RAIO-0917-56055

September 19, 2017

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 Response to NRC Request for Additional Information No. 101 (eRAI No. 8940) on the NuScale Design Certification Application

REFERENCE: U.S. Nuclear Regulatory Commission, "Request for Additional Information No. 101 (eRAI No. 8940)," dated July 21, 2017

The purpose of this letter is to provide the NuScale Power, LLC (NuScale) response to the referenced NRC Request for Additional Information (RAI).

The Enclosure to this letter contains NuScale's response to the following RAI Questions from NRC eRAI No. 8940:

- 19-17
- 19-18

This letter and the enclosed response make no new regulatory commitments and no revisions to any existing regulatory commitments.

If you have any questions on this response, please contact Darrell Gardner at 980-349-4829 or at dgardner@nuscalepower.com.

Sincerely,

Zackary W. Rad
Director, Regulatory Affairs
NuScale Power, LLC

Distribution: Gregory Cranston, NRC, OWFN-8G9A
Samuel Lee, NRC, OWFN-8G9A
Rani Franovich, NRC, OWFN-8G9A

Enclosure 1: NuScale Response to NRC Request for Additional Information eRAI No. 8940

Enclosure 1:

NuScale Response to NRC Request for Additional Information eRAI No. 8940

NuScale Power, LLC
1100 NE Circle Blvd., Suite 200 Corvalis, Oregon 97330, Office: 541.360.0500, Fax: 541.207.3928
www.nuscalepower.com

Response to Request for Additional Information
Docket No. 52-048

eRAI No.: 8940
Date of RAI Issue: 07/21/2017

NRC Question No.: 19-17

It is stated in Section 19.0 of the Standard Review Plan (SRP), Revision 3, “Probabilistic Risk Assessment (PRA) and Severe Accident Evaluation,” that if an applicant is seeking approval of an application for a plant containing multiple modules, the staff reviews the applicant’s assessment of risk from accidents that could affect multiple modules to ensure appropriate treatment of important insights related to multi-module design and operation. The staff will verify that the applicant has:

i. Used a systematic process to identify accident sequences, including significant human errors, that lead to multiple module core damages or large releases and described them in the application.
ii. Selected alternative features, operational strategies, and design options to prevent these sequences from occurring and demonstrates that these accident sequences are not significant contributors to risk. These operational strategies should also provide reasonable assurance that there is sufficient ability to mitigate multiple core damages accidents.

NuScale has addressed the risk from accidents that could affect multiple modules in section 19.1.7. The staff has reviewed the information in section 19.1.7 and also reviewed non-docketed supporting material as part of its ongoing audit of the NuScale PRA. Based on its review the staff believes that section 19.1.7 of the Final Safety Analysis Report (FSAR) does not provide an adequate description of those design features and/or operational strategies to prevent the sequences described in the FSAR from occurring or reduce the likelihood of occurring. Therefore, please provide a description of such features and/or operational strategies that can prevent or reduce the likelihood of occurrence for the following events that can affect multiple modules:

· Loss of Offsite Power

· Station Blackout

· Complete Loss of a support system or support subsystem, as appropriate, including

- o reactor closed cooling water system
- o circulating water system

- instrument air system
- common DC power systems
- plant control system

· Fire induced events

- loss of offsite power
- transient
- emergency core cooling demand
- loss of coolant accident inside containment

· Internal flooding

If an adequate description is provided in a parts of the FSAR other than chapter 19, simply reference the section of the FSAR it is provided in. If the description does not exist elsewhere in the FSAR, please provide it in response to the above request and include the description in an update to the FSAR.

NuScale Response:

Consistent with Standard Review Plan (SRP) Section 19.0, NuScale used a systematic process to identify accident sequences, including significant human errors that could lead to multiple module core damages or large releases. As summarized in FSAR Section 19.1, the risk associated with multiple module operation at power was assessed using a quantitative assessment that was performed for a single-module coupled with a qualitative evaluation of the risk of multiple module operation, including the risk impact of shared system faults. The risk associated with low power and shutdown operation was evaluated using a similar approach as that used for the full-power evaluation with the additional consideration of events that are unique to the NuScale design, notably the potential for a dropped module. The methodology for evaluating multiple module risk, risk metrics, and key insights for both internal and external events are provided in FSAR Section 19.1.7.

The design and operational features for preventing core damage in a single module are summarized in FSAR Section 19.1.3.1 and these features are also applicable in preventing potential damage due to postulated challenges to multiple modules. Table 19.1-2 of the FSAR summarizes design features inherent to the NuScale design that addresses characteristics of currently operating plants related to operational risk. Table 19.1-3 summarizes key design decisions that were supported by PRA analyses.

In the multi-module configuration, safety-related systems are module-specific and functionally independent of shared systems and other modules. Thus, challenges to plant operations are minimized from events that can affect multiple modules; each module has redundant divisions of safety-related equipment which are independently capable of shutting down each module and

keeping each module in a safe condition for an extended period of time. As discussed in multiple sections of the FSAR, the passive design and automated actions place the NuScale power modules in a safe state where they remain for at least 72 hours without operator action for design basis events (e.g., loss of offsite power) as well as the beyond design basis events (e.g., station blackout) cited in Question 19-17.

