NuScale Standard Plant
Design Certification Application

Chapter Nineteen
Probabilistic Risk Assessment and Severe Accident Evaluation

PART 2 - TIER 2

Revision 3
August 2019

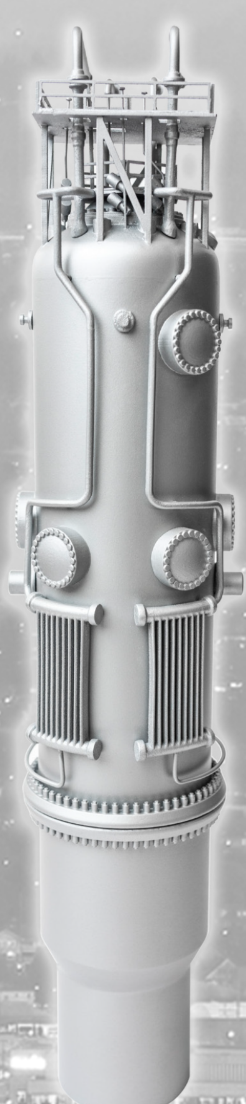


TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF TABLES

LIST OF TABLES

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

CHAPTER 19 PROBABILISTIC RISK ASSESSMENT AND SEVERE ACCIDENT EVALUATION

19.0 Probabilistic Risk Assessment and Severe Accident Evaluation

The purpose of this chapter is to describe the probabilistic risk assessment (PRA) which has been performed in accordance with 10 CFR 52.47(a)(27). Additionally, design features for the prevention and mitigation of severe accidents are also described in accordance with 10 CFR 52.47(a)(23).

As such, objectives of this chapter are to

- implement regulatory requirements, regulatory guidance and industry standards for a PRA and severe accident evaluation.
- provide a basis for update and upgrade of the PRA to support site-specific, as-built and as-operated considerations.
- demonstrate conformance with safety goals.
- provide insights on the robustness of the design to mitigate internal and external events.
- provide a basis for evaluating risk significant structures, systems, and components associated with an advanced design which uses simplified systems, natural circulation and passive components.
- provide insights on the effect of this advanced design on human performance requirements.

The PRA was performed for a "single module" using accepted industry techniques. The potential risk associated with multiple modules was evaluated based on insights from the formalized single module PRA. When referring to a specific module, the term "module" is used; when referring to multiple modules, the term "plant" or "site" is used.

When addressing general concepts, the term "PRA" as used in this chapter refers collectively to the Level 1 and Level 2 risk metric evaluation as well as the phenomenological evaluation of severe accident response. Due to the relatively small radionuclide inventory, risk metrics associated with a small modular reactor have different implications on public health and safety than those for larger plants. To reflect this perspective, and to clarify that the calculated risk metric values are based on a PRA for a single module, the terms "CDF" and "LRF" are used to present results for core damage frequency and large release frequency for a single module, respectively. The terms "MM-CDF" and "MM-LRF" are used when referring to "multiple module" (MM) risk metrics. The risk metric “CCFP” refers to the conditional containment failure probability associated with failure of a containment vessel (CNV) which houses each Nuclear Power Module (NPM).

The PRA demonstrates that the design exceeds NRC safety goals with a significant margin and thus, presents a very low risk to public health and safety.

19.0.1 Regulatory Requirements, Guidance and Industry Standards

The PRA was developed in accordance with applicable portions of 10 CFR 50 and 10 CFR 52, regulatory guidance and industry standards. Section 1.9 summarizes conformance with the Standard Review Plan, regulatory guides, NRC papers, interim staff guidance and generic issues. Additional regulatory and industry guidance such as that provided by NUREGs and NEI documents was also used and cited in this chapter as needed. The following high level regulatory and industry guidance documents were used in the development of the PRA, determination of risk significance and evaluation of conformance with safety goals:

- NRC Policy Statement, "Severe Reactor Accidents Regarding Future Designs and Existing Plants" (Reference 19.0-1)
- NRC Policy Statement, "Safety Goals for the Operations of Nuclear Power Plants" (Reference 19.0-2)
- NRC Policy Statement, "Nuclear Power Plant Standardization" (Reference 19.0-3)
- NRC Policy Statement, "Regulation of Advanced Nuclear Power Plants" (Reference 19.0-4)
- NRC Policy Statement, "The Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities" (Reference 19.0-5)
- SECY-90-016, "Evolutionary Light-Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements" (Reference 19.0-6)
- SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs" (Reference 19.0-7)
- 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) (Reference 19.0-8)
- Addenda to ASME/ANS RA-S-2008, ASME/ANS RA-Sa-2009 (Reference 19.0-9)
- ASME/ANS RA-Sb-2013, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications" (Reference 19.0-10)

19.0.2 Uses of the PRA and Severe Accident Evaluation

In the design phase, the NuScale PRA provides a systematic method to provide risk insights. Consistent with RG 1.206, the design phase PRA is used to

- identify and address potential design features and operational vulnerabilities. Such vulnerabilities include those in which a small number of failures, or common cause failures, leads to a probability of core damage, containment failure or radionuclide release which presents a risk that exceeds NRC safety goals.
- reduce or eliminate the significant risk contributors of existing operating plants that are applicable to the NuScale design by introducing appropriate features and requirements.
- select among alternative features, operational strategies, and design options to effectively minimize risk.
- evaluate the design's robustness, levels of defense-in-depth, and tolerance of severe accidents initiated by either internal or external events.

- evaluate the risk significance of specific human errors, including a characterization of the significant human errors for input to operator training programs and procedure refinement.
- demonstrate how the risk associated with the design compares against the NRC goals of less than 1×10^{-4}/year for core damage frequency and less than 1×10^{-6}/year for large release frequency. In addition, the design is evaluated against the containment performance goal, which includes (1) a deterministic goal that containment integrity be maintained for approximately 24 hours following the onset of core damage for the more likely severe accident challenges and (2) a probabilistic goal that the conditional containment failure probability be less than approximately 0.1 for the composite of the core damage sequences assessed in the PRA.
- assess the balance of preventive and mitigative features of the design, including consistency with the NRC guidance in SECY-93-087 and the associated staff requirements memorandum.
- evaluate whether the NuScale design represents a reduction in risk compared to existing operating plants.
- demonstrate that the design addresses known issues related to the reliability of core and containment heat removal systems at some operating plants (i.e., the additional TMI-related requirements in 10 CFR 50.34(f)).

The results and insights of the PRA are a source of information for other programs and processes:

- the process used to demonstrate whether the regulatory treatment of nonsafety-related systems (RTNSS) is sufficient and to identify the structures, systems, and components included in RTNSS.
- regulatory oversight processes and programs that are associated with plant operations, e.g., Technical Specifications, Reliability Assurance Program, human factors, and Maintenance Rule (10 CFR 50.65) implementation.
- the development of specifications and performance objectives for the plant design, construction, inspection, and operation, e.g., the Reliability Assurance Program and Technical Specifications.

19.0.3 Structure of Chapter 19

Section 19.1 summarizes the Level 1 and Level 2 PRA, which evaluates the risk associated with all modes of operation for both internal and external initiating events. The PRA was performed for a single module and used to develop insights for multiple modules, i.e., the plant. Major topics addressed in Section 19.1 are

- uses and application of the PRA.
- quality of the PRA.
- design features to minimize risk.
- internal event PRA methodology, data, sensitivities and results.

- external event PRA methodology, data, sensitivities and results. External events addressed for design certification are seismic, internal fires, internal flooding, external flooding, and extreme winds.
- PRA input to programs and processes.

Section 19.2 addresses the design features to prevent and mitigate severe accidents. Major topics addressed in Section 19.2 with regard to severe accidents are

- capability with regard to beyond design basis events, including those specifically identified by regulation, such as ATWS (10 CFR 50.62).
- severe accident phenomena and potential containment challenges.
- containment capability including ultimate pressure capacity and conditional containment failure probability.
- equipment survivability.
- severe accident management including design alternatives.

Section 19.3 addresses the consideration of nonsafety-related, risk signficant systems, including RTNSS designated systems.

Section 19.4 addresses the consideration of potential loss of large areas due to explosions or fires.

Section 19.5 addresses the capability to respond to potential aircraft impact events.

The PRA uses typical terminology to model potential initiating events. In two instances, this terminology may differ from the design specific interpretation applied in other DCD sections:

- LOCA: The LOCA initiating event category includes initiators that result in the release of reactor coolant due to pipe breaks or inadvertent valve opening, either inside or outside of the CNV; however, only pipe breaks inside containment meet the regulatory definition of LOCA.
- LOOP: The PRA analysis does not model operations using the island mode capability described in Section 8.3. A NuScale Power Module operating in island mode would be a source of normal AC power. The term LOOP, as used in the PRA analysis, would, without island mode, result in a loss of normal AC power.

19.0.4 References

19.0-1 U.S. Nuclear Regulatory Commission, "Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants," Federal Register, Vol. 50, No. 153, August 8, 1985, pp. 32138-32150.

19.0-2 U.S. Nuclear Regulatory Commission, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement," Federal Register, Vol. 51, No. 149, August 4, 1986, pp. 28044-28049.

19.0-3 U.S. Nuclear Regulatory Commission, "Nuclear Power Plant Standardization," Federal Register, Vol. 52, No. 178, September 15, 1987, pp. 34884-34886.

19.0-4 U.S. Nuclear Regulatory Commission, "Regulation of Advanced Nuclear Power Plants," Federal Register, Vol. 59, No. 149, July 12, 1994, pp. 28044-28049.

19.0-5 U.S. Nuclear Regulatory Commission, "The Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement," Federal Register, Vol. 60, No. 158, August 16, 1995, pp. 42622-42629.

19.0-6 U.S. Nuclear Regulatory Commission, "Evolutionary Light-Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements," Commission Paper SECY-90-016, January 12, 1990, and the related SRM dated June 26, 1990.

19.0-7 U.S. Nuclear Regulatory Commission, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs," Commission Paper SECY-93-087, April 2, 1993, and the related SRM dated July 21, 1993.

19.0-8 American Society of Mechanical Engineers, "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), New York, NY.

19.0-9 American Society of Mechanical Engineers/American Nuclear Society, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," Addenda to ASME/ANS RA-S-2008, ASME/ANS RA-Sa-2009, New York, NY.

19.0-10 American Society of Mechanical Engineers, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," ASME/ANS RA-Sb-2013 (Addenda to ASME/ANS RA-S-2008), New York, NY.

19.1 Probabilistic Risk Assessment

The NuScale probabilistic risk assessment (PRA) has been performed consistent with the requirements of 10 CFR 52.47(a)(27). It assesses the risk for a single NuScale Power Module (NPM) and includes both Level 1 and Level 2 evaluations. The NuScale PRA follows the guidance provided by Interim Staff Guidance (ISG) DC/COL-ISG-028 (Reference 19.1-3). This ISG specifically applies to design certification applications to address use of ASME/ANS RA-S-2008 and addenda ASME/ANS RA-Sa-2009 ("ASME Level 1 PRA Standard", Reference 19.1-1 and "ASME/ANS RA-Sa-2009", Reference 19.1-2), as endorsed by Regulatory Guide (RG) 1.200. The PRA supporting the design certification does not include a Level 3 evaluation (although a limited assessment was performed to support the severe accident management design alternatives [SAMDA] analysis).

