

October 24, 2018

Docket No. 52-048

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

SUBJECT: NuScale Power, LLC Submittal of Changes to Final Safety Analysis Report, Section 7.0, "Instrumentation and Controls – Introduction and Overview," and Section 7.2, "System Features"

- REFERENCES:**
1. Letter from NuScale Power, LLC to Nuclear Regulatory Commission, "NuScale Power, LLC Submittal of the NuScale Standard Plant Design Certification Application, Revision 1," dated March 15, 2018 (ML18086A090)
 2. Letter from NuScale Power, LLC to Nuclear Regulatory Commission, "NuScale Power, LLC Submittal of Changes to Final Safety Analysis report, Section 7.0, 'Instrumentation and Controls – Introduction and Overview,' and Section 7.1, 'Fundamental Design Principles'," dated September 4, 2018 (ML18247A186)

During the Advisory Committee on Safeguards (ACRS) full committee meeting on September 6, 2018, NuScale Power, LLC (NuScale) discussed certain Final Safety Analysis Report (FSAR) sections related to isolation of distributed control systems. After this meeting, NuScale discussed a potential FSAR update to clarify the design of the isolation devices. As a result of these discussions, NuScale has changed the relevant parts of FSAR Section 7.0 and 7.2 to add these clarifications.

The Enclosure to this letter provides a mark-up of the FSAR pages incorporating revisions to these sections in redline/strikeout format. NuScale will include this change as part of a future revision to the NuScale Design Certification Application.

This letter makes no regulatory commitments or revisions to any existing regulatory commitments.

If you have any questions, please feel free to contact Paul Infanger at 541-452-7351 or at pinfanger@nuscalepower.com.

Sincerely,



Jennie Wike
Manager, Licensing
NuScale Power, LLC

Distribution: Samuel Lee, NRC, OWFN-8G9A
Gregory Cranston, NRC, OWFN-8G9A
Omid Tabatabai, NRC, OWFN-8G9A

Enclosure: "Changes to NuScale Final Safety Analysis Report Sections 7.0, 'Instrumentation and Controls – Introduction and Overview,' and Section 7.2, 'System Features' "

Enclosure:

“Changes to NuScale Final Safety Analysis Report Sections 7.0, ‘Instrumentation and Controls – Introduction and Overview,’ and Section 7.2, ‘System Features’ “

including chemical, utility, and support process systems to the NPM. The MCS is part of the nonsafety-related network and includes the associated network equipment and appurtenances necessary for network communication.

The MCS provides component-level control and monitoring of safety-related components that are specific to an NPM. The monitoring of the safety-related components is achieved by receiving one-way communications from the MPS to the MCS through isolation one-way communication ports on the MIB communication module. The controls of the ESF components by the MCS are manual component-level manipulations used for maintenance, testing, or aligning the components following refueling or actuation and not for safety-related purposes. The control signal from the MCS is hard-wired and sent through a qualified isolation device through the HWM to the EIM in the MPS, which contains priority logic that requires a safety-related enable signal prior to allowing control of the device from the MCS.

Figure 7.0-17 represents the MCS internal functions and external interfaces.

The boundary of the MCS is at the terminations on the MCS hardware. The MCS supplies nonsafety-related inputs to the HSIs for nonsafety displays in the MCR, the remote shutdown station, and other locations where MCS HSIs are necessary. There are two boundaries between MCS and MPS, the fiber-optic isolated portion and the HWM boundary. The MCS has a direct, bi-directional interface with the PCS. The network interface devices for the MCS domain controller/historian provide the interface between the human machine interface (HMI) network layer and the control network layer. A one-way deterministic isolation device between the connection from the MCS to the plant network is provided. The one-way deterministic isolation device between the MCS and plant network shown in Figure 7.0-1 transmits network traffic from the MCS to the plant network in one direction only, which is enforced in the hardware design, not software. No software configuration or misconfiguration will cause the boundary device to reverse the direction of data flow.

The MCS uses logic processing in the cases where redundant input/output channels are used. Some logic supports the redundant-channel architecture used by the MPS, while other logic directly supports the process systems. The logic processing of multiple channels can include two, three, or four input signals.

RAI 01-61

COL Item 7.0-1: A COL applicant that references the NuScale Power Plant design certification is responsible for demonstrating the stability of the NuScale Power Module during normal and power maneuvering operations for closed-loop module control system subsystems that use reactor power as a control input.