As a result of the passive, fail-safe NuScale design features and operational strategies, the potential for an initiating event to affect the ability of multiple modules to respond to a plant upset is limited to nonsafety-related systems that support multiple module operation. These shared systems provide defense-in-depth backup to module-specific safety-related systems; the shared system hazard analysis is summarized in Table 19.1-76. The potential for events to result in damage to multiple modules (e.g., loss of offsite power, station blackout, complete loss of a support system, internal fire, internal flood) is mitigated by the passive, fail-safe NuScale design features and module-specific safety-related systems, as reflected in the low calculated individual module and multiple-module core damage frequencies. The full power internal events PRA for a single reactor module produces a core damage frequency that is extremely low in absolute terms and small in comparison to the NRC safety goal.

For clarification, FSAR Section 19.1.7.2 has been modified to reflect the functional independence of module safety systems and the potential effect of initiating events on shared systems. In FSAR Section 19.1.7.2, the discussion regarding risk significance has been modified to clarify the application of NuScale topical report TR-0515-13952-NP-A (FSAR Reference 19.1-8) to a multiple module configuration. FSAR Table 19.1-76 has also been modified to clarify the effect of some shared system faults.

Impact on DCA:

FSAR Section 19.1.7.2 and FSAR Table 19.1-76 have been revised as described in the response above and as shown in the markup provided in this response.

and 5.2E-13/mcyr, respectively. Figure 19.1-40 provides the point estimate MM-LRF by internal event initiator. As indicated in the figure, MM-LRF is dominated by outside containment pipe breaks.

Significant Multi-Module Sequences

The sequence with the highest contribution to MM-CDF is a reactor coolant system LOCA inside containment initiating event (IE-RCS---ALOCA-IC) followed by failure of ECCS, and failure to makeup RCS inventory from the CVCS, as illustrated by Figure 19.1-5, Sequence 3, which contributes about 31 percent of the MM-CDF. Sequences associated with a LOOP initiator (IE-EHVS--LOOP-----) followed by failure of the site AC power sources and incomplete actuation when the backup battery supplies are exhausted contribute more than 52 percent of the MM-CDF as indicated by Figure 19.1-9, Sequences 5 and 8.

The MM-LRF is dominated by outside containment pipe breaks occurring in the CVCS, with an injection line break contributing about 93 percent to the MM-LRF. The most significant sequence, illustrated in Figure 19.1-2, Sequence 7, is initiated by a CVCS injection line break outside containment (IE-CVCS--ALOCA-COC) followed by failure to makeup inventory by the CFDS and a failure to isolate the break as shown on the containment event tree, Figure 19.1-15, Sequence 3. The remaining initiators contribute negligibly to MM- LRF. The dominant contributors to MM-CDF do not contribute significantly to MM-LRF. Even though a multi-module core damage event is more likely with other initiating events, the CVCS line break initiating event also creates a direct release pathway and eliminates an RCS makeup path; thus, it is a more significant contributor to MM-LRF.

Significant Multi-Module Cutsets

Table 19.1-80 provides significant cutsets resulting from the multi-module full power internal events PRA. The top ten core damage cutsets are associated with about 40 percent of the MM-CDF. As seen from the table, with the exception of the first two cutsets, other cutsets taken individually are small contributors to the MM-CDF, and thus, are not presented in the table. The first two cutsets are associated with the initiating event IE-RCS---ALOCA-IC, which is primarily associated with spurious opening of an RSV. However, the cumulative total of all cutsets indicates that the LOOP initiator, IE-EHVS--LOOP-----, is the most significant initiator for MM-CDF. The dominant MM-LRF cutsets are associated with CVCS line breaks outside of containment.

RAI 09.05.04-1, RAI 19-17

Risk Significance

~~As was done for a single module, the multi-module PRA provides insights into the risk significance of SSC and operator actions with regard to CDF for multi-module risk. The methodology for evaluating significant SSC and operator actions with regard to multiple module risk is the same as that applied in evaluating single module risk.~~ Consistent with the risk significance determination methodology described in TR-0515-13952-NP-A (Reference 19.1-8), risk significance thresholds are applied on a single module level; therefore, insights related to multi-module design and operation were

identified through cutset reviews and sensitivity studies. As discussed in the multiple module "Key Insights" section, multi-module risk is significantly lower than risk from a single module; potential multi-module events are mitigated by safety systems that are functionally independent of shared systems and other modules.

RAI 09.05.04-1, RAI 19-17

~~There are no additional module-specific components that are found to be risk significant in the multiple module PRA than are identified as risk significant in the single module PRA. The site AC power sources, i.e., the shared backup diesel and CTG, are risk significant because of the importance of the site-wide LOOP initiator.~~

RAI 09.05.04-1, RAI 19-17

~~The only passive event meeting risk significance criteria is the event, ECCS--SYS-0001X-PTH-S, which represents a failure to transfer heat to the reactor pool from each module. As each module shares the reactor pool as an UHS, failure to transfer heat to the reactor pool is a risk significant event.~~

RAI 09.05.04-1, RAI 19-17

~~An additional human failure event, "CVCS--HFE-0001C-FOP-N" is found to be risk significant for MM CDF. The operator action for CVCS injection shows as risk significant in the MM PRA but not in the single module PRA. Accordingly, a sensitivity study was performed showing how sensitive the risk significance results are to the implemented HFE MMPSF value.~~

Key Assumptions

Key assumptions for the MM-PRA are:

- MMAF values are based on engineering judgment.
- Accident timing for multiple modules is not considered, i.e., multiple module failures are assumed to occur within the same 72-hour mission time as the single module event.
- Operator actions for inventory makeup from the CVCS and CFDS occur sequentially rather than simultaneously.
- Site-wide events are assumed to affect all modules equally.
- The calculated risk metrics apply to a multiple module event, irrespective of the number of installed modules, i.e., all modules are assumed to be affected due to an initiating event.

