" related discussion. It should add clarity to list this Commission policy

separately (e.g., under new section 4.1.4) because it pertains to the I&C architecture design bases and is a unique category different from regulations and regulatory guidance such as RGs.

14. Section 4.2, "I&C Relationship to Plant-Level Lines of Defense," states that "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 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 plant initiating events (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."

It is not clear to the NRC staff what "include the design functions" intends to convey regarding DL2, DL3, and DL4. Typically, design functions are accomplished by design features and programmatic elements. The topical report states that the first and fifth DLs include programmatic elements and design features. Can TerraPower explain or elaborate "the design functions" included in DL2, DL3, and DL4?

15. The topical report states that "no single layer, function, or feature is specifically relied upon to mitigate the postulated initiating event (PIE)" and uses the following expressions are used: Abnormal Operating Occurrence (AOO) PIE, Design Basis Event (DBE) PIE, and Beyond Design Basis Event (BDBE) PIE. NEI 18-04 uses the expression initiating event (IE) not PIE. Is a PIE in this topical report the same as an IE in NEI 18-04?

In NEI 18-04, LBEs, consisting of AOOs, DBEs, BDBEs, and Design Basis Accidents, are defined in terms of event sequences comprised of an IE, the plant response to the IE (which includes a sequence of successes and failures of mitigating systems) and a well-defined end state. The topical report states that "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." Tables 5-2 to 5-4 of NEI 18-04 use the IE terminology. Does an AOO PIE, a DBE PIE, and a BDBE PIE represent an IE corresponding to the specific event sequences of an AOO, DBE, or DBDE?

16. Table 4-2, "Instrumentation and Control System Classification," has the following note regarding the Anticipatory Automatic Seismic Trip System (AST): "*The licensee or applicant referencing this topical report will provide the AST architecture including interface with RTBs."

Can TerraPower provide more detail on this statement?

17. Section 4.4, "Function Allocation to I&C Systems," states that "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 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."

The NRC staff's review of this topical report is based on the preliminary design and requirements phase of the Natrium project. What is the change control process in the last sentence referring to?

18. Section 7.4, "Diversity" states that "The RadICS PSAI 7.9 is addressed by the Natrium I&C design, allocation of functions, safety classification and diversity and defense indepth 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 [Non-Safety Related with No Treatment] and NSRTS functions at DL4 including diverse Primary Sodium Pump and Intermediate Sodium Pump shutdown and trip. In addition, the RPS design implements the RadICS fail safe modes as indicated in PSAI 7.9."

Are there additional details (e.g., supporting documents) available for regulatory audit regarding the PRA and the plant DID analysis to address the RadICS PSAI 7.9? For example, is there a document on the plant-level DID analysis? The additional details may be needed for the NRC staff to conclude that this topical report adequately addresses PSAI 7.9 of the RadICS topical report.

19. Section 7.4.1, "SECY-22-0076," states that "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 [Safety Related]."

The NRC staff understands the NEI 18-04's plant-level assessment of the defense-indepth adequacy encompasses the I&C systems. However, the last two sentences are focused on the RPS only. Does Natrium's defense-in-depth and diversity assessment include other digital I&C systems listed in Table 4-2, "Instrumentation and Control System Classification," based on their risk significance?

20. Section 7.4.1, "SECY-22-0076," states that, for Point 2 of the SRM, "Natrium I&C implementation: The DID assessment is consistent with RG 1.233. The assessment includes both risk-informed and best-estimate analysis. The DID assessment is consistent with RG 1.233. The assessment includes both risk-informed and best-estimate analysis."

Based on the last sentence, does TerraPower perform its DID assessment using both deterministic and risk-informed options? For the former, each event evaluated in the accident analysis section of the safety analysis report is postulated to have occurred along with a concurrent digital I&C CCF, which is thus deterministic. For the latter, a risk-

informed approach such as NEI 18-04 is used considering the risks associated with selected LBEs that are 'event sequence families.'

21. Section 7.4.1, "SECY-22-0076," states that, for Point 3 of the SRM, "Natrium I&C implementation: The DID assessment establishes the defense lines and shows that design features are adequate to address CCF. The PRA DID analysis shows the RPS, with inherent internal diversity, sufficiently decreases the CCF risk beyond the high consequence BDBE region, such that the RPS CCF event can be further mitigated through DL4 functions."