The NuScale power plant normal operation and power maneuvering control functions are provided by the following MCS functions for each NPM:

- turbine trip, throttle and governor valve control
- turbine bypass valve control
- feedwater pump speed control

The boundary of the PCS is at the terminations on the PCS hardware. The PCS supplies nonsafety inputs to the HSIs for nonsafety displays in the MCR, the remote shutdown station, and other locations where PCS HSIs are necessary. The boundary between the PPS and PCS is at the output connection of the optical isolators in the PPS. The PCS has a direct, bi-directional interface with the MCS. The network interface devices for the PCS domain controller/historian provide the interface between the HMI network layer and the control network layer. A one-way deterministic isolation device between the connection from the PCS to the plant network is provided. The one-way deterministic isolation device between the PCS and plant network shown in Figure 7.0-1 transmits network traffic from the PCS to the plant network in one direction only, which is enforced in the hardware design, not software. No software configuration or misconfiguration will cause the boundary device to reverse the direction of data flow.

The PCS uses logic processing in the cases where redundant input/output channels are used. Some logic supports the redundant-channel architecture used by the PCS, while other logic directly supports the process systems. The logic processing of multiple channels can include two, three, or four input signals.

7.0.4.6.1 Plant Control System Segmentation

Segmentation is used in the PCS control architecture to provide functional independence between major control functions. The segmentation is a key defensive preventive measure against a failure in one controller group from causing an undesirable condition in another controller group. Preventive and limiting measures are determined by a susceptibility analysis that considers malfunctions and spurious actuations, as set forth in NRC DI&C-ISG-04, Section 3.1, staff position 5. The purpose of the susceptibility analysis is to identify control groups that may lead to the following effects:

- reactivity addition
- primary coolant pressure increase or decrease
- primary coolant temperature increase or decrease
- primary coolant level increase or decrease
- radioactive material release to the environment

The PCS control architecture is separated into multiple control segments based on their functions. The major PCS control segment subject to a coping analysis is described below. This segment has a direct impact on the effects listed above and serves functions relating to protection of plant assets, human habitability, and radioactivity control as follows:

- EHVS, EMVS, and ELVS Segment — The EHVS, medium voltage AC electrical distribution system (EMVS), and ELVS use the same segment of the PCS for automatic and remote control functions. For the EHVS, the PCS controls each breaker except for the breaker that connects the turbine generator to the off-site customer loads.

- RPV water level
- containment water level

The bypassed and operable status indication of safety interlocks is automatically provided in the control room as described in Section 7.2.13.6 and satisfies the requirements of 10 CFR 50.34(f)(2)(v) and RG 1.47.

The SDIS conforms to 10 CFR 50.34(f)(2)(iv) by providing the capability to display the Type B and Type C variables identified in Table 7.1-7 over anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions.

The reactor safety valve position indication is processed by the MPS and then sent to the SDIS and the MCS for display in the MCR. The reactor safety valve position indication is seismically qualified to Seismic Category I requirements and meets the requirements of 10 CFR 50.34(f)(2)(xi).

Consistent with 50.34(f)(2)(xvii) the SDI system provides the capability to monitor containment pressure, containment water level, and the reactor containment atmosphere for radioactivity released from postulated accidents. The MCS provides the recording function for the containment parameters.

Consistent with 10 CFR 50.34(f)(2)(xvii)(C) and 10 CFR 50.44(c)(4), The PSS containment sampling system includes oxygen and hydrogen analyzers to monitor the containment environment. These monitors are non-safety related instruments that continuously monitor oxygen and hydrogen concentrations in containment during operation and are capable of monitoring during beyond design-basis conditions. The analyzers are designed to be functional, reliable, and will meet design criteria discussed in Regulatory Position C.2 of RG 1.7. The hydrogen analyzer output signal is sent to the MCS, which can provide readout in the main control room. Additionally, local indication is also provided as a backup display/indication in event that information from MCS cannot be displayed in the control room post-accident.

Consistent with 10 CFR 50.34(f)(2)(xvii)(E), the PCS displays and records in the MCR information on noble gas effluent release points for the NuScale plant.

As described in Table 1.9-5, the NuScale design supports an exemption from the power supply requirements for pressurizer level indication included in 10 CFR 50.34(f)(2)(xx).

7.2.13.7 Other Information Systems

There is a unidirectional communication interface between the MCS and PCS networks and the plant network and is shown in Figure 7.0-1. The one-way deterministic isolation devices transmits network traffic from the MCS and PCS to the plant network in one direction only, which is enforced in the hardware design, not software. No software configuration or misconfiguration will cause the boundary device to reverse the direction of data flow. The MCS and PCS systems provide monitoring data via one-way communication interfaces to the plant network which provides data recording, trending, and historical retention that can be retrieved on the emergency operations facility stations and technical support center (TSC) engineering workstations.