RAI 09.05.04-1, RAI 19-17

Uncertainties

The multi-module classifications and adjustment factors are judged to be bounding, so uncertainty factors are not assigned to MMAFs or MMPSFs. Parametric uncertainty associated with the MM-PRA evaluation is reflected in parametric ranges on the risk metrics. New model uncertainties arise from the use of MMAFs and MMPSFs, but the

majority of model uncertainties are the same as those associated with the single module PRA. ~~Sensitivity studies address potential uncertainties in MMAF and MMPSF values.~~

RAI 09.05.04-1, RAI 19-17

Sensitivity Studies

~~Sensitivity studies were~~A sensitivity study was performed to evaluate the effect of variation in the MMAF ~~and MMPSF~~ coupling values.

RAI 09.05.04-1, RAI 19-17

~~In the first study, t~~The values for MMAFs are altered so that equipment that is specific to each module is less correlated. This sensitivity provides insights into the effect of shared systems on the calculated CDF and LRF values. The sensitivity is accomplished by reducing the module-specific values of MMAF by an order of magnitude, e.g., the MMAF for LOCA (Pipe Break) provided in Table 19.1-78 is reduced from 0.01 to 0.001. The results of this sensitivity study are summarized as

- MM-CDF is reduced by approximately one-third.
- MM-LRF is reduced by approximately an order of magnitude.
- Site-wide initiating events such as LOOPs and losses of support systems are larger contributors to MM CDF while a reactor coolant system LOCA inside containment becomes less important. This illustrates that the relative importance of initiating events is sensitive to the conditional MMAF values. However, the calculated LRF remains small because events are mitigated by module-specific equipment.
- The MM-CDF contribution of LOCAs inside containment is decreased relative to the base model. The contributions from incomplete ECCS actuations and RPV overpressurizations (associated with RSV failures) are increased. Based on utilized values for MMAFs and the highest contributing accident types (ECCS and RCS failures, both of which are module-specific systems), failures to module-specific systems are required for core damage.

In summary, the sensitivity study focusing on shared equipment illustrates that the multiple module core damage sequences are most likely associated with shared system faults and site-wide initiators. However, module-specific equipment failure is also required for core damage, which limits the likelihood (and frequency) of multiple module core damage scenarios and thus, the resultant MM-CDF and MM-LRF.

RAI 09.05.04-1, RAI 19-17

~~The second study evaluates the importance of the operator action to initiate CVCS inventory. With a MMPSF for module-specific operator actions (HFE) set to ten, as indicated in Table 19.1-79, a CVCS inventory makeup action appears as risk significant in the MM PRA. In the single module PRA, this event does not meet the risk significance criteria. The MMPSF was reduced by a factor of two to evaluate whether the operator action is sensitive to the MMPSF value representing the action for multiple modules, or if the action is risk significant because of dependence on other MM factors or shared systems. The results of this sensitivity study are summarized as:~~

RAI 09.05.04-1, RAI 19-17

- ~~MM-CDF is reduced by approximately 20 percent.~~

RAI 09.05.04-1, RAI 19-17

- ~~MM-LRF is reduced by approximately 50 percent.~~

RAI 09.05.04-1, RAI 19-17

- ~~Reducing the MMPSF for module specific operator actions reduced the importance of the CVCS injection operator action below the threshold for risk significance. Therefore, calculated values of MM-CDF and MM-LRF are sensitive to the value of the MMPSF HFE factor.~~

RAI 09.05.04-1, RAI 19-17

Key Insights

The results illustrate that MM CDF is almost a factor of ten lower than the single module CDF. It is highly unlikely that core damage to multiple modules occurs, even though equipment for multiple modules can be demanded due to site-wide events like a LOOP; ~~module-specific equipment mitigates potential multiple module initiating events~~safety-related systems are module-specific and and functionally independent of shared systems and other modules. Further, the MM LRF ~~frequencies are~~is nearly two orders of magnitude less than the base model results. ~~Large releases in multiple modules are unlikely because site-wide initiating events (such as a LOOP) do not directly cause a containment bypass.~~ The low risk is a result of the innovative, passively-safe NuScale plant design. Neither onsite nor offsite power is required for design basis accident mitigation; the NuScale Power Plant is designed to maintain core cooling, spent fuel pool cooling, and containment integrity, independent of AC or DC power sources, for an extended duration. In addition, no operator actions are credited in the evaluation of design basis events; the passive design and automated actions place the NPMs in a safe state for at least 72 hours without operator action.

RAI 09.05.04-1, RAI 19-17

As a result of the passive, fail-safe NuScale design features and operational strategies, the potential to impact the ability of multiple modules to respond to a plant upset is limited to nonsafety-related systems that support multiple module operation. These shared systems provide defense-in-depth backup to module-specific safety-related systems. As such, multi-module accident sequences are not significant contributors to risk; events that can affect multiple modules (e.g., LOOP, station blackout, complete loss of a support system, internal fire) are mitigated by the passive, fail-safe NuScale design, and module-specific safety-related systems.