The PRA evaluates the risk associated with operation of a single module at full power as well as low power and shutdown (LPSD) modes of operation for both the internal and the external initiating events that can be addressed at the design certification stage. The risk associated with multi-module operation is assessed using a systematic approach that includes both a qualitative evaluation of the potential impact of shared systems and a simple quantitative assessment based on the single-module, full-power, internal-events PRA to identify potential multi-module risk contributors.

Key aspects of the PRA and the associated insights are summarized in this section. Supporting documentation such as fault trees, initiating and basic event frequency calculations, human error calculation worksheets, and success criteria modeling is available to support U.S. Nuclear Regulatory Commission (NRC) reviews and audits.

19.1.1 Uses and Applications of the Probabilistic Risk Assessment

This section summarizes the uses of the PRA to support design certification, combined license (COL), construction, and operational activities.

19.1.1.1 Design Phase

The PRA is used during the design process to evaluate the safety of the NuScale Power Plant standard design. As such, dominant severe accident sequences, risk-significant structures, systems, and components (SSC) and key operator actions are identified. Insights from currently operating plants are evaluated for significance to the NuScale design. Conformance with NRC safety goals and design alternatives is evaluated. The specific uses of the PRA are summarized in Table 19.1-1. The section in which the use is described in more detail is also indicated.

19.1.1.2 Combined License Application Phase

The use of the PRA in the COL application phase is described in the following sections.

19.1.1.2.1 Use of Probabilistic Risk Assessment in Support of Licensee Programs

COL Item 19.1-1: A COL applicant that references the NuScale Power Plant design certification will identify and describe the use of the probabilistic risk assessment in support of licensee programs being implemented during the COL application phase.

19.1.1.2.2 Risk-Informed Applications

COL Item 19.1-2: A COL applicant that references the NuScale Power Plant design certification will identify and describe specific risk-informed applications being implemented during the COL application phase.

19.1.1.3 Construction Phase

The use of the PRA in the COL construction phase (from issuance of the COL up to initial fuel loading) is described in the following sections.

19.1.1.3.1 Use of Probabilistic Risk Assessment in Support of Licensee Programs

COL Item 19.1-3: A COL applicant that references the NuScale Power Plant design certification will specify and describe the use of the probabilistic risk assessment in support of licensee programs during the construction phase (from issuance of the COL up to initial fuel loading).

19.1.1.3.2 Risk-Informed Applications

COL Item 19.1-4: A COL applicant that references the NuScale Power Plant design certification will specify and describe risk-informed applications during the construction phase (from issuance of the COL up to initial fuel loading).

19.1.1.4 Operational Phase

The use of the PRA in the COL operational phase (from initial fuel loading through commercial operation) is described in the following sections.

19.1.1.4.1 Use of Probabilistic Risk Assessment in Support of Licensee Programs

COL Item 19.1-5: A COL applicant that references the NuScale Power Plant design certification will specify and describe the use of the probabilistic risk assessment in support of licensee programs during the operational phase (from initial fuel loading through commercial operation).

19.1.1.4.2 Risk-Informed Applications

COL Item 19.1-6: A COL applicant that references the NuScale Power Plant design certification will specify and describe risk-informed applications during the operational phase (from initial fuel loading through commercial operation).

19.1.2 Quality of the Probabilistic Risk Assessment

The PRA model is based on the module design for the purpose of design certification and not from an as-built, as-operated module or plant. For this reason, some of the supporting requirements of the PRA standard are not applicable or cannot be achieved (e.g., the ability to perform plant walkdowns); as such, DC/COL-ISG-028 was developed to convey the staff position on use of the PRA standard for a design certification application.

The NuScale PRA has sufficient detail to meet the NRC guidance in DC/COL-ISG-028. However, the level of detail is limited, as discussed in Section 19.1.2.2, because of design and operational uncertainties. To address uncertainties in the level of design and operating experience, as discussed in Section 19.1.2.2, NuScale has made bounding but realistic assumptions to ensure that an appropriate safety margin exists with respect to risk-informed information provided by the PRA.

The PRA was reviewed by an expert panel with membership external to NuScale. The panel membership included expertise in PRA, thermal hydraulics, seismic evaluation, and regulatory requirements. The expert panel addressed the general quality and completeness of the PRA. A self-assessment of the PRA was also performed; this self-assessment was reviewed by external consultants to ensure its accuracy. The self-assessment provided a detailed consideration of the PRA with respect to conformance with industry PRA standards. Feedback from the expert panel and self-assessment were reflected in the development of the PRA.

19.1.2.1 Probabilistic Risk Assessment Scope

The PRA addresses internal and external initiating events (or "initiators") and all operating modes, which are represented by specific evaluations of “full” or "at-power" conditions and at LPSD conditions. The PRA has been performed to evaluate the risk associated with a single module; the risk insights associated with a multiple module plant are based on insights from the single module PRA. Multiple-module risk evaluation is based on a 12-module configuration.

19.1.2.2 Probabilistic Risk Assessment Level of Detail

The level of detail in the PRA is consistent with its intended uses in support of design certification. However, at the design certification stage, there are limitations in available, detailed information by comparison to an as-built, as-operated plant. Further, because there is no operating experience with the NuScale design, insights from operating experience are limited. Thus, the level of detail in the PRA is limited because

- the specific layout and location of equipment and cabling are not known.
- the full and accurate capability of equipment and equipment operating characteristics are not known.
- plant-specific and operating data and procedures are unavailable.
- plant-specific experience to support human reliability analysis (HRA) is not available.
- plant walkdowns cannot be performed to gain as-built insights.
- plant-specific maintenance and testing schedules or data are unavailable.
- there are no similarly designed plants for comparison.
- a site has not been selected to support identification and evaluation of external hazards.

These factors contribute to the uncertainties associated with a design-stage PRA. The conservative, but realistic, assumptions that are applied to account for these uncertainties ensure an appropriate safety margin is present with respect to risk-informed information generated by the PRA and that key insights are not masked. The specific assumptions also account for design-specific uncertainty associated with unique component design features and thermal-hydraulic conditions of the NuScale design.

19.1.2.3 Probabilistic Risk Assessment Technical Adequacy

The PRA has been performed consistent with the guidance provided in DC/COL-ISG-028 which supplements RG 1.200 as an acceptable approach to demonstrate that the PRA used in the design certification application has a sufficient level of technical adequacy to support certification. The ISG includes applicability of the supporting requirements, feasibility of meeting the supporting requirements, and supplemental guidance for addressing the supporting requirements at the Capability Category I level. This ensures that the PRA relied on is sufficient to provide confidence in the results and risk insights.

The PRA has sufficient detail to meet the ISG guidance recommendations for Capability Category I supporting requirements. In the majority of cases, the level of detail provided in the PRA suffices in meeting Capability Category II supporting requirements of the ASME/ANS probabilistic risk assessment standard.

A NuScale plant can incorporate up to 12 modules. Evaluation of the risk of multiple-module operation is based on the single-module, full-power, internal-events PRA. A systematic process is used to identify accident sequences, including significant human errors, that are associated with multiple-module risk.

19.1.2.4 Probabilistic Risk Assessment Maintenance and Upgrade

The PRA is maintained and documented in a manner that facilitates PRA application, upgrade, and peer review. Key elements of PRA maintenance at the design stage PRA are:

- consistency with the design submitted for certification
- configuration control of applicable software and the PRA models of record
- documentation of sources and processes to determine model inputs
- documentation of assumptions
- documentation of sensitivity studies
- documentation of model results including uncertainties

To reflect changes after design certification, the PRA is maintained and upgraded by the COL applicant as required by 10 CFR 50.71(h)(1). The upgraded PRA must meet requirements of the NRC-endorsed PRA standards in effect one year prior to each required upgrade.

In the operational phase, the PRA is maintained and upgraded by the COL holder as required by 10 CFR 50.71(h)(2). The PRA must be upgraded every four years until the permanent cessation of operations per 10 CFR 52.110(a).

19.1.3 Special Design and Operational Features

The NuScale integral small modular reactor design is developed with consideration of features that enhance safety in comparison to earlier designs. Such features reduce the potential for core damage and limit the potential for radionuclide release from containment. Section 19.1.3.1 through Section 19.1.3.4 summarize these features.

19.1.3.1 Design and Operational Features for Preventing Core Damage

The NuScale design is simpler than typical, currently operating larger plants such that it minimizes plant challenges and enhances system reliability for responding to such challenges. Design features that reduce the potential for core damage include:

- The integral primary system with natural circulation of primary coolant has fewer components and is smaller in size. This reduces the core damage frequency (CDF) by eliminating many of the potential plant challenges associated with external piping.
  - Piping external to the reactor pressure vessel (RPV) is of relatively short length and small diameter.
  - There are no RPV or containment vessel (CNV) penetrations below the top of the reactor core.
- The large reactor coolant volume-to-reactor power ratio results in a thermal margin (difference between 2200 degrees F peak clad temperature and predicted peak clad temperature) in the limiting design basis loss-of-coolant accident (LOCA) event that is much larger than typical currently operating plants.
- Natural circulation primary system flow design results in reduced CDF by eliminating reactor coolant pump seal failure events because there are no reactor coolant pumps.
- The evacuated steel CNV allows elimination of RPV insulation, which eliminates potential sump blockage concerns. Concrete cracking issues are also eliminated.
- Containment volume is sized so that the core does not uncover for initiating events associated with loss of reactor coolant system (RCS) inventory inside containment or pipe breaks outside the CNV that are isolated.
- Passive, fail-safe safety systems for decay heat removal, emergency core cooling, and containment heat removal eliminate the need for external power under accident conditions.
  - Safety systems employ components that fail-safe to their accident response position on loss of power.

19.1.3.2 Design and Operational Features for Mitigating the Consequences of Core Damage and Preventing Releases from Containment

The NuScale design includes features that arrest the progression of a postulated core damage event and prevent releases from containment. Such features include:

- The containment system employs valves that fail-safe to their accident response position on loss of power.
- The evacuated containment results in an oxygen deficient environment that limits the formation of a combustible hydrogen mixture for postulated severe accidents.
- The steel CNV eliminates the potential for molten core-concrete interaction.
- The RPV and CNV are immersed in the reactor pool, which allows passive heat transfer from the core to the ultimate heat sink (UHS).
- The small, low power density of the NuScale core and un-insulated RPV enhance the potential for retention of core debris in the RPV in the event of core damage.

