Response to SDAA Audit Question

Question Number: A-19.1-19

Receipt Date: 04/17/2023

Question:

There are several locations throughout the NuScale SDA in Chapter 19 where it appears that an editorial change may be needed. The identified locations where this may be the case are:
1. In Section 19.1.7.3, it appears that the paragraph starting “For lower severity earthquakes, differences among NPMS…” is repeated.
2. In Table 19.1-21, under “Severe Accident Modeling (Level 2), the words “contaminant integrity” appear to be used in place of “containment integrity.”
3. In Section 19.3.2.3, the acronym “CDR” appears to be used in place of “CDF”.

Response:

The identified editorial changes have been incorporated into Chapter 19 of the standard design approval application.

Markups of the affected changes, as described in the response, are provided below:

Consistent with the risk-significance determination methodology described in TR-0515-13952-NP-A, risk-significance thresholds are applied on a single NPM level; therefore, insights related to multi-module design and operation are identified through cutset reviews and sensitivity studies. Table 19.1-21 summarizes the key assumptions associated with the multi-module PRA.

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 NPM PRA.

Two sensitivity studies are performed to evaluate the effect of variation in the MMAF and MMPSF coupling values. In the first study, values for MMAFs are altered so that NPM-specific equipment is less correlated. This focuses the quantification on shared and critical NPM-specific equipment. The first sensitivity study results show that reducing the NPM-specific MMAFs by a factor of ten reduces the MM-CDF by almost a factor of two and the MM-LRF by almost a factor of three. In the second study, the MMPSF for NPM-specific HFEs are decreased. The second sensitivity study results show that reducing the NPM-specific MMPSF from ten to two reduces the MM-CDF by over a factor of two and the MM-LRF by over an order of magnitude. These two sensitivity cases results show that the assumptions of correlation between module-specific failures and human performance has a significant effect on the estimated MM risk.

The results illustrate that MM CDF is almost a factor of five lower than the single NPM CDF. The risk is not inherent to any one system or initiator. Shared system initiators and site-wide events are the predominant contributors to core damage scenarios. Further, MM LRF is nearly a factor of thirty less than the single NPM results. As such, multi-module accident sequences are not significant contributors to risk; events that can affect multiple NPMs are mitigated by the passive, fail-safe design features, and NPM-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 NPMs is discussed below. Table 19.1-61 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.

Audit Issue A-19.1-19

Earthquakes, by their nature, affect multiple NPMs simultaneously. The modeling of multi-module seismic effects is outside the scope of a margin assessment. It should be noted, however, that bounding a single NPM core damage scenario as

applying to all NPMs is likely conservative for the higher likelihood, lower severity earthquakes. As ground accelerations become larger and larger, the conditional probability of inducing core damage in the first NPM, as well as multiple NPMs, approaches 1.0. ~~At lower severity earthquakes, differences among NPMs regarding building geometry, earthquake shear wave direction, and variances in configuration could be used to reduce the correlation among seismically-induced failures and limit the number of NPMs affected.~~

For lower severity earthquakes, differences among NPMs regarding building geometry, earthquake shear wave direction, alignment, and position are all relevant in the reduction of correlation among seismically-induced failures that limit the number of affected NPMs, as are NPM-specific estimates of in-structure demand.

For larger ground motions, structure failures likely impacting multiple NPMs are the dominant contributors to seismic risk. Related to RBC-related failures, catastrophic crane collapse into the reactor pool may affect multiple NPMs. However, such a collapse is unlikely based on the following:

- The peak acceleration of an earthquake is generally too short in duration relative to the period of seismic loading necessary to significantly affect the largest RBC support structures (e.g., bridge structure).
- The bridge is composed of large members with varying weight distributions that depend on the location of the hook across the bridge span and whether an NPM is significantly lifted or not (i.e., buoyancy considerations). Thus, simultaneous failure of multiple bridge seismic restraints or bridge structure connections is unlikely.
- The length of the RBC bridge girders is greater than the width between RBC support interfaces. Thus, girders are unlikely to collapse from the support surface in the event of a seismically-induced RBC failure.