19.1.7.3 Insights Regarding External Events for Multi-Module Operation at Full Power

Some external events have the potential to cause damage in multiple modules because of their site-wide effect in a common time frame. The potential for a seismic event, internal fire, internal flood, external flood or high winds to cause damage to multiple modules is discussed below. Table 19.1-82 summarizes the potential coupling effects associated with external events on systems modeled in the PRA. The table summarizes whether an additional contribution to system unavailability is included in the PRA model due to the external event. For example, the table indicates that an area

- ECCS actuation valves open on loss of DC power at 24 hours

In this accident sequence, decay heat is transferred from the core to the reactor pool by convection and conduction induced by passive circulation of RCS fluid. The module reaches this configuration with passive valve operation, initially by the DHRS and long term by the ECCS. Inventory makeup is not required. Assuming twelve modules are shutdown, and there is no refill of the reactor pool from an external source and no credit for the condensation of evaporated water being returned to the reactor pool, the reactor pool water is sufficient for substantially longer than 30 days to remove decay heat.

19.1.10 References

19.1-1 ASME/ANS RA-S-2008, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-S-2008 (Revision 1 RA-S-2002), American Society of Mechanical Engineers, New York, NY, April 2008.

19.1-2 ASME/ANS RA-Sa-2009, "Addenda to ASME/ANS RA-S–2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications", American Society of Mechanical Engineers, New York, NY, American Nuclear Society, La Grange Park, IL, February 2009.

19.1-3 ASME/ANS RA-S-1.2-2014, "Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs)", Issued for Trial Use and Pilot Application, January 2015.

19.1-4 NEI 04-10 "Risk-Informed Technical Specifications Initiative 5b, Risk-Informed Method for Control of Surveillance Frequencies," Rev. 1, Nuclear Energy Institute, Washington DC, April 2007.

19.1-5 NEI 06-09 "Risk-Informed Technical Specifications Initiative 4b, Risk-Managed Technical Specifications (RMTS) Guidelines," Rev. 0, Nuclear Energy Institute, Washington DC, November 2006.

19.1-6 NUREG-1855 "Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making," Main Report, March 2009.

19.1-7 EPRI TR-1016737 "Treatment of Parameter and Model Uncertainty for Probabilistic Risk Assessments," Electric Power Research Institute, Palo Alto, CA, December 16, 2008.

RAI 09.05.04-1, RAI 19-17

19.1-8 ~~TR-051-13952-A~~TR-0515-13952-NP-A, NuScale Power, LLC Licensing Topical Report, "Risk Significance Determination", Rev 0, October 2016.

19.1-9 NUREG-0396 (EPA 520/1-78-016), "Planning Basis for the Development of State and Local Government Radiological Emergency Response Plans in Support of Light Water Nuclear Power Plants," December 1978.

Table 19.1-76: Shared System Hazard Analysis

System	Modules Served	Multiple module function	Accident Mitigation Implication	Credited in model for single module
Boron Addition System (BAS)	12	Add chemical shim to reactor coolant from the CVCS.	~~An inability to inject boron when needed constitutes an inability to support the key safety function of reactivity control. Reactivity control is ultimately provided by the RTS in the event of a plant upset.~~Reactivity control is provided by two independent systems, movable control rod assemblies and boron in the reactor coolant system. In the PRA, the module specific RTS and control rods are considered for reactivity control. The boron addition system also supports the safety function of removing fuel assembly heat by providing a source of makeup water to the ~~RPV~~CVCS to replenish lost inventory for certain beyond design basis events. ~~Demineralized water could alternatively be relied on for this purpose.~~Although the PRA currently models the DWS as the supply source to CVCS because of its capability to support the full 72 hour PRA mission time, a sensitivity study crediting the BAS as the initial inventory source and switching over to the DWS showed negligible changes in risk and no new risk insights.	~~Yes~~No
Control Room Habitability System (CRHS)	12	Controls Control Room humidity, air pressure, ventilation, heating, cooling (including for Control Room equipment heat loads), and carbon dioxide levels.	Failure of the CRHS on its own does not hinder accident mitigation efforts because it is a standby system that offers defense-in-depth against beyond design basis accidents. The CRHS is signaled by the plant protection system when harsh conditions are detected in the CRB. The harsh conditions (e.g., high radiation levels) that threaten MCR habitability and demand actuation of the CRHS imply that a severe accident has progressed to the point of core damage with potential radionuclide release. At this point in the beyond design basis accident the key safety functions have already been compromised and severe accident mitigation strategies would need to enacted.	No
Normal Control Room HVAC System	12	Provides heating, ventilation, and air conditioning to the CRB.	~~There is insufficient information at the design stage to assess the MCR capability to withstand elevated ambient room temperatures.~~In the event of a loss of the normal control room HVAC system, the CRHS automatically provides air to the control room for at least 72 hours. A loss of the normal control room ventilation system does not adversely affect safety-related functions.	No
Reactor Building HVAC System	12	Provides heating, ventilation, and air conditioning for Reactor Building and fuel handling area.	It is expected that operations would continue despite a loss of the Reactor Building HVAC system in the short term. In the longer term, a controlled shutdown of the modules might be decided upon administratively for protection of plant assets. ~~Technical specification 3.3.6 states that the remote shutdown station shall be operable. The loss of HVAC equipment in the remote shutdown area would challenge this specification.~~	~~No~~Yes[1]

Table 19.1-76: Shared System Hazard Analysis (Continued)