19.1.3.3 Design and Operational Features for Mitigating the Consequences of Releases from Containment

The NuScale design includes features intended to terminate containment releases and minimize offsite consequences:

- A NuScale reactor core has a relatively small amount of radioactive material available for release during a postulated accident.
- The containment is partially immersed in an underground, stainless steel-lined, concrete pool (i.e., the UHS); the supply of cooling water substantially exceeds 30 days.
- In the event of a CNV breach below the reactor pool water level, the pool may act to filter radionuclides before they reach the environment.

19.1.3.4 Uses of Probabilistic Risk Assessment in the Design Process

The NuScale design was developed in consideration of issues associated with typical currently operating plants. Thus, there are several design features inherent to the NuScale design that address characteristics of currently operating plants related to operational risk. Table 19.1-2 summarizes these features, which contribute to a low NuScale risk profile. The PRA was used to further reduce the risk profile by evaluating design options during the design process. Table 19.1-3 summarizes key design decisions that were supported by PRA analyses. Further, evaluation of SAMDA, as described in Section 19.2.6, was supported by PRA analyses.

19.1.4 Safety Insights from the Internal Events Probabilistic Risk Assessment for Operations at Power

The internal events PRA for a single NuScale Power Module operating at full power is discussed in this section. Section 19.1.4.1 discusses the Level 1 model and results for a single module. Consideration of multiple-module operation, based on the single-module PRA, is also discussed.

Section 19.1.4.2 discusses the Level 2 PRA and associated results.

19.1.4.1 Level 1 Internal Events Probabilistic Risk Assessment for Operations at Power

Internal events, within the scope of the PRA, are those events that originate within the NuScale plant boundary that directly or indirectly perturb the steady-state operation of the plant and could lead to an undesired plant condition.

This section summarizes the Level 1 PRA (i.e., risk assessment associated with core damage) associated with operation of a single module. The full-power PRA addresses the risk associated with operation in Technical Specification Mode 1 (Operations).

Section 19.1.4.1.1 describes the Level 1 PRA for full-power operations;
Section 19.1.4.1.2 provides the results of that evaluation.

19.1.4.1.1 Description of the Level 1 Probabilistic Risk Assessment for Operations at Power

The following sections address the methodology, data, and analytical tool used to perform the full power, internal events Level 1 PRA.

19.1.4.1.1.1 Methodology

The PRA was constructed by first developing a representative spectrum of potential internal initiating events. For each initiating event, a "Level 1" event tree was constructed to illustrate the sequence logic for the module response. This logic illustrates module response to an initiating event by identifying appropriate "top events." The top events represent systems that can mitigate the respective initiating event, either by themselves or in combination with other systems. The top events of the event trees include both safety-related and nonsafety-related mitigating systems.

The top events of the event trees are modeled using fault trees. Fault trees were constructed to represent mitigating and associated support systems. In addition to component failures and phenomelogical events (e.g., heat transfer fails), the fault trees include operator actions as well as test and maintenance unavailabilities. Fault trees evaluate the failure probability of a given system based on defined success criteria and account for dependencies between systems. Several variations of system fault trees may be developed based upon the success criteria requirements for a particular initiating event, or for different initiating events.

Systems included in the PRA model are summarized in Table 19.1-4.
Table 19.1-5 is the system dependency matrix which illustrates the interrelationship between the frontline systems, as indicated in the horizontal axis, and their supporting systems, which are on the vertical axis. Frontline systems are defined as those included as top events on an event tree. Dependencies are identified by shaded boxes in the matrix; those with an “X” indicate a dependency of the frontline system on the support system. For example, the containment flooding and drain system (CFDS) includes a

dependency on the highly reliable DC power system (EDSS) to open the CIVs to support injection. An "X^5" identifies that the dependency between systems is not required for accident mitigation because the design is fail-safe. For example, the emergency core cooling system (ECCS) is dependent on power to maintain valves closed as indicated by the relationship with the module protection system (MPS) (which provides electrical power to maintain the valves in their non-actuated state); however, the relationship is indicated by "X^5" because the fail-safe design allows the valves to move to their open position without power (because the MPS generates an engineered safety features actuation system (ESFAS) signal on a loss of power). Therefore, due to the fail-safe design of passive systems, the loss of the normal MPS function is not needed because it results in removing power to the actuators such that components reach their safety position on loss of power. The matrix illustrates that limited support is required to fulfill PRA system functions because the design uses fail-safe safety systems that function without power (or operator action) and includes passive heat transfer to the UHS.

The methodology can be summarized in the following steps:

1) Identify the initiating events to be modeled. An initiating event may represent a specific potential challenge or group of challenges that have a common plant response.

2) Identify and define the key safety functions that need to be accomplished to preserve core cooling.

3) Determine the systems and operator actions to accomplish the safety functions.

4) Determine the success criteria for the safety functions and their associated systems and operator actions.

5) Determine the accident progression for each of the initiating events by considering success and failure of the safety functions and their associated systems and functions.

6) Describe graphically the accident progression in the form of event trees.

7) Identify the appropriate sequence logic from the event trees to represent potential core damage sequences.

8) Quantify core damage sequence probabilities, accounting for dependencies, based on the linking and quantification of the fault trees for the top events.

For each accident sequence represented by an event tree and its corresponding initiating event, the final outcome for each sequence is assigned an end state based on whether the module response to the initiating event is successful in terms of preventing core damage and containment failure:

OK - For an accident sequence to be defined a success, indicated by an event tree end state of "OK," the sequence of events ensures that the module is in a safe, stable state and can be maintained in this state for the mission time. The "stable" state implies that the module is not trending towards an undesirable condition at the end of the mission time. In this end state, the core is intact and cooled for the mission time.

Level2-ET - Accident sequences that do not end with successful mitigation are assumed to result in damage to the nuclear fuel. These sequences are evaluated further in the Level 2 PRA to determine the containment response. Such sequences are annotated by the transfer "Level2-ET" as the end state of the Level 1 event tree. The Level 1 and Level 2 event trees are directly linked through this transfer (i.e., bridge trees or plant damage state binning are not used). The Level 2 event tree is used to evaluate the containment response. The Level 2 event tree includes a large release ("LR") end state along with a core damage ("CD") end state that is used to quantify core damage.

19.1.4.1.1.2 Internal Initiating Events

A systematic approach is used to develop a comprehensive list of potential internal initiating events to be considered in the internal events PRA. The approach uses multiple techniques to reflect industry experience with currently operating pressurized water reactors (PWRs), and also accounts for the unique features of the design. Initiating events are identified using industry experience, failure modes and effects analysis (FMEA), and a master logic diagram (MLD).

Industry experience is considered by review of multiple industry (generic) data sources and PRA studies from operating plants and advanced reactor designs. Key industry sources are:

- NUREG/CR-5750, "Rates of Initiating Events at US Nuclear Power Plants: 1987-1995" with updates (Reference 19.1-11)
- NUREG/CR-6890, "Reevaluation of Station Blackout Risk at Nuclear Power Plants, Analysis of Loss of Offsite Power Events: 1986-2004" with updates (Reference 19.1-16)
- EPRI NP-2230, "ATWS: A Reappraisal. Part 3. Frequency of Anticipated Transients" (Reference 19.1-17)
- NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants" with updates (Reference 19.1-23)
- NUREG-1829, "Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process" (Reference 19.1-31)
- "Advanced Light Water Reactor Utility Requirements Document" (Reference 19.1-32)

Failure modes and effects analyses are performed on NuScale systems whose failures are judged to have the potential for inducing an upset condition (i.e., initiating event), or negatively affect the module’s ability to respond to an upset condition. The FMEA is used to identify plant-specific system and support system faults, which are then grouped in a manner that allows comparison to typical initiating event characterization. For example, the "loss of main steam system" identified in the FMEA is directly analogous to the same event identified in documented industry sources for currently operating PWRs.

The third technique that is applied to identify applicable initiating events is a "top-down" approach using an MLD. For this technique, piping connected to the RPV is reviewed to identify potential occurrences (e.g., pipe breaks, valve failures, loss of flow or inadvertant flow, pump failures) that could result in an upset condition. For example, consideration of feedwater piping yields the potential faults of a feedwater transient or a feedwater line break. To facilitate quantifying the initiating event frequency, the events identified by the MLD are then grouped in a manner that allows comparison to existing documented initiating event sources. Figure 19.1-1 provides the MLD-identified events, grouped according to transients associated with RCS heat removal, core heat removal, reactivity control, RCS pressure control, and RCS inventory control. The MLD technique did not identify initiating events that had not been identified by the other methods; but, it provides confirmation of the completeness of the initiating event spectrum.

The potential initiating events that are identified by the three techniques are reviewed for applicability to the NuScale design and, if appropriate, screened from further consideration. For example, initiators associated with reactor coolant pump faults are eliminated because reactor coolant pumps are not part of the NuScale design. The applicable initiators are then categorized based on module response, success criteria, timing, potential for radionuclide release, and the effects on the operability and performance of mitigating systems and plant operators. For example, pipe breaks in the main steam system (MSS) and feedwater system (FWS) can be grouped because the module response to these events can be analyzed in a common sequence evaluation for secondary side piping break. Five initiating event (IE) "categories" are established, as shown in the first column of Table 19.1-8:

- LOCA and decrease in reactor coolant inventory events
- steam generator tube failure (SGTF)
- secondary side line break
- loss of electric power
- transients

Each category is then subdivided, if necessary, to define specific initiating events for which event trees should be developed. The subdivision is based on similarity of potential module response. For example, the “secondary side line break” category is a grouping of pipe breaks or leaks in the main steam, feedwater, and decay heat removal lines, because the module response to each of these breaks or leaks can be assessed by a common event tree. As another example, the “LOCA and Decrease in Reactor Coolant Inventory Events" category includes IEs that result in the release of reactor coolant due to pipe breaks or inadvertent valve opening, either inside or outside of the CNV; however, only pipe breaks inside containment meet the regulatory definition of LOCA. The resultant IEs and associated event tree labels are provided in the "Initiator" and “Label” columns, respectively, of Table 19.1-8. The “Description” column provides a detailed description of the initiator. The eleven initiators with associated event trees represent the spectrum of module responses to potential internal event challenges.

The frequency of the IEs is discussed in Section 19.1.4.1.1.5.

19.1.4.1.1.3 Success Criteria

Success criteria are used to distinguish "success" or "failure" in the event tree sequence logic. Per the ASME/ANS PRA Standard, the success criteria reflect "the minimum number or combinations of systems or components required to operate, or minimum levels of performance per component during a specific period of time, to ensure that the safety functions are satisfied." In the PRA, partial functioning for example, reduced flow rate, is not modeled.