In terms of initiating an upset to steady-state operations, multiple areas in the plant contain equipment that, if subjected to the effects of a fire, may result in a trip of multiple NPMs. This trip could be a direct response based on a loss of equipment or could be initiated by operators.

The system insights show that the only susceptibility to a common internal fire event is through the backup power supply system and the nonsafety-related makeup systems, CVCS and CFDS. When these systems are subjected to the effects of a fire, they are not credited in this assessment.

An internal fire may create the demand for more than one NPM to shut down, but given the fail-safe design of the DHRS, ECCS, and CIVs, there are no multi-module dependencies in the design that result in an elevated conditional probability of core damage or large release given core damage in the first NPM.

In terms of initiating an upset to steady-state operations, multiple areas in the plant contain equipment that, if flooded, may result in a trip of multiple NPMs. This

Audit Issue A-19.1-19

Table 19.1-21: Key Assumptions for the Probabilistic Risk Assessment

FULL POWER, INTERNAL EVENTS
Accident Sequence
If makeup inventory is needed, operators are assumed to initially align CVCS for coolant addition through the pressurizer spray line. If the RPV water level continues decreasing and operators observe increasing core temperatures, operators are assumed to realign CVCS coolant addition through the injection line.
Success Criteria
Procedures are assumed to direct operators to preserve the key safety function to remove fuel assembly heat even in cases where they would need to breach the containment boundary (e.g., operators would open the CVCS CIVs to inject makeup following incomplete ECCS actuation).
In the absence of an effective heat removal mechanism during a nominally intact reactor coolant pressure boundary scenario (that is, DHRS fails and RSVs fail to open), the RPV is expected to develop a leak (e.g., pressurizer heater access port bolted flange), and core damage is assumed.
Systems Analysis
Equipment is assumed to be operable without HVAC to support the PRA function. The small size of the equipment together with the slower progression of events provide sufficient time for any mitigating actions that might be needed.
Valve alignment for mitigating systems is assumed to include the capability to open following a loss of support systems (e.g., loss of instrument air) and accessibility for local access.
Shared systems (e.g., CFDS, DWS), are assumed to be available to support accident mitigation.
Failures are assumed to be “as-is”; failure constitutes the lack of signal generation, transmission, or interpretation through MPS equipment to the end-device.
Human Reliability Analysis
Maintenance on multiple system trains is assumed to be performed on a staggered basis; a maintenance error in the first train is assumed to be discovered before an error in the second train could occur.
For scenarios in which operators unisolate containment to initiate injection, but fail to prevent core damage, they are assumed to restore containment isolation.
Post-initiator human actions that include use of the O-1 override are assumed to require operators open the reactor trip breakers or wait until the high pressurizer level signal is no longer present, if needed.
Operators are assumed to control CVCS flow to provide necessary inventory for cooling; makeup actions are intended to maintain pressurizer level in the normal operating band.
Data Analysis
Passive safety system reliability of the DHRS and ECCS natural circulation heat transfer mechanisms are representative of the as-built, as-operated module
Component failure rates, based on design-specific analyses, are representative of the as-built module. Examples include “fails to operate” for the ECCS hydraulic-operated valve and equipment interface module.
FULL POWER, EXTERNAL EVENTS
Internal Flooding PRA
Flooding frequencies are assumed based on generic data for turbine and auxiliary buildings, including human-induced mechanisms. This is likely conservative since the NuScale design has fewer systems (hence fewer potential sources of internal flooding).
An internal flood does not result in an RSV demand if RTS and DHRS are successful.
Internal Fire PRA
Redundant divisions of safe shutdown equipment and cabling are assumed to be appropriately separated to assure at least one safe shutdown train is available following a fire.
Fire barriers are assumed between fire compartments and provide a fire resistance rating of 3 hours.
Seismic Margin Assessment
Generic spectral acceleration capacities for general component types (e.g., valves, heat exchangers, circuit breakers) are assumed applicable to components used in the NuScale design.

