UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

September 26, 2018

Ms. Margaret M. Doane
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: INTERIM LETTER: CHAPTERS 7 AND 8 OF THE NRC STAFF'S SAFETY EVALUATION REPORT WITH OPEN ITEMS RELATED TO THE CERTIFICATION OF THE NUSCALE SMALL MODULAR REACTOR

Dear Ms. Doane:

During the 656th meeting of the Advisory Committee on Reactor Safeguards, September 6-7, 2018, we met with representatives of NuScale Power, LLC (NuScale) and the NRC staff to review Chapter 7, "Instrumentation and Controls," and Chapter 8, "Electric Power," of the safety evaluation report (SER) with open items associated with the NuScale design certification application (DCA). Our NuScale Subcommittee also reviewed these chapters on June 6 and August 23, 2018. During these meetings, we had the benefit of discussions with NuScale and the staff. We also had the benefit of the referenced documents.

CONCLUSIONS and RECOMMENDATION

1. We have identified no major issues at this time. However, there are items, such as those noted below, that need to be resolved because they may alter this conclusion.

2. The staff should ensure that the unidirectional communication interfaces labeled on Figure 7.0-1 in Chapter 7 of NuScale's design certification application as "PCS Unidirectional Data Diode" and "MCS Unidirectional Data Diode" are one-way, hardware-based devices that neither use nor are configured by software to demonstrate complete isolation from external communications.

3. The staff's safety evaluation report for Chapter 8 has not yet resolved the significant open item of whether the design certification application meets the specifications of topical report TR-0815-16497-P-A and its associated safety evaluation limitations and conditions.

BACKGROUND

NuScale submitted a DCA for its small modular reactor on December 31, 2016. The staff's Phase 2 SER chapters related to the DCA include open items. In addition to a description of the staff review and their bases for acceptance of the DCA, the SER chapters also identify the information a combined license applicant must provide.

Our review is being conducted on a chapter-by-chapter basis to identify technical issues that may merit further consideration by the staff. This process will aid in the resolution of concerns and facilitates timely completion of the design certification review. Accordingly, the staff has provided Chapters 7 and 8 of the SER with open items for our review. The staff's SER and our review of these chapters addressed DCA Chapter 7, Revision 1 and Chapter 8, Revision 0 and supplemental material, including NuScale responses to staff requests for additional information.

DISCUSSION
For this interim letter, we note the following observations on selected elements of the design addressed in these chapters.

DCA Chapter 7 - Instrumentation and Control

A NuScale Power Plant can consist of up to 12 NuScale Power Modules (NPMs). Each NPM has a safety-related module protection system (MPS) for reactor trip and engineered safety features actuation and a non-safety-related module control system (MCS) control network for balance of plant control functions. The MPS also provides read-only monitoring data to the main control room and MCS control network. The overall NuScale Power Plant has a shared non-safety-related plant protection system (PPS) and shared non-safety-related plant control system (PCS) control network, each of which serve the non-NPM-specific plant systems that support all NPMs in the NuScale Power Plant.

Chapter 7 of the DCA describes the overall NuScale Power Plant instrumentation and control (I&C) systems architecture that integrates the safety-related MPS and the non-safety-related MCS, PPS, and PCS, and other associated non-safety systems. It also identifies the control of access features (both internal plant access and the prohibition of remote access from external sources) for the overall NuScale Power Plant I&C systems architecture.

The overall I&C systems of the NuScale design are implemented using three major platforms: 1) a safety-related field programmable gate array-based platform for the safety-related MPS, 2) a non-safety-related field programmable gate array-based platform for the PPS, and 3) a non-safety-related distributed control system microprocessor-based platform for the data processing system and two non-safety-related control systems: MCS control network and PCS control network.

For the MPS, the approved NuScale topical report, TR-1015-18653-P-A, “Design of the Highly Integrated Protection System [HIPS] Platform,” Revision 2, provides a detailed description of how the digital instrumentation and control (DI&C) system architecture for the MPS meets the fundamental design principles of independence, redundancy, predictability and repeatability, and diversity and defense-in-depth. The topical report describes key design concepts for a generic DI&C platform. It describes the design attributes and physical configuration of the HIPS platform standardized circuit boards and their chassis. When properly configured, HIPS is designed to provide the reactor trip system and engineered safeguards actuation system for a nuclear power plant.