The process for defining success criteria for the event tree sequences is performed by defining success in three progressive stages: overall success criterion, functional success criteria, and system success criteria. The overall success criterion is prevention of core damage. Accident sequences that are considered success or "OK" do not result in core damage for the duration of the mission time defined for the PRA, and are in a stable or improving module configuration using the following definitions:

- <u>Mission time</u> is defined as the period of time that a system or component is required to operate to perform its function after an IE. A 72-hour mission time, starting with T=0 defined as the start of the IE, is used to demonstrate that the overall success criterion (prevention of core damage) has been met, with module conditions being stable or improving.
- <u>Core damage</u> is defined as occurring when the fuel peak cladding temperature, as determined by thermal-hydraulic simulation, exceeds 2200 degrees F.

Functional success criteria are then developed based on the safety functions necessary to support the overall success criterion. The functional success criteria are the minimum set of functions whose success is needed to prevent core damage and a large release. The safety functions and method of achieving the functions are summarized as follows:

- Fuel assembly heat removal: This function refers to the transfer of core heat to the UHS after a module upset that demands a reactor trip. The function can be achieved by safety-related or nonsafety-related systems that can provide core cooling. Depending on the IE and accident sequence, core cooling can be achieved passively by actuation of the decay heat removal system (DHRS) or ECCS. In the absence of these preferred, automatic methods, operator action can establish chemical and volume control system (CVCS) makeup inventory to the RPV or flood the CNV from the CFDS. Repeated cycling of a reactor safety valve (RSV) also relieves pressure and sufficiently cools the fuel by adding water to the CNV which provides passive conductive and convective cooling from the RCS to the reactor pool.

- Reactivity control: This function refers to the limiting of core power generated by the fission reaction. The function is achieved if the core is rendered subcritical by insertion of control rods as demanded by a reactor trip signal. In an anticipated transient without scram (ATWS) event, as the fuel heats up and the moderator density decreases, core power is reduced; this negative reactivity feedback maintains fuel assembly heat removal while avoiding core damage.
- Containment integrity: This function refers to establishing and controlling the containment radionuclide barrier. It is achieved when sensors detect abnormal process conditions and the MPS generates a containment isolation signal for the containment system (CNTS) isolation valves to close. Containment isolation supports the system success criteria for avoiding core damage by:

  a) Achieving DHRS passive core cooling by closing the main steam isolation valve (MSIVs) and the feedwater isolation valves (FWIVs).

  b) Limiting the loss of primary coolant following a pipe break outside containment.

  c) Ensuring effective ECCS passive core cooling by retaining primary coolant inside the CNV, which facilitates the transfer of heat from the fuel to the reactor pool.

  d) Limiting the transfer of mass and energy from the primary side to the secondary side following an SGTF.

The system success criteria are the minimum performance requirements of a system needed to accomplish a safety function. The performance requirements are characterized by such features as the number of trains required, the necessary flow rate, and the required valve alignment. Support systems like electrical power are also considered for their role in supporting the function of frontline systems. Sometimes the system success criteria are dependent on the IE and the success or failure of the top events that precede it in a particular accident sequence. As such, success criteria may vary as a function of module status. The system success criteria are reflected in the system fault tree models and represented by a thermal-hydraulic simulation using the NRELAP5 code. Table 19.1-7 summarizes the success criteria associated with the top events of the event trees.

Table 19.1-6 provides key information for each severe accident sequence in which core damage does not occur, that is, an end state denoted by "OK." The event tree, sequence, and representative thermal-hydraulic simulation are identified in the table. Event tree top events and success criteria are listed, for example, "S" in the RSV column indicates that the minimum performance requirement for RSV success, which is one RSV cycling open and closed, has been met. Finally, the table also illustrates failures associated with each sequence, for example, "FO" indicates an RSV failing to close.

19.1.4.1.1.4 Accident Sequence Determination

Accident sequences modeled in the PRA are represented by the various "paths" through the event trees that are developed to depict the module response to each IE. The Level 1 event trees are provided as Figure 19.1-2 through Figure 19.1-12.

To define an accident sequence, event trees are constructed to model and delineate the mitigating responses to an IE. The mitigating responses provided by frontline systems are labeled as top events and are represented by the headings in the event tree. The sequential order from left to right of the top events is predominately determined by the order in which the mitigating systems are expected to actuate, either automatically, or from operators executing proceduralized responses. The mitigating functions can be successful with automatic actuation, manual actuation (i.e., operator action), or by passive performance. A node in the event tree where branching occurs indicates that a particular function (i.e., top event) is questioned for availability. Success of a function is indicated on the event tree as an up branch while a downward branch indicates a failure of the function. The delineation of the accident sequences is determined by the combination of an IE and the event tree top event successes and failures. Success or failure of a top event can be dependent on the success or failure of the top events preceding it, or in some cases may not be relevant, or the systems represented by the top events may be unavailable in the accident sequence being analyzed. Therefore, not every accident sequence path includes a branch point for each top event in the event tree, as indicated by a straight line rather than a branch point.

The right hand side of the event tree defines the end state of the sequence:

- The "End State" column categorizes the end state of the accident sequence. Each accident sequence is defined as: 1) a successful module response without core damage (OK), 2) core damage requiring evaluation of containment response, indicating a transfer to Level 2 (LEVEL2-ET), or 3) a transfer to another event tree for additional analysis of the module response (e.g., TGS-TRAN-NPC-ET).
- The "Comments" column in the event tree references the representative thermal hydraulic stimulation identification number for the sequence.

A brief summary of each event tree follows.

CVCS--ALOCA-COC: CVCS Charging (Injection) Line Pipe Break Outside Containment

The CVCS--ALOCA-COC event tree, provided in Figure 19.1-2, illustrates the accident sequence logic for an IE that involves a CVCS injection line break outside of the CNV. The distinguishing characteristic of this initiator is that CVCS makeup cannot be credited to provide RCS inventory because of the break location. The break is simulated as a double-ended guillotine break of the CVCS injection line in the Reactor Building (RXB) immediately outside the containment.

If an injection line pipe break outside containment were to occur, the expected module response is a reactor trip due to low pressurizer level or low pressurizer pressure, isolation of the break in the CVCS line and actuation of the DHRS with the result that the reactor reaches a safe, stable condition by natural recirculation through the DHRS without operator action (Sequence 1).

If CIVs close but both trains of DHRS are unavailable, then heat-up of primary coolant and pressurization of the RPV occurs to the point of RSV demand. Successful opening of one RSV relieves pressure to the point of RSV reclosure. If one RSV successfully cycles open and closed, as needed, over the 72-hour mission time then sufficient heat is removed through containment into the reactor pool by passive convection and conduction to cool the module to a safe, stable configuration (Sequence 2).

Failure of an RSV to re-close results in an open path of steam to containment which leads to a reduction in RPV water level. The RCS makeup by the CVCS is not credited because the break location is assumed to result in a flow diversion. CNV water level eventually increases to the point of reaching a demand for ECCS actuation. Due to the stuck open RSV, the pressure in the RPV would be well below the ECCS inadvertent actuation block (IAB) setpoint, permitting ECCS valve opening. Successful opening of ECCS valves leads to the OK end state (Sequence 3). Failure of ECCS to function as a recirculation path represents a continuation of inventory loss to containment through the stuck open RSV and excessive heat-up of the core resulting in eventual core damage and evaluation in the Level 2 analysis (Sequence 4).

Failure of both RSVs to open prevents the ECCS valves from opening due to the ECCS inadvertent actuation block. There is no credit for operator action to mitigate this event. Continued pressurization of the RPV would occur until there is a breach in the pressure boundary. Reactor coolant would be expelled into the CNV through the failed boundary, reducing coolant water level and resulting in eventual core damage and evaluation in the Level 2 analysis (Sequence 5).

For sequences in which isolation of the injection line break has failed, the discharge of reactor coolant would necessitate inventory addition to avoid core damage. Operator intervention to establish flow from the CFDS to the RPV would avoid core damage in combination with passive cooling through ECCS operation (Sequence 6). A failure of CFDS or ECCS would mean that there would be insufficient RPV water to facilitate passive cooling and result in core damage (Sequences 7 and 8).

The event tree consists of thirteen accident sequences. Eight sequences involve successful actuation of the reactor trip system (RTS). The remaining sequences involve failure of the RTS and depict the module response to an ATWS. The ATWS response is similar to the non-ATWS response; one exception is that DHRS is not considered because, for an ATWS, a demand for an RSV is not avoided with successful DHRS operation. Therefore, the results are the same with DHRS success or failure. Further, the CFDS is not credited to mitigate an unisolated break if the reactor fails to trip; that is, given the additional power due to the ATWS, the containment flooding and drain system does not guarantee success.

CVCS--ALOCA-LOC: CVCS Letdown (Discharge) Line Pipe Break Outside Containment

The CVCS--ALOCA-LOC event tree, provided as Figure 19.1-3, illustrates the accident sequence logic for an IE that involves a break in the CVCS piping downstream of the discharge containment isolation valve. The module response to a CVCS--ALOCA-LOC initiator is similar to that described for a CVCS--ALOCA-COC except that CVCS makeup can be credited because RCS inventory makeup is possible by establishing CVCS makeup to the RPV after reopening the appropriate CIVs.

With a CVCS discharge line pipe break occurring outside containment, the expected module response is a reactor trip due to low pressurizer level or low pressurizer pressure, isolation of the break in the CVCS line and actuation of the DHRS with the result that the reactor reaches a safe, stable condition by natural recirculation through the DHRS without operator action (Sequence 1).

The module response is similar to the response to a CVCS injection line break in terms of DHRS, reactor safety valve, ECCS, and CFDS functions. Because the break has occurred in the discharge line, flow through the CVCS injection line or the CVCS pressurizer spray line can be credited for makeup for this IE.The potential for inventory addition through the CVCS is reflected in top event CVCS-T01.

The event tree consists of eighteen accident sequences. Eleven sequences involve successful actuation of the RTS. The remaining sequences involve failure of the RTS and depict the module response to an ATWS. The ATWS response is similar to the non-ATWS response; one exception is that DHRS is not considered because an RSV is demanded irrespective of DHRS success and successful RSV operation is sufficient to maintain core cooling. Further, the CFDS is not credited to mitigate an unisolated break if the reactor fails to trip; that is, given the additional power due to the ATWS, the containment flooding and drain system does not guarantee success.

CVCS--ALOCA-CIC: CVCS Charging (Injection) Line LOCA Inside Containment

The CVCS-ALOCA-CIC event tree, provided in Figure 19.1-4, illustrates the accident sequence logic for an IE that involves a break in the CVCS injection line between the inboard containment isolation valve and the RPV. In this situation, primary coolant inventory inside the RPV discharges into the sub-atmospheric CNV through the break.

If an injection line LOCA inside containment were to occur, the expected module response is a reactor trip due to rapid pressurization of the CNV reaching the containment pressure setpoint. Reaching the containment pressure setpoint also initiates containment isolation, which is modeled in the Level 2 event tree. Discharge of reactor coolant into the CNV would continue because the flow cannot be isolated. The reduction in RPV water level would eventually result in high CNV water level, which initiates ECCS. Heat removal by natural circulation then occurs to place the module in a safe, stable condition (Sequence 1).

