August 31, 2017

MEMORANDUM TO: Samuel S. Lee, Chief
Licensing Branch 1
Division of New Reactor Licensing
Office of New Reactors

FROM: Omid Tabatabai, Senior Project Manager /RA/
Licensing Branch 1
Division of New Reactor Licensing
Office of New Reactors

SUBJECT: U.S. NUCLEAR REGULATORY COMMISSION STAFF AUDIT REPORT FOR THE REVIEW OF NUSCALE POWER, LLC, DOCUMENTS RELATED TO NUSCALE DESIGN CERTIFICATION APPLICATION, TIER 2, CHAPTER 7, "INSTRUMENTATION AND CONTROLS" (DOCKET NO. 52-048)

From May 8, 2017 to June 30, 2017, the U.S. Nuclear Regulatory Commission (NRC) staff conducted a regulatory audit of certain design documents to facilitate the review of the Instrumentation and Control (I&C) portions of the NuScale Power, LLC (NuScale) design certification application (DCA), Tier 2, Chapter 7, "Instrumentation and Controls." Specifically, the staff audited pertinent documents related to the DCA, Tier 2, I&C related information:

- Section 7.1.3, "Redundancy,"
- Section 7.1.5, "Diversity and Defense in Depth,"
- Section 7.1.8, "Hazard Analysis,"
- Section 7.2.3, "Reliability, Integrity, and Completion of Protective Action," and
- Section 7.2.8, "Auxiliary Features."

The NRC staff conducted its audit on NuScale's electronic reading room (eRR). The purpose of this audit was: (1) to review and verify the supporting information presented to the staff for review in the DCA; and (2) to assess the need for NuScale to formally submit relevant non-docketed design information that the staff may need to rely on to make for its regulatory and safety determination. The NRC staff conducted the audit in accordance with the Office of New Reactors (NRO) Office Instruction NRO-REG-108, "Regulatory Audits."

CONTACT: Omid Tabatabai, NRO/DNRL
301-415-6616

The public and non-public versions of the audit report are available in Agencywide Document Access and Management System (ADAMS) with Accession Nos. ML17228A807, and ML17228A788, respectively.

Docket No.: 52-048

Enclosure 1: Summary of Staff's Audit of Information in NuScale Design Certification Application, Tier 2, Chapter 7, "Instrumentation and Controls"

Enclosure 2: List of Staff's Editorial Comments

cc: NuScale DC ListServ

SUBJECT: U.S. NUCLEAR REGULATORY COMMISSION STAFF AUDIT REPORT FOR THE REVIEW OF NUSCALE POWER, LLC, DOCUMENTS RELATED TO NUSCALE DESIGN CERTIFICATION APPLICATION, TIER 2, CHAPTER 7, "INSTRUMENTATION AND CONTROLS" (DOCKET NO. 52-048) DATED AUGUST 31, 2017

DISTRIBUTION:
PUBLIC
LB1 R/F
SLee, NRO
IJung, NRO
SGreen, NRO
OTabatabai, NRO
LBetancourt, NRO
FAkstulewicz, NRO
NuScale DC Listserv
RidsOgcMailCenter
RidsNroDnrlLB1
RidsOpaMailCenter
RidsAcrsAcnwMailCenter

ADAMS Accession No.: ML17228A807 *via email* NRO-002

OFFICE	NRO/DNRL/LB1: PM	NRO/DNRL/LB1: LA*	NRO/DEIA/ICEB: BC
NAME	OTabatabai	SGreen*	IJung*
DATE	08/11/2017	08/21/2017	08/15/2017

OFFICIAL RECORD COPY

SUMMARY OF STAFF'S AUDIT OF INFORMATION
IN NUSCALE DESIGN CERTIFICATION APPLICATION,
TIER 2, CHAPTER 7, "INSTRUMENTATION AND CONTROLS"

NRC Audit Team:

- Luis D. Betancourt, Electronics Engineer, Audit Lead
- Dinesh Taneja, Senior Electronics Engineer
- Joseph M. Ashcraft, Electronics Engineer
- Sergiu S. Basturescu, Electronics Engineer
- Dawnmathews Kalathiveettil, Electronics Engineer
- Derek S. Halverson, Digital Instrumentation and Controls Engineer
- David Curtis, Acting Chief
- Jeffrey S. Schmidt, Senior Reactor Operations Engineer
- Timothy T. Drzewiecki, Reactor Operations Engineer
- James M. Gilmer, Reactor Operations Engineer
- Rebecca L. Karas, Chief
- Omid Tabatabai, Senior Project Manager

I. Purpose

From May 8, 2017 to June 30, 2017, the U.S. Nuclear Regulatory Commission (NRC) staff conducted a regulatory audit of detailed design documents to facilitate review of the Instrumentation and Control (I&C) portions of the NuScale Power, LLC (NuScale) design control document (DCD) Tier 2, Revision 0 (Reference (Ref.) 1). The audit included the following NuScale documents:

- Section 7.1.3, "Redundancy,"
- Section 7.1.5, "Diversity and Defense in Depth,"
- Section 7.1.8, "Hazard Analysis,"
- Section 7.2.3, "Reliability, Integrity, and Completion of Protective Action," and
- Section 7.2.8, "Auxiliary Features."

The NRC staff audited the design documents in the applicant's electronic reading room (see Section IV of this report). The purpose of this audit was: (1) to verify some the claims made in the DCD regarding protection against single failure, diversity and defense-in-depth (D3), redundancy, and development life cycles of the I&C systems; and (2) to ensure the need for docketing some of the non-docketed design information for making a reasonable assurance of safety finding.

The NRC staff conducted the audit in accordance with Office Instruction NRO-REG-108, "Regulatory Audits" (Ref. 2).

Enclosure

II. Background and Audit Basis

On March 23, 2017, the NRC staff accepted the design certification application (DCA) for docketing for the NuScale small modular reactor (Ref. 3). The NRC staff initiated Phase 1 of the DCA review on March 20, 2017. Since docketing the NuScale DCD for a detailed review, the NRC staff has held several meetings with NuScale to discuss regulatory and technical matters related to the DCD Tier 2, Chapter 7, "Instrumentation and Controls." Upon the initial review of the DCD, the NRC staff found a need for auditing some of the detailed design documents supporting the design information presented in the NuScale DCD.

III. Audit Objectives

The objective of this audit was: (1) to verify some the claims made in the DCD regarding protection against single failure, diversity, defense in depth, redundancy, and development life cycles of the I&C systems; and (2) to ensure the need for docketing some of the non-docketed design information for making a reasonable assurance of safety finding.

IV. Scope of the Audit

The NRC staff performed the audit of documents and methodologies related to:

- Failure Modes and Effects Analysis (FMEA) of the Module Protection System (MPS) and the Neutron Monitoring System (NMS),
- Hazard Analysis (HA) of the MPS and NMS,
- D3 Coping Analysis for Postulated Digital-Based Common Cause Failure (CCF) Vulnerability, and
- Segmentation Analyses for the Module Control System (MCS) and Plant Control System (PCS).
- Specifically, the NRC staff reviewed the following documents:
- ED-E011-3952, Revision 2, "MPS Process Block Diagrams."
- ER-0000-4937, Revision 0, "MPS Digital-Based Common Cause Failure Coping Analysis."
- ER-E011-2477, Revision 1, "Module Protection System Hazard Analysis."
- ER-E000-4335, Revision 0, "Analysis of Common-Cause Failure in Process Control Systems."
- ER-E011-2227, Revision 1, "Failure Modes and Effects Analysis (FMEA) for the Module Protection System (MPS)."
- ER-E013-3847, Revision 0, "Neutron Monitoring System Hazard Analysis."

- ER-E013-3892, Revision 0, “Neutron Monitoring System Failure Modes and Effects Analysis.”

V. Audit Activities and Summary of Findings

The regulatory audit began with an entrance meeting at 8:30 a.m. on Monday, May 8, 2017. At the entrance meeting, the NRC staff discussed the schedule of activities for the audit and the agenda. The NRC staff audit focused on the following four areas: (1) FMEAs of the MPS and NMS, (2) HAs of the MPS and NMS, (3) D3 coping analysis postulated digital-based CCF Vulnerability, and (4) segmentation analyses for the MCS and PCS.