System	Modules Served	Multiple module function	Accident Mitigation Implication	Credited in model for single module
Pool Leakage Detection System	12	Leak detection systems for the reactor, refueling and spent fuel pools.	During the course of establishing a safe, shutdown condition for a plant upset, operators would be monitoring the effectiveness of the UHS closely because it is the source of passive cooling for the afflicted module(s). The pool leak detection system would serve as a redundant source of information to the MCR to indicate reactor pool viability. A loss of the reactor pool leakage detection system is a loss of defense-in-depth and would not significantly hamper accident mitigation.	No
Containment Flooding and Drain System (CFDS)	6 x 2	Add water to containment prior to refueling and to remove water from the containment prior to reactor startup.	The CFDS offers defense-in-depth as a means for passive containment heat removal in certain beyond design basis events whereby the safety-related response of establishes the DHRS or the ECCS as heat sinks were ineffective. Given how CFDS is designed with two subsystems dedicated to six modules each, it is assumed capable of delivering water to an afflicted module in each six-module set simultaneously.	Yes
Reactor Component Cooling Water System (RCCWS)	6 x 2	~~Cooling water that may become radioactive that is used to cool~~ Provides cooling to primary system components, e.g. control rod drive mechanisms.	The systems interfacing with the site cooling water are not safety-related including the RCCWS. ~~All modules could enter a safe, shutdown condition by shutting down and rejecting heat to the reactor pool without being hindered by the loss of reactor component cooling water because the heat loads would be removed from service.~~Failure of an RCCW subsystem could result in manual shutdown of up to six modules and a complete loss of the RCCWS could result in a manual shutdown of all modules, but neither situation will have an impact on safety-related functions.	No
Process Sampling System (PSS)	12	Collects liquid and gaseous samples from process fluid streams.	This system does not serve a function related to the avoidance of core damage.	No
Feedwater Treatment (FWT)	6 x 2	Feedwater treatment includes the chemical addition tanks and pumps used to make adjustments to secondary side chemistry.	This system does not serve a function related to the avoidance of core damage.	No
Condensate Polisher Resin Regeneration System (CPRRS)	6 x 2	Resin regeneration for the condensate polishers.	This system does not serve a function related to the avoidance of core damage.	No
Chilled Water System	12	Provides cooling water for air handling units.	There is insufficient information at the design stage to assess how equipment would respond to a loss of heating, ventilation and air conditioning.	No
Auxiliary Boiler System (ABS)	12	Provides steam for turbine generator gland seals, building heat/hot water, and module heatup system heaters.	This system does not serve a function related to the avoidance of core damage.	No

Table 19.1-76: Shared System Hazard Analysis (Continued)

System	Modules Served	Multiple module function	Accident Mitigation Implication	Credited in model for single module
Turbine Lube Oil Storage System	6 x 2	Provides clean and dirty turbine lube oil storage, transfer, and treatment.	This system does not serve a function related to the avoidance of core damage.	No
Cathodic Protection System	12	Provides oxidation protection for plant tanks and pipes in contact with the ground.	This system does not serve a function related to the avoidance of core damage.	No
Circulating Water System	6 x 2	Supplies cooling water to the condensers of the main turbines, and auxiliary equipment and services. Includes treatment.	A loss of circulating water may result in a loss of condenser vacuum or a loss of feedwater and would require that all modules enter shutdown using the reactor pool as the UHS. Circulating water does not interface with any of the safe shutdown equipment.	Yes[1]
Site Cooling Water System	12	Site cooling water supplies a heat sink to reactor pool cooling and spent fuel pool cooling which serve a role in fuel assembly heat removal for sequences that rely on the reactor pool as the UHS.	This system does not serve a function related to the avoidance of core damage.	No
Potable Water System	12	Provides drinking water for plant personnel.	This system does not serve a function related to the avoidance of core damage.	No
Utility Water System	12	Provides clarified water supply to the plant.	This system does not serve a function related to the avoidance of core damage.	No
Demineralized Water System (DWS)	12	Provides transport and distribution of demineralized makeup water; includes demineralizers, pumps, filters, and storage tanks. Includes treatment.	In the event of a LOCA, demineralized water from the demineralized water storage tank or borated water from the boric acid storage tank can be used to replenish the lost primary coolant through connections to the CVCS injection piping. This directly supports the safety function of fuel assembly heat removal for certain accident sequences.	Yes
Nitrogen Distribution System	12	Nitrogen storage and distribution system used for tank pressurization and other applications.	This system does not serve a function related to the avoidance of core damage.	No
Service Air System	12	Air distribution system for plant service applications, such as temporary supply for pneumatic equipment.	This system does not serve a function related to the avoidance of core damage.	No

Table 19.1-76: Shared System Hazard Analysis (Continued)