In the event of ECCS failure, the last top event (CVCS-T04) models potential compensatory measures carried out by operators to inject makeup water to the RPV. For CVCS-T04 success, DHRS is required and a flow path would need to be established through the pressurizer spray supply lines after diagnosing that the in-containment LOCA is due to the CVCS injection line break. The operator action requires re-opening CIVs, aligning a flowpath from the demineralized water system (DWS), activating a makeup pump, and switching over to the pressurizer spray lines (Sequence 2). An unsuccessful CVCS injection leads to core uncovery and evaluation in the Level 2 analysis (Sequence 3). Without DHRS heat removal, makeup coolant would be insufficient to prevent core uncovery and damage (Sequence 4).

The event tree consists of eight accident sequences. Four sequences involve successful actuation of the RTS. The remaining sequences involve failure of the RTS and depict the module response to an ATWS. The ATWS response is identical to the non-ATWS response.

RCS---ALOCA-IC: LOCA Inside Containment

The RCS---ALOCA-IC event tree, provided as Figure 19.1-5, illustrates the accident sequence logic for an IE that involves an RPV steam or water line break, spurious opening of an RSV, or LOCA resulting from a failure in a pressurizer heater penetration. These events result in RCS inventory loss that cannot be isolated and RCS fluid is retained inside the CNV.

The accident progression and expected module response is similar to initiating event CVCS-ALOCA-CIC. The last top event (CVCS-T01) models potential operator action to inject makeup water to the RPV from the CVCS injection line following ECCS failure. This operator action requires re-opening CIVs, aligning a flowpath from the DWS and activating a makeup pump.

The event tree consists of six accident sequences. The module response to an ATWS is identical to the non-ATWS response.

ECCS--ALOCA-RV1: Spurious Opening of an ECCS Valve

The ECCS--ALOCA-RV1 event tree, provided as Figure 19.1-6, illustrates the accident sequence logic for an IE that involves the spurious opening of an ECCS reactor recirculation valve (RRV) or reactor vent valve (RVV). Opening of either an RRV or RVV results in discharge of RCS fluid into the CNV. This event has been included in the loss of RCS inventory category that has been given the shortcut name of “LOCA” even though the spurious opening of an ECCS valve is not by definition a LOCA. The event tree is developed separately from the other inside containment loss of RCS inventory initiators because of the impact on the operation of the ECCS. That is, if the initiator is an open RVV, ECCS mitigating system failures are limited to other failures, not including the RVV.

The event tree has a logic structure similar to the CVCS--ALOCA-CIC event. There are six accident sequences and the module response to an ATWS is identical to the non-ATWS response.

MSS---ALOCA-SG: Steam Generator Tube Failure

The MSS---ALOCA-SG event tree, provided as Figure 19.1-7, illustrates accident sequence logic for an IE that involves an SGTF. For an SGTF, the general accident scenario description is that a single tube fails; in such an event, higher pressure on the outside of the tube forces primary coolant into the failed tube and coolant inventory is potentially lost outside of the containment through the main steam line. In contrast to currently operating plants, the steam generator tubes are in compression (i.e., secondary coolant is on the inside of the tubes and primary coolant is on the outside); thus, multiple tube failures are not judged to be a credible IE.

The expected response to an SGTF is a reactor trip on low pressurizer level or low pressurizer pressure, followed by a containment isolation signal due to low-low pressurizer level. Containment isolation, among other protective actions, would close the MSIVs and the FWIVs on both steam generators. The low-low pressurizer level actuates containment isolation and subsequent high main steam pressure actuates DHRS. With the reactor tripped, the affected steam generator (indicated as #2 in the event tree) isolated, and a single train of DHRS in service on the intact steam generator, the module reaches a safe and stable configuration (Sequence 1).

Failure of the DHRS train on the intact steam generator would result in heat-up of primary coolant and pressurization of the RPV to the point of RSV demand. Successful opening of one RSV would relieve pressure to the point of RSV reclosure. If one RSV successfully cycles open and closed, as needed, over 72-hour mission time, sufficient heat is removed through containment into the reactor pool by natural circulation to cool the module to a safe, stable configuration. The ECCS is not demanded in this situation (Sequence 2).

Failure of an RSV to re-close results in an open path of steam to containment, which leads to a reduction in RPV water level. The ECCS would be demanded on high CNV level. The differential pressure between the RPV and the CNV would be low enough to nullify the ECCS IAB. Successful ECCS actuation provides sufficient natural recirculation cooling to cool the module to a safe, stable configuration (Sequence 3).

Failure of the ECCS valves to open as designed could be compensated by operator action to inject makeup water to the RPV from the CVCS, as illustrated by Sequence 4. This operator action requires re-opening CIVs, aligning a flow path from the DWS and activating a makeup pump. Sequence 5 represents unsuccessful injection of makeup water to the RPV.

Given DHRS failure, if both RSVs fail to open, the RPV remains at high pressure and opening of the ECCS valves is prevented due to the IAB. The reactor pressure continues to increase and core damage ensues (Sequence 6).

If the SGTF were not isolated, as illustrated by Sequences 7 through 11, there is a loss of coolant path and the need for makeup water. Makeup water can be provided by the operator realigning and initiating the CVCS for injection. Success requires at least one of two CVCS pumps to inject makeup inventory through the injection line (Sequences 7 and 10). If CVCS failure were to occur, an alternate method of inventory addition could be implemented using the CFDS and ECCS, as indicated by Sequence 8. Success of the CFDS requires the operator to align and start at least one of two available containment fill pumps and open two isolation valves. Failure of CFDS or failure of ECCS results in core damage (Sequences 9 and 11).

The event tree consists of eighteen accident sequences. Eleven sequences involve successful actuation of the RTS. The remaining sequences involve failure of the RTS and depict the module response to an ATWS. The ATWS response is similar to the non-ATWS response; one exception is that DHRS is not considered because an RSV is demanded irrespective of DHRS success. Further, the CFDS is not credited to mitigate an unisolated break if the reactor fails to trip; that is, given the additional power due to the ATWS, the containment flooding and drain system does not guarantee success.

<u>TGS---FMSLB-UD: Secondary Side Line Break</u>

The event tree TGS---FMSLB-UD--ET, provided as Figure 19.1-8, illustrates the accident sequence logic for an IE that involves a pipe break in feedwater, main steam, or decay heat removal systems.

The expected module response to this initiator depends on the location of the secondary line break, with the initial module response being a reactor trip. For breaks occurring inside containment, a reactor trip signal is expected on high containment pressure. For main steam line or DHRS steam line breaks outside containment, a reactor trip signal is expected on low steam pressure or high reactor power. For feedwater line or DHRS condensate line breaks outside of containment, a reactor trip signal is expected on high pressurizer pressure.

Following the reactor trip, successful DHRS operation (without an RSV demand) would remove decay heat to the reactor pool by natural circulation to cool the module to a safe, stable configuration (Sequence 1). If an RSV is demanded to open following success of DHRS, successful cycling of the RSV leads to a safe, stable configuration (Sequence 2). If an RSV sticks open, ECCS can provide heat removal (Sequence 3). If ECCS does not initiate, the operator can add inventory with CVCS (Sequence 4). If the operator is unsuccessful, the core continues to heat up without the removal of decay heat leading to core damage and evaluation in the Level 2 analysis (Sequence 5).

If both trains of DHRS are unavailable, then heat-up of primary coolant and pressurization of the RPV occurs to the point of RSV demand. Successful opening of one RSV relieves pressure to the point of RSV reclosure. If one RSV successfully cycles open and closed, as needed, over the 72-hour mission time then sufficient heat is removed through containment into the reactor pool by natural circulation to cool the module to a safe, stable configuration (Sequence 6).

Failure of an RSV to re-close results in an open path of steam to containment that leads to an eventual reduction in RPV water level. The ECCS is demanded on high CNV water level. The differential pressure between the RPV and the CNV would be low enough to release the ECCS inadvertent actuation block. Successful ECCS provides sufficient natural recirculation cooling to cool the module to a safe, stable configuration (Sequence 7).

Failure of the ECCS valves to open as designed could be compensated by operator action to inject makeup water to the RPV from the CVCS. This action includes the need to align the flow path from DWS to the RPV and activate a CVCS makeup pump. (Sequence 8). Unsuccessful operator action leads to core damage (Sequence 9).

Given DHRS failure, if both RSVs fail to open, the RPV remains at high pressure and opening of the ECCS valves is prevented due to the IAB. The RPV pressure continues to increase and core damage ensues (Sequence 10).

The event tree consists of 15 accident sequences. Ten sequences involve successful actuation of the RTS. The remaining sequences involve failure of the RTS and depict the module response to an ATWS. The ATWS response is identical to the non-ATWS response except that DHRS is not considered because RSVs are demanded irrespective of DHRS success.

<u>EHVS--LOOP: Loss of Offsite Power</u>

The EHVS--LOOP event tree, provided as Figure 19.1-9, illustrates the accident sequence logic for an initiating event that involves the loss of offsite power (LOOP). The LOOP event occurs when the connection to the transmission grid is lost; without island mode, the 13.8 kV and switchyard system (EHVS), the medium voltage AC electrical distribution system (EMVS), and the low-voltage AC electrical distribution system (ELVS) alternating current (AC) buses would eventually deenergize due to the loss of load on and power from the turbine generator system (TGS). The PRA analysis does not model operations using the island mode capability described in Section 8.3. Any NPM operating in island mode would be a source of normal AC power. A LOOP, as used in the PRA analysis, would, without island mode, result in a loss of normal AC power.

The expected module response to a LOOP is startup of the auxiliary AC power source (AAPS) or a backup diesel generator (BDG). For the PRA model, the AAPS is assumed to be a combustion turbine generator (CTG). Use of a CTG or BDG is illustrated by Figure 19.1-9 Sequences 1 and 2, respectively. Starting and loading either the CTG or a BDG requires operator action. If either of these AC power sources is restored, the event appears as a transient; thus, the sequences transfer to the TGS-TRAN-NPC event tree provided as Figure 19.1-11.

Sequences 3 through 16 evaluate the module response without either the offsite or onsite AC sources, that is, a "loss of all AC." Section 8.4 discusses the design capability with respect to "Station Blackout" as defined by 10 CFR 50.63. In an event with a loss of all AC, the expected module response is a reactor trip and actuation of the DHRS. One train of DHRS constitutes success, with the result that the reactor reaches a safe condition by natural recirculation through the DHRS without operator action. If AC power is restored within 24 hours, the module reaches a long term safe and stable configuration without an ECCS demand, as indicated by Sequence 3. If AC power is not restored within 24 hours, ECCS automatically opens to the fail-safe condition and the module is in a safe configuration (Sequence 4). An incomplete ECCS actuation leads to core damage (Sequence 5).