The scope of this topical report is limited to the HIPS platform. However, it does not illustrate its interface with any other safety or non-safety systems, external power supplies, other details of plant monitoring, or communications external to the overall plant I&C system. Design features that control access from internal networks or external sources are not described in this topical report.

In its safety evaluation for the HIPS topical report, the staff identified 65 application specific action items (ASAIs) that must be implemented for NRC approval of the HIPS platform for safety-related applications in any nuclear power plant. The determination of full compliance with the regulations remains subject to a plant-specific licensing review of a full system design based on the HIPS platform. The staff also concluded that the HIPS platform meets the applicable regulatory requirements for safety-related I&C systems, provided each plant-specific and application-specific use meets the limitations and conditions delineated in the 65 ASAIs. We documented our review and agreement with the staff's safety evaluation on TR-1015-18653-P in our letter dated, April 24, 2017.

In Chapter 7 of the DCA, the applicant states that the design concept for each NPM MPS incorporates by reference the HIPS topical report without deviation. It also identifies the disposition of each of these ASAIs. The staff review determined that the HIPS platform modules and their design features are configured to meet the fundamental DI&C principles of independence, redundancy, predictability and repeatability, and diversity and defense-in-depth. The staff also concluded that the HIPS platform for the MPS meets the applicable regulatory requirements for safety-related I&C systems and that the application satisfies the application-specific information requirements specified in the HIPS topical report safety evaluation. Therefore, the NRC staff considers all ASAIs closed and the application of the HIPS for the MPS is satisfactory.

The non-safety-related PPS is implemented using HIPS platform modules to monitor parameters at the plant level and to execute actuations in response to normal and off-normal conditions. The PPS monitors and controls systems common to all NPMs in the NuScale Power Plant and provides read-only monitoring data to the main control room and PCS control network.

The MCS and PCS control networks are non-safety-related control systems and are implemented with a distributed control system microprocessor-based platform. Each distributed control system utilizes a redundant and fault-tolerant architecture. The MCS control network provides monitoring and component-level control for NPM balance-of-plant control functions and the PCS control networks provides monitoring and component-level control for non-NPM-specific plant components. These networks provide monitoring data to the plant network through unidirectional data diodes. The plant network communicates all data and other information through a bidirectional, software-implemented and configured firewall, which could be accessed by unintended entities external to the NuScale Power Plant.

Segmentation is used to separate control functions in the MCS and PCS control network architectures into groups based on a susceptibility analysis. It is used as a defensive and preventative measure to provide functional independence between major control functions to prevent a failure in one controller group from causing an undesirable condition in another controller group. Segmentation also ensures that a failure of these systems does not adversely affect the MPS functions and prevents any multiple failures resulting in spurious actuations or events that could create an unanalyzed condition. The staff reviewed the technical basis of the segmentation analysis and confirmed the applicant's assertions that a failure in any of the control segments does not have an adverse impact on safety-related systems.

Control of Access

The HIPS topical report safety evaluation did not include an evaluation of control of access for an overall plant I&C system. The HIPS topical report safety evaluation included ASAIs to

specify the information needed to complete an assessment of the physical and administrative controls for access to the MPS. The DCA Chapter 7 SER states the following: "Remote access to the MPS is prohibited. However, the MPS permits administrative control of direct access to safety system equipment," and "The I&C architecture is designed with four security levels of which Security Level 4 is the highest. The MPS is identified as a Security Level 4 digital system. The design of the MPS prohibits remote access to systems within the Security Level 4 domain."

The staff evaluated the resolution of the control of access ASAIs and the physical and administrative controls for access to the MPS provided in DCA Chapter 7. The staff finds that the MPS internal and external control of access features are acceptable based on their ability to prevent inadvertent or unauthorized electronic or physical access to the safety system. We agree with this conclusion relative to internal and remote access to the MPS.

The HIPS topical report clearly and explicitly delineates the form of one-way communications both internal to the MPS and for MPS communications external to the MPS to the non-safety related MCS control network as follows:

> each CM [communication module] . . . can provide one-way isolated communications to another CM or system, or receive one-way data from another CM or system. Each communication channel can be configured as transmit or receive only. When the communication channel is configured for transmit only, the receive capability is physically disabled by hardware. When the communication channel is configured for receive only, the transmit capability is physically disabled by hardware.