System	Modules Served	Multiple module function	Accident Mitigation Implication	Credited in model for single module
Instrument and Control Air System	12	Air compression and distribution system to provide compressed air for pneumatically actuated valves and instruments. Also supplies service air system.	The loss of instrument air ~~represents~~will cause closure of the secondary main steam isolation valves and is considered an initiating event with a trip on all modules. ~~Following this, decay heat removal should be provided offered by the DHRS and the ECCS. The CVCS makeup provision following an incomplete actuation of ECCS would align to a supply from the boron addition system when each module's CVCS makeup isolation valve fails to the open position and~~In addition, because each module's makeup combining valve fails to the ~~boron addition system position~~BAS following a loss of instrument air, CVCS is not considered for accident mitigation following the loss of support system initiator.	Yes[1]
Turbine Building HVAC System	6 x 2	Provides heating, ventilation, and air conditioning for turbine building.	There is insufficient information at the design stage to evaluate the ability of equipment to continue operation under conditions beyond their environmental qualifications.	No
Diesel Generator Building HVAC System	12	Provides heating, ventilation, and air conditioning for the diesel generator building.	The effect of elevated ambient conditions on equipment performance is not established at the design stage. A complete loss of the diesel generator building would affect the plant response to only a LOOP.	No
Annex Building HVAC System	12	Provides heating, ventilation, and air conditioning for the annex building.	This system does not serve a function related to the avoidance of core damage.	No
Fire Protection System	12	Prevents fires and minimizes the damage caused by fires.	The fire protection system is the means for preventing fire propagation. A fire has the potential to affect key safety functions depending on where it occurs.	No
Balance-of-Plant Drain System	6 x 2	Provides drainage for non-radioactive waste from balance-of-plant floor drains and non-radiological controlled locations.	This system does not serve a function related to the avoidance of core damage.	No
13.8 KV and Switchyard System (EHVS)	12	This electrical system begins at the circuit breakers which connect the switching station to the off-site transmission system and ends at the terminals of the plant main generator and at the high voltage terminals of the unit auxiliary transformers.	The plant is designed to cope with a station blackout beyond 72 hours through a combination of engineered safety features that actuate on loss of control power and passive cooling to the reactor pool. Although not modeled in the PRA, the system includes cross ties that automatically transfer supply power following a fault. The PRA models a combustion turbine generator as the auxiliary AC power source that can supply power to the EHVS.	Yes
Medium Voltage AC Electrical Distribution System (EMVS)	12	Provides power at 4160 VAC to busses servicing medium voltage loads.	The plant is designed to cope with a station blackout beyond 72 hours through a combination of engineered safety features that actuate on loss of control power and passive cooling to the reactor pool.	Yes

Table 19.1-76: Shared System Hazard Analysis (Continued)

System	Modules Served	Multiple module function	Accident Mitigation Implication	Credited in model for single module
Low Voltage AC Electrical Distribution System (ELVS)	12	Provides power at 120 VAC and 480 VAC to busses servicing low voltage loads.	The ELVS ~~system~~, although associated with a single module, has loads like DWS which are associated with multiple modules. ~~The loss of DWS would impact water makeup capacity for LOCA events.~~However, the DWS loads for a multi-unit plant will be distributed among different modules to minimize the burden. Although not modeled in the PRA, the system also includes cross ties that automatically transfer supply power following a fault. The BDGs can also supply power to the ELVS.	Yes
~~Safety DC Electrical and Essential AC Distribution~~Highly Reliable DC Power System (EDSS)	12	Failure-tolerant source of 125V DC power to plant loads including emergency lighting, module/plant protection, and post-accident monitoring loads.	Loss of EDSS common loads would complicate emergency response efforts from the MCR with the loss of emergency lighting, loss of control room habitability supporting equipment and failure of the monitoring from both the safety display and indication system and plant protection system; the EDSS common plant subsystem (i.e., EDSS-C) is not modeled in the PRA, only the module-specific portion of the EDSS subsystem (i.e., EDSS-MS) is modeled.	~~Yes (module specific portion)~~No (common plant system is not modeled)
Normal DC Electrical and AC Distribution System (EDNS)	12	Provides power to nonsafety control and instrumentation loads.	The loss of the EDNS would not hinder the ability of each module to reach a shutdown condition because the control rods would be released into the core by gravity. The EDNS would impede the ability of operators to monitor and respond to accidents because of the loss of MCR panels. Operators would need to rely on the safety display and indication system for monitoring of the RTS and engineered safety features.	No
Backup Power Supply System	12	Backup power source to onsite power using either a diesel generating set or a combustion gas turbine generating set, or other power supply source.	The unavailability of the two backup diesel generators and auxiliary AC power source would reduce defense-in-depth of the station, specifically in response to loss of an offsite power event. The plant is designed to cope with a station blackout beyond 72 hours through a combination of engineered safety features that actuate on loss of control power and passive cooling to the reactor pool.	Yes
Plant Lighting System	12	Provides normal, emergency and security plant lighting.	Loss of normal and emergency lighting would hinder operators' ability to respond to accidents using normal lighting.	No
Grounding and Lighting Protection System	12	Provides plant grounding and lightning protection	This system does not serve a function related to the avoidance of core damage.	No

Table 19.1-76: Shared System Hazard Analysis (Continued)

System	Modules Served	Multiple module function	Accident Mitigation Implication	Credited in model for single module
Safety Display and Indication (SDI)	12	Provides important to safety visual display and indication in the MCR of information from the MPS and the plant protection system.	The SDI displays offer an alternative indication of plant status to the MCR panels. If the MCR panels are offline due to a station blackout then the SDI offers 72 hours of operability from the EDSS common plant batteries. This timeframe is greater than the 40 minutes duty life of the backup batteries for EDNS servicing the MCR displays. The system is not credited for mitigating accidents.	No
Plant Control System (PCS)	12	Process control and monitoring for plant-wide or shared instrumentation and control systems including radiological and historical information systems. This system includes manual controls and visual display units.	The shutdown of all 12 modules would commence automatically if the system is failed. Operators could monitor the status of the plant and control safety-related protective actions using the SDI panels combined with MPS safety-related hand switches. The system is not credited for mitigating accidents.	~~No~~Yes[1]
Plant Protection System (PPS)	12	Plant-wide or shared important to safety instrumentation and control systems (e.g., control room habitability actuation).	~~Failure of the CRHS on its own does not hinder accident mitigation efforts because it is a standby system that offers defense-in-depth for beyond design basis accidents. The system is not credited for mitigating accidents~~Although the primary role of the PPS is to provide information on control room habitability conditions and send plant parameters to the safety display and indication system, its failure does not hinder accident mitigation; plant monitoring and control would remain available from the main control room.	No
Radiation Monitoring System	12	Detectors necessary for monitoring radiation levels of various plant areas (not associated with a specific process or mechanical system). Automatic responses (alarms, controls, etc.) from these detectors to be provided by the module control system or the PCS as necessary.	This system does not serve a function related to the avoidance of core damage.	No
Health Physics Network	12	Includes plant radiation monitoring, indication, and alarm equipment necessary to ensure occupational doses to plant personnel are as low as is reasonably achievable.	This system does not serve a function related to the avoidance of core damage.	No
Meteorological and Environmental Monitoring System	12	Provides atmospheric monitoring to advise plant personnel of impending climate conditions.	This system does not serve a function related to the avoidance of core damage.	No