If an RSV opens and cycles to control RPV pressure, Sequences 6, 7, and 8 mirror sequences 3, 4, and 5. Failure of an RSV to re-close results in an open path of steam to containment which leads to a reduction in RPV water level. CNV water level eventually increases to the point of triggering a demand for ECCS actuation. Successful ECCS actuation leads to the OK end state (Sequence 9). Failure of ECCS to function as a recirculation path represents a continuation of inventory loss from the RCS through the stuck open RSV, excessive heat-up of the core and eventual core damage as indicated by Sequence 10. With the loss of power, makeup inventory from the CVCS or CFDS is not available.

If both trains of DHRS fail, heat-up of the primary coolant and pressurization of the RPV continues to the point of RSV demand. Successful opening and cycling of one RSV relieves pressure and allows module cooling through the containment; if power is restored within 24 hours, the core is cooled without a demand for ECCS valve operation (Sequence 11). If power is not restored within 24 hours, ECCS valves automatically open to their fail-safe condition (Sequence 12). Unsuccessful ECCS valve opening leads to core damage (Sequence 13). If an RSV is stuck open, Sequences 14 and 15 represent successful and unsuccessful ECCS actuation, respectively.

Given DHRS failure, if both RSVs had failed to open when demanded to relieve reactor pressure, the ECCS inadvertent actuation block would prohibit the ECCS valves from opening. With AC power unavailable, the CVCS is precluded from operating and acting as a heat sink. Failure to remove decay heat results in the RPV pressurizing until there is a breach in the pressure boundary. Reactor coolant would be expelled into the CNV through the failed boundary, reducing coolant water level and resulting in core damage as indicated by Sequence 16.

The event tree consists of 22 accident sequences. The first two sequences result in transfers to the general reactor trip event tree in Figure 19.1-11 reflecting that AC power is available from an onsite source. For scenarios where AC power is not available, fourteen sequences involve successful actuation of the RTS. The remaining sequences involve failure of the RTS and depict the module response to an ATWS. The ATWS response is identical to the non-ATWS response except that DHRS is not considered because RSVs are demanded irrespective of DHRS success.

EDSS--LODC-----ET: Loss of Direct Current (DC) Power

The EDSS--LODC event tree, provided as Figure 19.1-10, illustrates the accident sequence logic for an initiating event that involves the loss of DC power. The loss of DC power initiating event involves the coincident de-energization of at least two EDSS buses up to all four EDSS buses. At least two of the four EDSS buses are required to fail simultaneously in order for the reactor trip signal and engineered safety features to be actuated. If all four EDSS buses de-energize concurrently then indication and control from the main control room (MCR) would be lost and no operator intervention is credited. This is modeled using a conditional basic event in the fault tree logic for top event CVCS-T05 that accounts for the fraction of the initiating event frequency represented by a common cause failure (CCF) of four EDSS buses.

The expected module response to the loss of AC voltage to two or more EDSS buses would be a reactor trip signal, containment isolation signal and ECCS actuation signal, due to the MPS two-out-of-four voting trip determination logic. The engineered safety features signal would actuate the DHRS as well as close the CIVs, MSIVs, and the FWIVs. The DHRS would suffice as a heat sink until this configuration is interrupted by the opening of the ECCS valves. The IAB feature would prevent opening the ECCS valves until the differential pressure between the RPV and CNV reduces below the setpoint. Successful ECCS valve opening provides sufficient natural recirculation cooling to cool the module to a safe, stable configuration (Sequence 1).

An incomplete ECCS actuation could be compensated by operator intervention to inject makeup water to the RPV from the CVCS (CVCS-T05). However, this operator action can be accomplished only if there is MCR panel indication necessitating control power through at least one online EDSS bus (Sequence 2). Failure of this action, or the inability to take action due to a complete loss of DC power, results in core damage as illustrated by Sequence 3.

If both trains of DHRS fail, heat-up of the primary coolant and pressurization of the RPV continues to the point of RSV demand. Successful opening of one RSV relieves pressure to the point of RSV reclosure. If one RSV successfully cycles open and closed, sufficient heat is removed through containment into the reactor pool by natural circulation to cool the module. This cooling method is interrupted by ECCS valve opening when the RPV pressure is reduced below the IAB setpoint. Successful opening of ECCS valves results in a safe configuration as indicated by Sequence 4. Incomplete ECCS valve opening can be compensated by operator intervention to inject water with the CVCS (Sequence 5). Failure of both ECCS and CVCS makeup results in core damage (Sequence 6).

Given DHRS failure, if both RSVs had failed to open when demanded to relieve reactor pressure, the ECCS inadvertent actuation block would prohibit the ECCS valves from opening. Failure to remove decay heat results in the RPV pressurizing until there is a breach in the pressure boundary. Reactor coolant would be expelled into the CNV through the failed boundary, reducing coolant water level and resulting in core damage (Sequence 7).

The event tree consists of 10 total accident sequences. Seven sequences involve successful actuation of the RTS. The remaining sequences involve failure of the RTS and depict the module response to an ATWS. The expected module response is heat transfer to the reactor pool by a cycling RSV. Three end states are modeled for ATWS. Sequence 8 represents the successful operation of ECCS when the IAB setpoint is reached. Sequences 9 and 10 lead to core damage from an unsuccessful ECCS valve opening or core damage due to RPV overpressurization, respectively.

TGS---TRAN--NPC: General Reactor Trip

The TGS---TRAN-NPC event tree, provided as Figure 19.1-11, illustrates the accident sequence logic for an initiating event that involves a general reactor trip. Transients include events such as a loss of feedwater flow, loss of main condenser vacuum, loss of cooling water systems, and a manual trip. The key characteristic of a general reactor trip is the availability of PRA-modeled support systems such as AC power and instrument air.

The general reactor trip would cause an imbalance between the heat generated by the fuel and that being rejected through the turbine generator and main condenser. The expected module response to this imbalance would be an increase in pressurizer pressure resulting in a reactor trip signal and DHRS actuation, without RSV demand, to place the module in a safe configuration, as indicated by Sequence 1. If only a single train of DHRS is functioning and is demanded on high pressurizer pressure, it may not remove heat quickly enough to prevent RPV pressure from reaching the RSV setpoint, thus, successful RSV functioning may be needed to place the module in a safe configuration as indicated by Sequence 2. Failure of an RSV to reclose would lead to ECCS actuation (Sequence 3), or if ECCS fails to function, inventory addition from the CVCS is required to place the module in a safe configuration as indicated by Sequence 4. Failure to add inventory from the CVCS results in core damage (Sequence 5).

If both trains of DHRS fail, heat-up of the primary coolant and pressurization of the RPV continues to the point of RSV demand. If one RSV successfully cycles open and closed, as needed, over the mission time, sufficient heat is removed through containment into the reactor pool by natural circulation to cool the module to a safe, stable configuration as indicated by Sequence 6.

Failure of an RSV to re-close results in an open path of steam to containment which leads to a reduction in RPV water level. The CNV water level eventually increases to the point of triggering a demand for ECCS actuation to prevent core damage (Sequence 7). Due to the stuck open RSV, the pressure in the RPV would be well below the ECCS inadvertent actuation block setpoint. Failure of ECCS actuation, leads to Sequences 8 and 9, which mirror Sequences 4 and 5.

If both RSVs had failed to open when demanded to relieve reactor pressure, the ECCS inadvertent actuation block would prohibit the ECCS valves from opening. For this event, operator action could be taken, as modeled by top event CFDS-T01, to flood the CNV and avoid pressurization of the RPV to the point of breach (Sequence 10). Sequence 11 represents the failure to flood the CNV with CFDS leading to RPV overpressurization.

The event tree consists of 22 accident sequences. Eleven sequences involve successful actuation of the RTS. The remaining sequences involve failure of the RTS and depict the module response to an ATWS. The ATWS response is identical to the non-ATWS response except that RPV pressure reaches the RSV setpoint and thus, RSV opening is demanded. In addition, normal operation of the CVCS pressurizer spray and CVCS discharge is capable of preventing RPV over-pressurization following an ATWS event with success of one train of DHRS and failure-to-open of both RSVs.

<u>TGS---TRAN---NSS: Loss of Support Systems</u>

The TGS---TRAN---NSS event tree, provided as Figure 19.1-12, illustrates the accident sequence logic for an IE that involves loss of support systems causing unavailability of CVCS or CFDS for inventory addition. The loss of a support system IE includes events such as the loss of instrument air or multiple AC power buses (i.e., EHVS, EMVS, ELVS) that result in a reactor trip.

A reactor trip is expected on a low AC voltage or high steam pressure due to closure of the MSS secondary isolation valves. The expected module response is a reactor trip with DHRS operation removing decay heat. If the RPV pressure does not increase to the point of RSV demand and the module reaches a safe, stable configuration (Sequence 1). If only a single train of DHRS is functioning and is demanded on high pressurizer pressure, it may not remove heat quickly enough to prevent RPV pressure from reaching the RSV setpoint, thus, successful RSV functioning would be needed to place the module in a safe configuration as indicated by Sequence 2. Failure of an RSV to reclose would lead to an ECCS demand; if ECCS is successful, core damage is prevented (Sequence 3). If ECCS fails to function, core damage occurs as indicated by Sequence 4 because CVCS is assumed not to be available due to loss of a support system.

If both trains of DHRS fail, heat-up of the primary coolant and pressurization of the RPV continues to the point of RSV demand. If one RSV successfully cycles open and closed, as needed, over the mission time, sufficient heat is removed through containment into the reactor pool by natural circulation to cool the module to a safe, stable configuration as indicated by Sequence 5.

Failure of an RSV to re-close results in an open path of steam to containment which leads to a reduction in RPV water level. The CNV water level eventually increases to the point of triggering a demand for ECCS actuation to prevent core damage (Sequence 6). Due to the stuck open RSV, the pressure in the RPV would be well below the ECCS inadvertent actuation block setpoint. Unsuccessful actuation of ECCS leads to core damage (Sequence 7).

Given DHRS failure, if both RSVs had failed to open when demanded to relieve reactor pressure, the ECCS inadvertent actuation block would prohibit the ECCS valves from opening. For this event, containment flooding is not credited due to the loss of support systems and core damage is assumed to occur as a result of the RPV overpressurization, as indicated by Sequence 8.

The event tree consists of 12 accident sequences. Eight sequences involve successful actuation of the RTS. The remaining sequences involve failure of the RTS and depict the module response to an ATWS. The ATWS response is identical to the non-ATWS response except that DHRS is not considered because RSVs are demanded irrespective of DHRS success.

19.1.4.1.1.5 Data Sources and Analysis

This section provides the sources of numerical data used in the Level 1 PRA. Initiating event frequencies, component failure rates, equipment unavailabilities, human error probabilities, and common-cause failure parameters are discussed.