DCA Chapter 7 describes detailed MPS internal communication and external communication from the MPS. It also describes control of physical and administrative access to the MPS. However, the staff's DCA Chapter 7 SER did not describe how the PPS communicates in detail with the PCS control network, main control room, and the Technical Support Center. We assume that the evaluation relative to access for the MPS applies equally to the PPS, since 1) the PPS is specified to be designed using HIPS modules including the communication module, 2) the use of the communication modules and other HIPS modules are shown on Figure 7.0-1, "Overall Instrumentation and Controls System Architecture Diagram," in Chapter 7, Revision 1, of NuScale's DCA, and 3) Note 1 in that Figure states that PPS provides "separated, optically isolated, unidirectional data to MCS and PCS (read-only data)," On that basis we extend our agreement on access to the PPS as well.

Figure 7.0-1 of the DCA also shows communication from the MCS control network and PCS control network through unidirectional data diodes (labeled as PCS Unidirectional Diode and MCS Unidirectional diode) to the Plant Network. The Plant Network then communicates data and other information through a bidirectional, software-implemented and configured firewall to entities external to the NuScale Power Plant. A description of this device is in DCA Section 7.2.13.7, which calls it a unidirectional communication interface. During the August 23, 2018 Subcommittee meeting, the applicant stated that this device will be specified in their application as to whether it is digital-, hardware-, or software-based. The applicant further stated that they will monitor the attributes of how that device functions. Thus, the device could end up being software controlled and configured instead of a one-way, hardware-based device, which neither uses nor is configured by software. Both of the control networks communicate through unidirectional data diodes to the Plant Network, which then communicates all data and other information through a bidirectional software implemented and configured firewall to all entities external to the NuScale Power Plant. Implementing these unidirectional data diodes as

software-based, rather than hardware-based (that neither use nor are configured by software), will present a significant vulnerability to having both NPM and non-NPM control systems compromised.

Regarding Chapter 7, the staff should ensure that the unidirectional communication interface (Figure 7.0-1 Unidirectional Data Diodes: PCS and MCS) are one-way, hardware-based devices that neither use nor are configured by software to be consistent with the clearly specified performance-based design required for the internal MPS and PPS communications and external communications to the MCS and PCS control networks.

DCA Chapter 8 Electric Power

Our letter of July 26, 2017, found that NuScale topical report TR-0815-16497-P is acceptable for use as a reference document for the NuScale plant electrical systems design subject to the staff's limitations and conditions. If the design in the NuScale DCA can meet the conditions of applicability in topical report Table 3-1; the augmented design, qualification, and quality assurance provisions in Table 3-2; and the staff limitations and conditions, the design would not require Class 1E AC electric power. We asked that the staff add an additional condition that the design, qualification, and quality assurance provisions described in Table 3-2 should be applied to any non-safety AC or DC power supplies that support 1) operation of risk-significant systems or components or 2) performance of risk-significant human actions that are identified in the site-specific probabilistic risk assessment. The staff disagreed, but we maintain that our request remains valid.

Electric power systems in a nuclear power plant do not establish classification requirements on other systems. Rather, the electrical loads determine the classification requirements for the electrical power system. The NuScale plant is designed such that it does not require onsite or offsite AC electrical power to cope with design basis events. Safety systems are not reliant on AC or DC power for actuation. At a more detailed level, electric power is not relied upon to meet specified acceptable fuel design limits and to protect the reactor coolant pressure boundary as a result of anticipated operational occurrences or postulated accidents. Because NuScale does not require a Class 1E onsite AC power system, they requested exemption from GDC 17, "Electric Power Systems."

We and the staff addressed this design in our reviews of topical report TR-0815-16497-P. The NuScale DCA Chapter 8 describes the NuScale electric power system, references the topical report for the acceptability of such a design, and states that their design meets the specifications of the topical report and its associated safety evaluation. Thus, the staff must ensure that the actual NuScale design meets the specifications of the topical report and the associated safety evaluation limitations and conditions. The staff has begun that process and has asked a number of questions that they expect will allow them to determine this one and important issue: does the NuScale design meet the topical report specifications and the related safety evaluation limitations and conditions?