Table 19.1-21: Key Assumptions for the Probabilistic Risk Assessment (Continued)

Generic fragilities are assumed applicable to components in the NuScale design. The RXB is assumed to meet the seismic margin requirements of 167% of the reference earthquake for site-specific and soil-dependent seismic hazards (e.g., sliding, overturning, slope failure [instability], liquefaction). This is a design expectation.
Seismically-induced damage to reactor internals (e.g., fuel assembly, core supports, riser structure) such that the core may not be cooled is assumed to be not credible. This is a design expectation.
High Winds PRA
Although the plant is expected to use forecasting tools, a high winds event is assumed to result in a loss of offsite power with safety system actuation on low AC voltage (i.e., RTS, DHRS, and isolation of CIVs).
External Flooding PRA
An external flood that exceeds the design basis flood level is assumed to have a recurrence interval of 500 years; external flooding frequency is 2E-3/yr.
Although the plant is expected to use forecasting tools, 90 percent of external floods are assumed to include significant warning time for operators to perform a controlled shutdown, the remaining 10 percent are assumed to result in a loss of offsite power with safety system actuation on low AC voltage (i.e., RTS, DHRS, and isolation of CIVs). Controlled shutdowns are assumed to result in negligible risk, and are not evaluated. Most natural flooding occurs as a result of excessive precipitation, which is relatively slow developing.
LOW POWER and SHUTDOWN[1]
The mean probability that a dropped NPM fails to remain upright is 0.5, and uncertainty is characterized with a uniform distribution.
MULTIPLE MODULE EVALUATION
Accident timing for multiple modules is not considered; that is, 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.
Calculated risk metrics apply to a multiple module event, irrespective of the number of installed modules; that is, all modules are assumed to be affected because of to an initiating event.
SEVERE ACCIDENT MODELING (Level 2)
In RPV overpressure scenarios, core damage is assumed with no impact on containment~~contaminant~~ integrity.

Note 1: Key assumptions for the LPSD include key assumptions made in the Full Power PRA, as applicable.

modeling and performance of passive safety systems, including the likelihood that the passive safety systems might operate outside of the conditions where core heat removal would be effective.

Audit Issue A-19.1-19

The PRA model includes the failure probabilities and associated uncertainty estimates provided in Section 19.1.4 for failure of the two safety-related passive heat removal systems to operate effectively. The evaluation for RTNSS C likewise includes these failure probabilities. As described above and as demonstrated by the focused PRA, the design meets the CDF~~R~~ and LRF RTNSS C acceptance criteria without relying on nonsafety-related SSC. The assessment of the uncertainty of decay heat removal system and ECCS effectiveness justifies not including nonsafety-related active systems in the scope of the RTNSS Program for the RTNSS C criterion.

No nonsafety-related SSC are credited to meet NRC safety goals, to reduce the occurrence of initiating events, or to compensate for the uncertainties regarding passive systems in the PRA and in the modeling of severe accident phenomenology. Therefore, no nonsafety-related SSC meet the RTNSS C criteria.

19.3.2.4 Regulatory Treatment of Nonsafety Systems D

Evaluation of RTNSS D criteria involves identification of SSC functions necessary to meet containment performance goals during severe accidents. The containment performance goal is a measure of how well containment performs if challenged. The conditional containment failure probability is a probabilistic method used to evaluate containment performance and is calculated by dividing the LRF by the CDF. The numeric value of the containment performance goal is a conditional containment failure probability of 0.1, meaning that containment should fail no more than 10 percent of the times that core damage occurs. The PRA demonstrates that the conditional containment failure probability of 0.1 is met without relying on nonsafety-related SSC.

Analyses performed to support the development of the PRA model have determined there are no severe accident phenomena that pose a credible threat to the integrity of the CNV either within 24 hours or beyond 24 hours following the onset of core damage. Section 19.1 and 19.2 provide details on these considerations.

Since both the probabilistic and deterministic containment performance goals are met by relying on only safety-related SSC, no SSC are classified as RTNSS D.

19.3.2.5 Regulatory Treatment of Nonsafety Systems E

Evaluation of RTNSS E criteria involves identification of potential significant adverse interactions among passive safety-related systems and active nonsafety-related SSC. This evaluation is accomplished by analyzing the system functions that are identified through the D-RAP process. After identification of