Table 19.1-76: Shared System Hazard Analysis (Continued)

System	Modules Served	Multiple module function	Accident Mitigation Implication	Credited in model for single module
Communication System	12	Provides redundant offsite and onsite plant voice communication systems.	This system does not serve a function related to the avoidance of core damage.	No
Plant-Wide Video Monitoring System	12	Monitoring for areas frequently accessed where work is frequently preformed and areas of radiological significance.	This system does not serve a function related to the avoidance of core damage.	No
Seismic Monitoring System	12	Monitors and collects seismic data in to provide for analysis of seismic data and to notify the operator that a seismic event exceeding a preset value has occurred.	This system does not serve a function related to the avoidance of core damage.	No

Notes:

1. Considered in the context of an initiating event (i.e., challenge to continued plant operation).

Response to Request for Additional Information
Docket No. 52-048

eRAI No.: 8940
Date of RAI Issue: 07/21/2017

NRC Question No.: 19-18

The staff conducts its review of section 19.1.7 of the NuScale FSAR, "Multi-module Risk," using the following review process provided in Standard Review Plan (SRP) Chapter 19.0, Revision 3, "Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors":

"…the staff reviews the applicant's assessment of risk from accidents that could affect multiple modules to ensure appropriate treatment of important insights related to multi-module design and operation. The staff will verify that the applicant has:

1. *Used a systematic process to identify accident sequences, including significant human errors that lead to multiple module core damages or large releases and described them in the application.*
2. *Selected alternative features, operational strategies, and design options to prevent these sequences from occurring and demonstrated that these accident sequences are not significant contributors to risk. These operational strategies should also provide reasonable assurance that there is sufficient ability to mitigate multiple core damages accidents."*

The staff has reviewed information in Section 19.1.7 of the FSAR addressing multi-module risk; examined additional clarifying information during an audit of the fire PRA; and reviewed information in Appendix 9A of the FSAR, which includes the fire hazards analysis and a description of the fire safe-shutdown path. Some of this information suggests that there may be (1) single fire areas that contain equipment in redundant safety divisions relied upon for safe shutdown for multiple modules or (2) multiple fire areas in close proximity to one another that contain redundant equipment relied upon for safe shutdown for multiple modules. In light of this, the staff needs additional information to confirm that accident sequences stemming from fires are not significant contributors to multi-module risk. Specifically:

1. Please identify any single fire or flood areas that contain equipment in redundant safety divisions relied upon for safe shutdown of multiple modules. If such fire or flood areas exist, please (a) describe those design features and operational strategies put in place to ensure that any simultaneous fire or flood damage to safe shutdown equipment for multiple modules can be mitigated and (b) provide qualitative assessments of the likelihood of a fire or flood in the area and the likelihood that damaged equipment will achieve its fail-safe condition.

2. Please identify (a) those single fire or flood areas that contain safe shutdown equipment from a single safety division for multiple modules; and (b) those design features and operational strategies to prevent fires and floods from spreading to a fire or flood area that contains the redundant safe shutdown equipment for those same modules, including but not limited to, fire or flood barriers and physical separation.

Information provided in response to the above request should be included in an update to the FSAR.

NuScale Response:

Question 1: Multiple divisions of equipment that are required for safe shutdown will be located are in the main control room, under the bioshield, and inside the containment. Of these areas, only the main control room contains equipment for multiple modules. No other areas contain redundant structures, systems, and components (SSCs), including cabling, which, if subject to fire or flood, can prevent the performance of a safety function.

Question 2: Single fire and flood areas may contain safe shutdown equipment for a single safety division of multiple modules.

The following information provides additional detail regarding these aspects of the design:

Floods

Systems required for safe shutdown are safety-related and designed to perform their safety functions without electrical power. The systems require only valve operation to function and the loss of power to these systems results in these valves moving to their fail-safe positions. As such, it is highly unlikely that a flooding event would prevent a safety-related component from performing its safety function. In addition, flood protection criteria are identified in FSAR Section 3.4.1 and FSAR Table 3.4-2. Section 19.1.5.3 of the FSAR evaluates the risk for a single module associated with internal flooding; FSAR Section 19.1.5.4 evaluates external flooding risk. The discussion in FSAR Section 19.1.7 uses insights from the single-module evaluation to evaluate the potential effect of flooding on multiple modules. Item 2 of Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) Table 3.11-2 and Item 2 of ITAAC Table 3.13-1 address the design commitment that internal flooding barriers provide confinement so that the impact from internal flooding is contained within the area of origin for the reactor building and control building, respectively. Specific mitigation strategies for rooms requiring flood protection will be selected by the COL applicant as required by COL Item 3.4-2. COL Item 19.1-8 addresses the need to confirm the applicability of assumptions made in the PRA and modify the analysis as necessary for the as-built/as-operated plant.