We have identified no other issues at this time. However, because of this significant open item, there are a number of system interactions with the electric power systems that may alter this conclusion.

Chapters 7 and 8 Summary

The staff should ensure that the unidirectional communication interfaces labeled on Figure 7.0-1 as “PCS Unidirectional Data Diode” and “MCS Unidirectional Diode” are one-way, hardware-based devices that neither use nor are configured by software to demonstrate complete isolation from external communications.

The staff’s SER for Chapter 8 has not yet resolved the significant open item of whether the DCA meets the specifications of topical report TR-0815-16497-P-A and its associated safety evaluation limitations and conditions.

Sincerely,

/RA/

Michael Corradini
Chairman

REFERENCES

1. U.S. Nuclear Regulatory Commission, “NuScale Power, LLC, Design Certification Application - Safety Evaluation With Open Items for Chapter 7, ‘Instrumentation and Controls’,” July 18, 2018 (ML18038A790).
2. NuScale Power, LLC, Design Certification Application, Chapter 7, “Instrumentation and Controls,” Revision 1, March 2018 (ML18086A177).
3. U. S. Nuclear Regulatory Commission, “NuScale Power, LLC, Design Certification Application - Safety Evaluation With Open Items for Chapter 8, ‘Electric Power’,” May 4, 2018 (ML18060A115).
4. NuScale Power, LLC, Design Certification Application, Chapter 8, “Electric Power,” Revision 1, March 2018 (ML18086A179).
5. NuScale Power, LLC, “NuScale Power, LLC Submittal of the NuScale Standard Plant Design Certification Application (NRC Project No. 0769),” December 31, 2016 (ML17013A229).
6. NuScale Power, LLC, TR-1015-18653-P-A, “Design of the Highly Integrated Protection System Platform,” Revision 2, May 23, 2017 (ML17143A437).
7. NuScale Power, LLC, TR-1015-18653-P, “Design of the Highly Integrated Protection System Platform,” Revision 1, October 2016 (ML16309A614).
8. Advisory Committee on Reactor Safeguards, “Safety Evaluation of the NuScale Power, LLC Licensing Topical Report 1015-18653-P, Revision 1, ‘Design of the Highly Integrated Protection System Platform’,” April 24, 2017 (ML17108A433).
9. Advisory Committee on Reactor Safeguards, “Safety Evaluation of the NuScale Power, LLC Topical Report TR-0815-16497-P, ‘Safety Classification of Passive Nuclear Power Plant Electrical Systems, Revision 1’,” July 26, 2017 (ML17205A380).

10. NuScale Power, LLC, TR-0815-16497-P, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 1, February 2017 (ML17048A460).

11. U. S. Nuclear Regulatory Commission, “NuScale Power, LLC Safety Evaluation for Topical Report TR-0815-16497, Revision 1, ‘Safety Classification of Passive Nuclear Power Plant Electrical Systems’,” June 2017 (ML17170A196).

12. NuScale Power, LLC, TR-0815-16497-P-A, “Safety Classification of Passive Nuclear Power Plant Electrical Systems,” Revision 1, February 23, 2018 (ML18054B606).

10. NuScale Power, LLC, TR-0815-16497-P, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 1, February 2017 (ML17048A460).

11. U. S. Nuclear Regulatory Commission, “NuScale Power, LLC Safety Evaluation for Topical Report TR-0815-16497, Revision 1, ‘Safety Classification of Passive Nuclear Power Plant Electrical Systems’,” June 2017 (ML17170A196).

12. NuScale Power, LLC, TR-0815-16497-P-A, “Safety Classification of Passive Nuclear Power Plant Electrical Systems,” Revision 1, February 23, 2018 (ML18054B606).

Accession No: ML18270A374 **Publicly Available Y** **Sensitive N**
Viewing Rights: ☒ NRC Users or ☐ ACRS Only or ☐ See Restricted distribution *via email

OFFICE	**ACRS/TSB**	**SUNSI Review**	**ACRS/TSB**	**ACRS**	**ACRS**
NAME	MSnodderly	MSnodderly	MBanks	AVeil	MCorradini *(AVeil for)*
DATE	9/26/18	9/26/18	9/26/18	9/26/18	9/26/18

OFFICIAL RECORD COPY