The expression "...sufficiently decreases the CCF risk beyond the high consequence BDBE region" is not clear. Explain this expression further. Regarding "..., such that the RPS CCF event can be further mitigated through DL4 functions," is the RPS CCF event the only event of concern?

22. SRM-SECY-22-0076 Point 4 states that:

"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."

What are the risk-informed critical safety functions for the TerraPower design?

23. Section 7.4.1, "SECY-22-0076," states that, for Point 4 of the SRM, "Natrium I&C implementation: The DL4 functions provide defense in-depth and diversity to address the low risk/consequence BDBEs, including RPS CCF."

How is addressing the low risk/consequence BDBEs consistent with Point 4 of the SRM or the RG 1.233 process? If a BDBE is low risk or low consequence, does it need to be addressed from the DID adequacy perspective?

Team Assignments

Reed Anzalone	Senior Nuclear Engineer	
Joe Ashcraft	Electronics Engineer, Audit Lead	
Roel Brusselmans	Project Manager, Audit Manager	
Calvin Cheung	Electronics Engineer	
Ralph Costello	Senior Security Specialist (Cyber)	
Stephanie Devlin-Gill	Senior Project Manager	
lan Jung	Senior Reliability and Risk Analyst	
Dinesh Taneja	Senior Electronics Engineer	

Logistics

Entrance Meeting	July 8, 2024
Exit Meeting	August 12, 2024

Audit meetings will take place in a virtual format, using Microsoft Teams or another similar platform. Audit meetings will be scheduled on an as-needed basis after the entrance meeting and once the NRC staff has had the opportunity to review any documents placed in the online

reference portal. The audit will begin on July 8, 2024, and continue as necessary, with activities occurring intermittently during the audit period. The audit period may be reduced or extended, depending on the progress made by the NRC staff and TerraPower in addressing audit questions.

Special Requests

The NRC staff requests that TerraPower ensure that their technical staff are available to answer questions during the audit. The NRC staff also requests that TerraPower provide access to supporting documents via the TerraPower online reference portal.

Deliverables

At the completion of the audit, the audit team will issue an audit summary within 90 days after the exit meeting but will strive for a shorter duration. The audit summary will be declared and entered as an official agency record in ADAMS and be made available for public viewing through the publicly available records component of ADAMS. If you have questions about this audit, please contact me at 301-415-0829 or via email at Roel.Brusselmans@nrc.gov.

Sincerely,

/**RA**/

Roel Brusselmans, Project Manager Advanced Reactors Licensing Branch 1 Division of Advanced Reactors and Non-Power Production and Utilization Facilities Office of Nuclear Reactor Regulation

Docket No.: 99902100

cc: TerraPower Natrium via GovDelivery

SUBJECT: TERRAPOWER, LLC – AUDIT PLAN FOR TOPICAL REPORT "INSTRUMENTATION AND CONTROL ARCHITECTURE AND DESIGN BASIS TOPICAL REPORT," REVISION 1 (CAC / EPID NO.00431 / L-2024-TOP-0006) DATED: JUNE 24, 2024

DISTRIBUTION:

PUBLIC **RidsNrrDanu Resource** RidsNrrDanuUal1 Resource RidsACRSMailCTR Resource RidsOgcMailCenter Resource FSacko, NRR IJung, NRR RCostello, NSIR JAshcraft, NRR DTaneja, NRR CCheung, NRR RBrusselmans, NRR SDevlin-Gill, NRR MSutton, NRR JBorromeo, NRR DGreene, NRR RAnzalone, NRR CdeMessieres, NRR

ADAMS Accession No: ML24163A003

NRR-106

OFFICE	NRR/DANU/UAL1:PM	NRR/DEX/EICB:BC	NRR/DANU/UAL1:BC
NAME	RBrusselmans	FSacko	JBorromeo
DATE	6/14/2024	6/17/2024	6/24/2024
OFFICE	NRR/DANU/UAL1:PM		
NAME	RBrusselmans		
DATE	6/24/2024		

OFFICIAL RECORD COPY