Initiating Event Frequencies

Each of the IE categories in Table 19.1-8 is represented by one or more initiating events that are used in the PRA. Each initiating event represents a grouping of potential module events that require a reactor trip or controlled shutdown and is associated with a common module response. Initiating event frequencies are typically developed using Bayesian estimation methods. This statistical inference methodology employs generic industry "prior" data and plant-specific data to produce a posterior distribution of event frequency using Bayes' Theorem. NuScale does not have operating experience to draw from. As such, most initiating event frequencies are estimated based solely on the generic prior of a parameter's value. Failure rate data collected by the NRC through Licensee Event Reports (LERs) from the U.S. nuclear industry serve as the basis of prior information. Studies of NuScale-specific advanced system design features (e.g., helical-coil steam generator tubes) were performed to support the development of initiating event frequencies. Initiating event frequencies are provided in terms of occurrences per module critical year (mcyr); the analysis assumes a module availability of 100 percent. Table 19.1-8 provides the mean frequency and error factors for each initiator. The following summarizes the method for assessing frequencies for each initiator.

As indicated in Table 19.1-8, the “Loss-of-Coolant Accident” category includes primary coolant leakage from piping and components as well as inadvertent valve openings in the reactor coolant pressure boundary. Different initiating events are defined based on the location of the break, or on the type of valve that opens, and on the mitigation capability following the occurrence. Unlike typical currently operating plants, it is unnecessary to define LOCAs by size because the makeup capability is sufficient for all break sizes and inadvertent valve opening, that is, the passive ECCS functions in the same manner to mitigate all break sizes and inadvertent (single) valve opening inside containment.

- IE-CVCS--ALOCA-COC: This initiator consists of either an RCS injection line break or a pressurizer spray supply line break outside of containment. The calculation of the IE frequency is based on generic prior data using the mean pipe failure rates for "external leak large" and "external leak small" of non-emergency service water piping found in NUREG/CR-6928. The failure rates in NUREG/CR-6928 are given in terms of occurrences (i.e., leaks) per foot per hour. This is converted to occurrences per module critical year by multiplication with approximate line lengths and the number of hours in a year. The prior distributions are combined by summation and this result is fitted to a lognormal distribution.
- IE-CVCS--ALOCA-LOC: This initiator consists of RCS discharge line breaks outside of containment. The calculation of the IE frequency is based on generic prior data using the mean pipe failure rates for "external leak large" and "external leak small" of non-emergency service water piping found in NUREG/CR-6928. The failure rates in NUREG/CR-6928 are given in terms of occurrences (i.e., leaks) per foot per hour. This is converted to occurrences per module critical year by multiplication with approximate line lengths and the number of hours in a year. The prior distributions are combined by summation and this result is fitted to a lognormal distribution.
- IE-CVCS--ALOCA-CIC: This initiator consists of an RCS injection line break inside containment. The calculation of the IE frequency is based on generic prior data using mean pipe failure rates for "external leak large" and "external leak small" of non-emergency service water piping, found in NUREG/CR-6928. The failure rates in NUREG/CR-6928 are given in terms of occurrences (i.e., leaks) per foot per hour. This is converted to occurrences per module critical year by multiplication with approximate line lengths and the number of hours in a year. The prior distributions are combined by summation and this result is fitted to a lognormal distribution.
- IE-RCS---ALOCA-IC: This initiator consists of either a break in the RCS discharge line inside containment, a break in the pressurizer spray supply line inside containment, a break in the RPV high point degasification line, a spurious operation of an RSV, or a resultant LOCA from the pressurizer heaters failing to trip, post-transient, causing a pressurizer heater penetration failure. (An RCS injection line break inside containment is covered by the IE-CVCS--ALOCA-CIC initiator). The calculation of the IE frequency is based on generic prior data using mean pipe failure rates for "external leak large" and "external leak small" of non-emergency service water piping found in NUREG/CR-6928. The failure rates in NUREG/CR-6928

are given in terms of occurrences (i.e., leaks) per foot per hour. This is converted to occurrences per module critical year by multiplication with approximate line lengths and the number of hours in a year. The failure rate for the spurious operation of a safety relief valve or code safety of the RCS is found in NUREG/CR-6928. There are two reactor safety valves on the RPV. The failure rate for the induced LOCA resulting from the pressurizer heaters failing to trip is calculated based on the general transient IE frequency, using a developed fault tree. The prior distributions are combined by summation and this result is fitted to a lognormal distribution.

- IE-ECCS--ALOCA-RV1: This initiator represents an inadvertent opening of any one of the five ECCS valves while the module is at critical operation. The IE frequency is quantified using a fault tree model that analyzes the failure mechanisms that could result in a spurious opening of an ECCS valve.

As indicated in Table 19.1-8, the SGTF is given a separate category because of its characteristic of coincidentally breaching the reactor coolant pressure boundary and challenging the secondary side heat sink.

- IE-MSS---ALOCA-SG: This initiator is an SGTF. The operating environment of the NuScale design for the steam generators is opposite that of most existing PWRs. In the NuScale design, secondary coolant flows through the steam generator tubes. Therefore, the higher pressure is external to the tubes and the force exerted is a compression on the tubes rather than internal tension burst pressure on the tube walls such as for typical PWRs. In addition to this operational environment difference, the NuScale design is helical as opposed to the U-shaped or once-through tube design of PWR steam generators. Fretting and other wear characteristics are expected to be different in the NuScale design. Design differences were taken into consideration in an independent study commissioned by NuScale investigating the NuScale helical coil. The IE frequency is based on that study, which employs a probabilistic physics of failure method to account for those degradation mechanisms that are relevant to the NuScale design.

As indicated in Table 19.1-8, the “Secondary Side Line Break” category considers pipe breaks and significant leaks in the main steam, feedwater, and decay heat removal lines, as well as spurious operation of the main steam safety valves inside and outside containment.

- IE-TGS---FMSLB-UD: This initiator consists of the ways in which a pipe leak can occur in the main steam, feedwater, or DHRS lines. An independent study, commissioned by NuScale, was performed to estimate the frequency for a secondary side line break given NuScale-specific system design. Degradation mechanisms were evaluated to obtain design-centric data sets by screening out the mechanisms not applicable to the design. Field experience data and failure rate information form the basis of estimating conditional rupture probabilities given size, component type, and degradation mechanism. The likelihood of a pipe flaw propagating to a significant structural failure is expressed by the conditional failure probability. The frequency of pipe breaks is then summed for the conditional rupture probabilities and corresponding component types.

As indicated in Table 19.1-8, the “Loss of Electric Power” category consists of a LOOP and a loss of DC power. The LOOP initiating event depicts a loss of AC power to plant transformers. The category includes plant-centered, switchyard-centered, grid-centered, and weather-related LOOP events. The loss of two or more DC buses has been included as a unique initiator, "Loss of DC Power," for this category.

- IE-EHVS--LOOP---: This initiator represents a loss of AC power to the station. The calculation of the IE frequency is based on generic prior data using the entire data set from 1997 through 2014 reported in INL/EXT-16-37873 (Reference 19.1-24). The generic prior data consist of NRC data records that account for LOOP contributions: switchyard, weather-related, grid, and plant-centered events during power operation. The operating experience from the four categories is retained in the LOOP frequency estimation because the full prior dataset is considered appropriate for a plant that does not yet have a selected site in the United States. The data are assumed to fit a lognormal distribution.
- IE-EDSS--LODC---: This initiator represents a de-energization of at least two highly reliable DC buses. A loss of two of four buses initiates a signal for reactor shutdown and containment isolation. The IE has been quantified by reviewing past U.S. nuclear power plant operating experience for occurrences of DC bus failure. This review yielded two occurrences in over 5000 years of bus operating years. A failure rate of two or more buses deenergizing due to a common cause was calculated using generic alpha factors.

As indicated in Table 19.1-8, the “Transients” category includes internal initiating events that are not included in the other categories. Such events result in a reactor shutdown, and may or may not have support systems available. Transients that result in automatic trip or immediate operator action to trip the reactor are included.

- IE-TGS---TRAN-NPC: This initiator represents plant transients that necessitate a shutdown of the reactor and that have not already been covered by other IEs. The calculation of the IE frequency is based on prior experience of PWRs in the United States from 1988 to 2013. The source of prior data is a collection of event types taken from the 2013 update of Reference 19.1-11. The event types postulated to contribute to a loss of component cooling water, loss of feedwater, loss of condenser heat sink, and general transients at PWRs are included. The data are assumed to fit a lognormal distribution.
- IE-TGS---TRAN-NSS: This initiator represents the loss of support systems such as a partial loss of AC power and loss of instrument air thereby leading to the unavailability of the CVCS and the CFDS to provide inventory. The calculation of the IE frequency is based on prior data of event types taken in the United States from 1988 to 2013. The event types postulated to contribute to a loss of support system events are a partial loss of AC power

and a loss of instrument air. The data are assumed to fit a lognormal distribution.

Component Failure Rates and Equipment Unavailability

Most basic events in the NuScale PRA are based on generic failure probabilities. A few basic events use modified generic values and a smaller number are based on analyses that are developed to reflect a unique design feature. The components modeled in the PRA range from relatively small items such as breakers, to larger equipment such as pumps. These components can fail due to random causes, related or CCF, or unavailability due to testing and maintenance activities.

The general approach to quantifying component unreliability is summarized as:

1) Specify component boundaries: The boundary for modeled components are set to match the component boundaries associated with the generic data of NUREG/CR-6928.

2) Compare the NuScale plant-specific design with the industry generic data for consistency.

3) If the industry generic data are not appropriate for the NuScale design, then generic data are modified to better represent the design, or special analyses are performed to characterize the component failure probabilities.

Following the guidance in NUREG/CR-6928, beta and gamma distributions were used to model uncertainties in the basic event parameters. Beta distributions were used for demand failure probabilities such as fail to start, fail to open or close. Gamma distributions were used for time-based events such as fail to run, fail to remain open, spurious operation.

Table 19.1-9 identifies failure rates that were developed by modifying generic data to better represent the NuScale design. The table indicates the source of the underlying generic data as well as a summary of the use of the modified data in the PRA.

Table 19.1-10 identifies failure rates for basic events that do not have generic data directly applicable to the NuScale design. These basis events may include component level, system level, and phenomenology dependent events. The table indicates the mean failure rate and associated error factors.

Thermal-Hydraulic Uncertainty

Because NuScale passive safety systems rely on natural circulation of reactor coolant rather than forced flow, the relatively low driving forces introduce thermal-hydraulic uncertainty that is considered in the system reliability assessment in addition to the component failure rates. Unlike component failure rate modeling, which is based in large part on operating experience, there is little directly applicable data for thermal-hydraulic uncertainty. Thus, thermal-hydraulic uncertainty was evaluated based upon methods outlined in EPRI 1016747 (Reference 19.1-12) and IAEA TECHDOC-1752 (Reference 19.1-13). The thermal-hydraulic uncertainty is characterized by a passive safety system reliability evaluation in which the thermal-hydraulic failure probability of the system is calculated. This is incorporated into the applicable fault trees as an additional contributor to the system failure probability.