Throughout the audit, the NRC staff held question-and-answer sessions with NuScale to address NRC staff’s questions while reviewing documents. The NRC staff provided interim status briefings for each week’s activities and observations. The exit meeting was held at 11:00 a.m. on Wednesday, July 5, 2017. At the exit meeting, the NRC staff further communicated the results of their document reviews, discussed revisions to the design documents, and the issuance of request for additional information (RAI) 9032, Question 30467.

Below is a summary of the audit activities, observations, and follow-up actions:

1.0 FMEA OF THE MPS AND NMS

Module Protection System

The FMEA for the MPS is a methodology for evaluating the MPS to determine where and how its structures, systems and components could fail and assess the impact of the consequences of failures on the safe operation of the plant. [

]

The NRC staff’s audit verified that no failure modes of the MPS were identified that were undetectable or would prevent the MPS from performing its reactor trip system (RTS), engineering safety features actuation system (ESFAS), and accident monitoring functions. The MPS is designed such that a single failure in one separation group or division will not interfere with the proper operation of the redundant separation groups or division. In addition, the MPS is designed to eliminate all non-detectable failures. Further, any potential non-detectable failures identified by the FMEA were addressed by a combination of alarms, self-test features, and periodic surveillance testing.

The applicant agreed to modify the FMEA for the MPS to correct several editorial errors identified during the audit (see Enclosure 2 of this report).

Module Protection System

The FMEA analyzes the NMS-excore and NMS-refueling subsystems. The FMEA assessed a single NMS-excore channel, and a single NMS-refuel channel. It was not in the scope of this FMEA to evaluate external influences upon the control system which may contribute to its failure.

The NRC staff's audit verified that no single failure exists that would prevent the NMS from performing its primary function. A failure of one channel (separation group) of the NMS still allows the MPS to perform its safety function due to the two-out-of-four coincidence voting logic used by the MPS.

The applicant agreed to modify the FMEA for the NMS to correct several editorial errors identified during the audit (see Enclosure 2 of this report).

2.0 HA OF THE MPS AND NMS

Module Protection System

DSRS Chapter 7.0, Appendix A, "Instrumentation and Controls – Hazard Analysis," describes the system HA as a process for examining an I&C system to identify unintended or unwanted I&C system operation, including the impairment or loss of the ability to perform a safety function.

The purpose of HA was to present the results of the system HA for the MPS in conjunction with plant safety analyses, FMEAs, D3 analyses, and multi-discipline design reviews as an additional means of ensuring the correctness and completeness of the requirements for the MPS. The MPS system HA was not intended to evaluate the hazard conditions and mitigating factors for the entire NuScale Power Plant. It was intended to evaluate those conditions and factors associated with the MPS and the systems that directly interact with the MPS that can result in unintended or unwanted system operation including a failure to initiate a protective action.

The HA was based on a review of the expected processes that will be performed by the MPS. Several assumptions were made about those processes that may change as the design is evolved which will have an effect on the accuracy of this analysis. Other assumptions have been left open such as timing requirements in the system response. These details are worked out during the detailed design, which will also have an effect on the analysis.

Additional considerations that have been included in the HA include ignoring the effects of redundancy and defense-in-depth. Many of the hazards conditions identified in the HA were partially or fully mitigated by these characteristics. However, identifying the conditions as if each division of control is a stand-alone system allows a validation of the efficacy of that mitigation.

[

]

The NRC staff observed that the HA of the MPS demonstrates that controls have been placed to mitigate or eliminate hazards that would prevent the MPS from performing its primary function. The NRC staff notes that the HA is a living document. The HA of the MPS will change and evolve as the system detail design progresses. The applicant agreed to modify the HA for the MPS to correct several editorial errors identified during the audit (see Enclosure 2 of this report).