Fires

Safe shutdown can be achieved following a fire in any area of the plant as discussed in FSAR Section 9A.6. Table 9A-7 of the FSAR identifies the systems required for safe shutdown.

Redundant divisions of safe shutdown systems are separated and protected from the effects of fire events, as discussed in FSAR Section 9A.6.3.1. Details regarding the fire detection and suppression systems are provided in FSAR Appendix 9A.5.1.

Similar to a module response to flooding, it is unlikely for a fire to result in damage to a safety-related component such that it cannot perform its safety function. Because NuScale's safety-related equipment is actuated on a loss of power, fire-induced circuit failures would have to manifest as hot shorts that persist for extended periods of time to prevent the safety function from occurring. That is, if the short clears (grounds), an affected component will move to its fail-safe position.

Cable routing and final control circuit designs have not yet been established. As such, elements in the fire PRA which are dependent on such details have a degree of uncertainty. Item 3 of ITAAC Table 3.7-1 addresses the need to perform a safe-shutdown analysis for the as-built plant, which will be informed by final cable routing and control circuit designs. COL Item 19.1-8 addresses the need to confirm the applicability of assumptions made in the PRA and modify the analysis as necessary for the as-built/as-operated plant. The PRA assumption regarding separation of redundant cabling in FSAR Table 19.1-46 has been revised for clarity.

Areas Containing Multiple Equipment Divisions

Multiple divisions of equipment that are required for safe shutdown will be located are in the main control room, under the bioshield, and inside the containment. Of these areas, only the main control room contains equipment for multiple modules. The main control room contains no flooding sources and, as identified in FSAR Table 3.4-2, is protected from the effects of flooding. Although not credited in the PRA, the anticipated operator action is to trip all reactors and isolate containment on all modules before evacuating the main control room in the unlikely event of a fire in the room.

Equipment under the bioshield and inside the containment is not susceptible to failure resulting from flooding. During normal operation, the containment is maintained at near vacuum conditions; this, coupled with a lack of combustibles, results in a fire being virtually impossible, as indicated in FSAR Section 9A.6.4.2.

The area under the bioshield is inaccessible when the bioshield is in place which eliminates the possibility of a transient fire. With a lack of ignition sources and minimal combustible loading, the probability of a fire in this area is judged to be negligible. Even in the highly unlikely occurrence of a fire, under the bioshield, the robust design of components, as described in FSAR Section 9A.6.4.3, in the area makes fire-induced failures unlikely.

Multi-Module Summary

Other than the main control room, there are no fire or flood areas that contain redundant safety equipment associated with the safe shutdown of multiple modules. In an area where multiple modules may be affected by a fire or flood event, potentially affected modules are capable of safely shutting down because (i) safety systems are not shared between modules and (ii) each module is supported by redundant divisions of safety-related equipment.

Impact on DCA:

FSAR Table 19.1-46 has been revised as described in the response above and as shown in the markup provided in this response.

RAI 19-18

Table 19.1-46: Key Internal Fire Probabilistic Risk Assessment Assumptions

Assumption	Basis
Fire compartments are screened if a fire in the compartment does not result in an automatic or manual plant trip and does not contain mitigating equipment.	Common engineering practice
For buildings that are not within the scope of the FHA, the fire compartment is the entire building. Other elements, not located inside a building, are grouped into a single fire compartment unless substantial fire barriers exist to justify separation (e.g., the plant yard area, transformers).	Common engineering practice
Cable routing and raceways are not defined at the design certification stage; fire affects are assumed from component and control equipment locations.	Engineering judgment
Fire-induced initiating events are grouped into four categories: a spurious ECCS valve opening, LOOP, RCS LOCA inside containment, and transient.	Engineering judgment
Fire frequencies are based on mapping plant ignition sources to generic fire bins and associated frequencies, and generally include equally weighted transient ignition sources. The highest error factor associated with any bin in a compartment was used for the compartment.	Common engineering practice
Detailed control circuits are not designed at the design certification stage; simplified circuit analysis is based on the material of construction and separation requirements.	Engineering judgment
Separation of redundant safe shutdown equipment and cabling is achieved ~~(i.e., one division of safe shutdown equipment remains free of fire damage for a fire in any fire compartment)~~.	Although not defined at design certification, the Fire Safe Shutdown Plan requires fire separation.
Electrical protective devices, including circuit breakers and fuses, are appropriately coordinated to preclude the possibility of fault current exceeding cable ampacity and also preclude the possibility of circuits credited in the FPRA from becoming associated with other circuits by sharing a common power supply.	Common engineering practice
A fiber optic control cable is not capable of causing a spurious component operation because it is not capable of producing a “hot short” per NEI 00-01. Therefore, when a fire is capable of damaging a fiber optic cable, it is only modeled as a loss of control.	Common engineering practice
No credit is taken for hot shorts to clear when they affect the inventory in the DHRS heat exchangers.	Bounding assumption
Simplified fire scenarios were developed for general compartment fires, MCR fires and multi-compartment fires.	Bounding simplification
A fire spreading from one compartment to another requires the failure of at least one passive fire barrier and the fire suppression system. Fires spreading into multiple additional compartments are judged to not be credible.	Engineering judgment
Screening probabilities are used for failure of fire suppression and passive barrier features.	Common engineering practice
Consistent with the internal events analysis, high stress was considered for operator actions.	Engineering judgment
Risk associated with seismic-fire interactions is small; no unique seismic fire hazards were identified and seismic events are not expected to challenge the fire suppression system.	Engineering judgment