Neutron Monitoring System

DSRS Chapter 7.0, Appendix A describes the system HA as a process for examining an I&C system to identify unintended or unwanted I&C system operation, including the impairment or loss of the ability to perform a safety function.

The purpose of HA was to present the results of the system HA for the NMS in conjunction with plant safety analyses, FMEAs, D3 analyses, and multi-discipline design reviews as an additional means of ensuring the correctness and completeness of the requirements for the NMS.

The NMS system HA was not intended to evaluate the hazard conditions and mitigating factors for the entire NuScale Power Plant. It was intended to evaluate those conditions and factors associated with the NMS and the systems that directly interact with the NMS that can result in unintended or unwanted system operation including a failure to initiate a protective action.

The HA in this report is based on a review of the expected processes that will be performed by the NMS. Several assumptions were made about those processes that may change as the design is evolved which will have an effect on the accuracy of this analysis. Other assumptions have been left open such as timing requirements in the system response. As these details are worked out in the design this will also have an effect on the analysis.

Additional considerations that have been included in the analysis include ignoring the effects of redundancy and defense-in-depth. Many of the hazards conditions identified in this analysis were partially or fully mitigated by these characteristics. However, identifying the conditions as if each division of control is a stand-alone system allows a validation of the efficacy of that mitigation.

The NRC staff observed that the NMS HA demonstrates that controls have been placed to mitigate or eliminate hazards that would prevent the NMS from performing its primary function. The NRC staff notes that the HA is a living document. The HA of the NMS will change and evolve as the detailed system design progresses.

3.0 D3 COPING ANALYSIS FOR POSTULATED DIGITAL-BASED CCF VULNERABILITY

DCD Section 7.1.5 describes the vulnerabilities of the reactor coolant system (RCS) flow sensors and pressure sensors to software CCFs which could result in the disabling of the RTS and ESFAS. ER-0000-4937, Revision 0 provided the basis for the alternative protective actuation signals to demonstrate diversity and evaluated the consequences of the postulated failures to demonstrate defense-in-depth.

During the audit, NRC staff found that more clarification was needed for understanding the low RCS flow event. The applicant stated that RCS flow rate is a function of reactor power in the NuScale design, such that low RCS flow is only possible during startup conditions. The low-low RCS flow protective function is credited for actuating RTS and the chemical volume and control system isolation in the event of a module heatup system (MHS) malfunction that causes an RCS flow reversal. The applicant stated that this event is not considered credible in combination with a digital-based CCF of the RCS flow sensor due to the very short, and limited operating window where the MHS failure could occur. This resulted in RAI 9032, Question 30467 (Ref. 4), where the NRC staff requested the applicant to provide the technical basis which led them to conclude that an MHS malfunction event in combination with a digital-based CCF of the RCS flow is not credible.

The applicant agreed to modify the D3 coping analysis to correct several editorial errors identified during the audit (see Enclosure 2 of this report).

4.0 SEGMENTATION ANALYSES FOR THE MCS AND PCS

DCD Section 7.0.4.5.1 describes the MCS segmentation and DCD Section 7.0.4.6.1 describes the PCS segmentation. ER-E000-4335, Revision 0 provided the basis for understanding the segmentation of these plant systems. The NRC staff assessed the MCS and PCS segmentation analyses described in ER-E000-4335, Revision 0 and had no observations.

5.0 CONCLUSION

Based on the audit observations, the NRC staff issued RAI 9032, Question 30467 regarding the D3 coping analysis. In addition, the applicant committed to address the observations that resulted in revisions to their design documents. The NRC staff will review the RAI response during the Phase 2 review. This audit report will be referenced in Sections 7.1.3, 7.1.5, 7.1.8, 7.2.3, and 7.2.8 of the staff's final safety evaluation report for the NuScale DCA review.

6.0 REFERENCES

1. NuScale, DCD Tier 2, Chapter 7, “Instrumentation and Controls,” Revision 0 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML17013A278)

2. NRO Office Instruction, NRO-REG-108, “Regulatory Audits,” Revision 0, April 2009 (ADAMS Accession No. ML081910260).

3. NRC letter to NuScale, “NuScale Power, LLC. – Acceptance of an Application for Standard Design Certification of a Small Modular Reactor,” March 23, 2017 (ADAMS Accession No. ML17074A087).

4. NRC letter to NuScale, “Request for Additional Information Letter No. No. 171),” August 12, 2017 (ADAMS Accession No. ML17224A021).

5. NRC, “Design Specific Review Standard for NuScale Small Modular Reactor Design, Chapter 7 – Instrumentation and Controls,” U.S. Nuclear Regulatory Commission, Washington, DC, August 5, 2016 (ADAMS Accession No. ML15355A295).

STAFF'S EDITORIAL COMMENTS

ER-E011-2227, Revision 1, "Failure Modes and Effects Analysis (FMEA) for the Module Protection System (MPS)."

Editorial Comments				
No.	**Date**	**Page**	**Staff's Comment**	**Status**
E-1	6/27/17	13	Section 2.1.5, "Scheduling and Voting Module" Fourth sentence: Replace "perform" with "performs." "…for each safety function and perform a 2oo4…"	**Status:** **Resolved / Confirmatory Item** The applicant agreed with this proposed change.
E-2	6/27/17	13	Section 2.1.6, "Equipment Interface Module" Second sentence. Replace "perform" with "performs." "…from the three SVM and perform a 2oo3…"	**Status:** **Resolved / Confirmatory Item** The applicant agreed with this proposed change.
E-3	6/27/17	13	Section 2.1.6, "Equipment Interface Module" 7th Sentence: Replace "heatet" with "heated." "…, except the pressurizer heatet trip breakers,…"	**Status:** **Resolved / Confirmatory Item** The applicant agreed with this proposed change.
E-4	6/27/17	14	Section 2.1.10, "Reactor Trip Breaker" Fourth sentence: Replace "drivce" with"drive." "…removing power from the control drivce mechanisms."	**Status:** **Resolved / Confirmatory Item** The applicant agreed with this proposed change.
E-5	6/27/17	15	Section 2.2.2, "Gateways" Second paragrapgh, second sentence: Replace "." with "," "Communication modules. HWM, and the SFM are …"	**Status:** **Resolved / Confirmatory Item** The applicant agreed with this proposed change.
E-6	6/27/17	24	Section 3.3.5, Electromagnetic and Radio Frequency Interference "…failures to electromagnetic compatibility…" should contain the word "due."	**Status:** **Resolved / Confirmatory Item** The applicant agreed with this proposed change.

Enclosure 2

ER-E013-3892, Revision 0, "Neutron Monitoring System Failure Modes and Effects Analysis"

Editorial Comments				
No.	**Date**	**Page**	**Staff's Comment**	
E-7	6/27/17	17	Section 3.2, "Single Failure Criterion" Second bullet: Add "d" to "cause." "All failures cause by the single failure"	**Status: Resolved / Confirmatory Item** The applicant agreed with this proposed change.
E-8	6/27/17	--	Section 5.0, "Results and Recommendations" Replace "MPS" with "MCS" "Comparisons between Power Range Linear and Intermediate Range Linear flux shall be made within the MPS to assist with failure identification…"	**Status: Resolved / Confirmatory Item** The applicant agreed with this proposed change.

ER-0000-4937, Revision 0, "MPS Digital-Based Common Cause Failure Coping Analysis"

Editorial Comments				
No.	**Date**	**Page**	**Staff's Comment**	
E-9	6/27/17	21	Section 2.3.1.3, "Increase in RCS Inventory" First sentence should have an "a" between "is" and "slow."	**Status: Resolved / Confirmatory Item** The applicant agreed with this proposed change.
E-10	6/27/17	27	Section 2.3.2.3, "Low and Low-low RCS Flow" Last sentence should be "postulated as concurrent."	**Status: Resolved / Confirmatory Item** The applicant agreed with this proposed change.
E-11	6/27/17	28	Section 2.3.3.3, "Low-low RCS Flow" First sentence should be "actuations are not" instead of "actuations is not."	**Status: Resolved / Confirmatory Item** The applicant agreed with this proposed change.