Because of the lack of applicable data, thermal-hydraulic uncertainty was evaluated for the DHRS and ECCS, which rely on natural circulation flow to achieve their functions. To estimate the reliability of the passive safety systems with respect to thermal-hydraulic functionality, failure metrics were defined. For the ECCS, peak clad temperature exceeding 2200 degrees F is used as the metric; for the DHRS, the metric of exceeding RPV failure pressure with no other systems available is used. The framework of the evaluation then is depicted by the failure probability

$$P(L>C)$$

where P is the probability that the load, L, exceeds the capacity, C. The load distribution is the figure of merit after incorporating the uncertainties in the thermal-hydraulic parameter values. The system capacity is the failure metric.

The approach to including thermal-hydraulic uncertainty in the PRA model is that uncertainties in the phenomena that may affect the performance of passive safety systems are evaluated with a thermal-hydraulics code to assess system success or failure. The approach is summarized as:

1) Determine the severe accident sequences to be evaluated. The evaluated sequences are those that rely on passive safety system function for success and that occur with a frequency of at least one percent of the CDF. The remaining sequences are grouped according to similarity in thermal-hydraulic phenomena. The groupings are steam LOCA inside containment, liquid LOCA inside containment, pipe break outside containment, and other general transients that do not include a loss of primary coolant. A representative sequence from each grouping is selected for evaluation.

2) Determine the thermal-hydraulic phenomena that are significant to passive safety system reliability. The selection of phenomena to consider for further evaluation begins with expert judgment, where experience with the effect and uncertainty of each phenomenon is used to create an initial list of phenomena for consideration. The phenomena identified as impacting passive reliability are given in Table 19.1-11 for the ECCS and Table 19.1-12 for the DHRS.

3) Compute values for passive safety system reliability based on the applicable phenomena. The passive safety system reliability values were derived using a response surface methodology. Using this method, input parameters to the thermal-hydraulics code are uniformly distributed to

characterize the system response. The inputs are then resampled with the intended distributions into the previously calculated system response for comparison with the failure metric.

Table 19.1-10 provides the calculated probabilities for failures of passive heat transfer.

Human Error Probabilities

An HRA is performed to identify potential human failure events (HFEs) and to systematically estimate the probability of those events using bounding methods in the absence of as-operated facility information. The methods that have been used in other nuclear power plant PRAs, as found by surveying the literature, and the methods applied in the NuScale PRA produce comparable HFE values. Both "pre-initiator" and "post-initiator" human actions are considered in the HRA. The HRA primarily applied the approach provided in NUREG/CR-4772 (Reference 19.1-41) to estimate pre-initiator operator actions using the Accident Sequence Evaluation Program Human Reliability Analysis Procedure (ASEP) methodology and primarily NUREG/CR-6883 (Reference 19.1-22) to estimate the post-initiator operator actions using the SPAR-H Human Reliability Analysis methodology.

Pre-initiator or "latent" errors, also referred to as "Type A" HFEs, can occur as a result of maintenance, testing, or calibration activities (before an initiating event) resulting in unavailability of the associated equipment when demanded. During maintenance, testing or calibration, equipment may be disabled or placed in an abnormal alignment that may render the function of that equipment unavailable. Human errors can occur when restoring or realigning the equipment into the normal configuration. A failure during these activities that results in equipment not being restored or aligned to normal is considered a pre-initiator human error. Consistent with the ASEP methodology, the following summarizes the process used to evaluate pre-initiator HFEs:

- Identify activities and practices that may adversely impact the availability of mitigating systems if performed incorrectly.
- Screen out those activities for which sufficient compensating factors can be identified that would limit the likelihood or consequences of errors in those activities.
- Model specific HFEs for each activity that cannot be screened out and incorporate them into the PRA model.
- Evaluate the human error probability (HEP) of the event including consideration of dependencies.

Critical operator actions are considered in the pre-initiator analysis. These include (1) failure to restore a component or system following maintenance, (2) failure of a component or system because of miscalibration errors, (3) failure to restore a component or system following testing of that component or system, or (4) other miscellaneous plant-specific actions. A system or component that is governed by Technical Specification requirements and part of the initiating event analysis, is examined for potential pre-initiator errors. Table 19.1-13 identifies the pre-initiator human actions that require detailed modeling. These actions affect the module condition before a potential initiating event, and thus, are applicable to all initiators. The table also provides the HEP and associated error factor for each action.

The human error probabilities are evaluated using the basic HEP of 0.03 provided in Reference 19.1-41, adjusted for human factors conditions, potential recovery factors, and dependence. The HEP assigned in the evaluation could be increased for unusually poor human factors such as inadequate procedures; however, such factors were not identified. Potential recovery factors such as a post-maintenance testing were evaluated, if appropriate, which decreased the assigned HEP. Considering that Type A HFEs occur prior to the initiator, they are not dependent on the accident scenario. Further, maintenance actions are assumed to not be performed on multiple trains concurrently. Therefore, no dependency applies to pre-initiator HFEs.

Post-initiator actions, also referred to as "Type C" HFEs, are those actions performed by an operator after an abnormal event has started. The actions are divided into diagnosis tasks and action tasks, both of which are needed to maintain or ensure reactor protection once an abnormal event has occurred. Diagnosis refers to the determination of the correct course of action within the time available to permit performing the required post-diagnosis actions. Action tasks include manually initiating a system, aligning and actuating a system for injection, recovering a failed system, and other activities performed while following plant procedures. The HEPs are considered in terms of "diagnosis" and "action" and modified as appropriate to consider performance shaping factors and dependence among tasks. Consistent with the SPAR-H methodology, the following summarizes the process used to evaluate post-initiator HFEs:

- identify activities and actions that could be performed by the operator after an off-normal event has started
- screen out actions that would not affect core damage development if operator failure occurs
- model specific HFEs for each activity that cannot be screened out and incorporate them into the PRA model
- evaluate the HEP including the consideration of dependencies

Table 19.1-14 identifies the post-initiator human actions that require detailed modeling. The post-initiator operator actions are generally those actions performed by the operator to place a mitigating system in service, including manual operation of a component and manual initiation as backup to auto-initiation. These actions affect the module response after a potential initiating event; thus, the applicable initiating event(s) is also identified. The table provides the HEP and associated error factor for each modeled human action.

The HEPs provided in Table 19.1-14 reflects the combined "diagnosis" and "action" probabilities. Diagnosis refers to determining the correct course of action to permit carrying out the required post-diagnosis actions. Action refers to tasks such as manually initiating a system in the course of following plant procedures. The diagnosis error probability is evaluated using a nominal probability of 0.01, adjusted for human factors conditions such as stress level, through the use of performance shaping factors, which are multipliers on the nominal probability. Similarly, the action error probability is evaluated using a nominal probability of 0.001, adjusted for human factors conditions as described in performance shaping factors.

Even though individual calculations were performed for each post-initiator operator action, a generic HFE basic event quantification approach has been incorporated by setting the first HFE in a sequence to the bounding calculated post-initiator HEP. Assuming dependence on additional HFEs in the sequence captures the concern of a lower bound on single HEPs, and prevents the potential of inappropriate cutset truncation of cutsets with numerous HFEs.

Dependency as applied to post-initiator HFEs reflects the possibility that the likelihood of an error is correlated to the probability of a prior error in a cutset. For the case of a second HFE in a cutset, the dependency is assumed to have moderate dependence. In the case of an HFE that is the third HFE in a cutset sequence, the dependency is assumed to have high dependence. Additional HFEs in a cutset are set to complete dependence.

Recovery actions are actions taken in addition to those actions initially identified by the HRA. They are typically included to allow credit for recovery from selected failures. At this stage of the design, recovery actions are not modeled in the NuScale PRA, as the HFEs for manual, local actions are not considered to be recovery actions for control room actions that fail as a result of human error (i.e., they are actions taken in place of control room actions).

Potential HFEs that are modeled are "errors of omission." With regard to "errors of commission," accident sequences are reviewed to identify the potential for an operator to get confused and inappropriately initiate an action. The potential actions that would fail or otherwise make unavailable a mitigating system, or that would have the potential to worsen an accident, are not found to be applicable failure modes in the sequences (e.g., unisolating the CFDS during a LOCA inside containment would be an error of commission that would create a potential release pathway; however, that action would also be associated with RCS injection which would not worsen the accident sequence). Thus, errors of commission are not modeled in the PRA (acts of sabotage and intentional acts of commission are also not included).

Consistent with industry practice, "Type B" HFEs are those that occur during normal operation and cause an initiating event and, thus are accounted for statistically by including them in the initiating event frequencies.

Test and Maintenance Unavailability

Test and maintenance basic events are included in the fault trees to account for component unavailability due to maintenance or testing when a module is in operation. NuScale design-specific test and maintenance unavailability data are not available so generic data and assumptions have been used as bounding values in the PRA model. Both corrective and preventative maintenance activities are considered when incorporating data into the model. Preventative maintenance is related to planned activities, which are performed to maintain equipment reliability; corrective maintenance refers to the repair of a component after it has failed or demonstrated degraded performance.

In the situation of parallel pumps in the system with at least one pump running, the test and maintenance basic event assumes that administrative controls would prohibit multiple pumps from being out of service for test and maintenance simultaneously. In the situation of a three pump system, the test and maintenance unavailability is calculated by increasing the probability by a factor of three, and associating the test and maintenance unavailability with one of the standby pumps.

The test and maintenance unavailabilities are modeled for the CVCS, CFDS, DWS, EDSS, ELVS, EHVS, and the MPS. Test and maintenance for the DHRS and ECCS occurs only during reactor outages while the module is flooded, and is therefore not modeled. The source for generic data supporting the test and maintenance unavailability values is NUREG/CR-6928.

Common Cause Failure Parameters

A CCF event is defined as an event leading to the failure or unreliable state of more than one component at the same time and due to the same shared cause. Common cause failure events require the existence of some cause-and-effect relationship that links the failures of a set of components to a single shared root cause. This may be the result of a shared attribute such as component type, location, component function, manufacturer, internal design envelope, operational states and modes, or testing and maintenance practices. A CCF event consists of component failures that meet the following criteria:

- two or more redundant components, including redundant component trains of the same type, fail or are degraded at the same plant and in the same system,
- component failures occur within a selected period of time such that success of the PRA mission would be uncertain,
- the component failures result from a single shared cause and are linked by a coupling mechanism such that other components in the group are susceptible to the same cause and failure mode, and
- the equipment failures are not caused by the failure of equipment outside the established component boundary.

Common cause failure is modeled using the "Alpha Factor" approach (α-factor model) described in NUREG/CR-5485 (Reference 19.1-60) to calculate the common cause basic event probability. The α- factor model is used because it

- is a multi-parameter model that can handle high redundancy levels.
- is based on ratios of failure rates which makes the assessment of its parameters easier when statistical data are unavailable on the number of group demands (i.e., the denominator).
- has a simpler statistical model, and produces more accurate point estimates as well as more representative uncertainty distributions compared to other parametric models which have the above two properties.

With respect to the test and maintenance contribution, the PRA assumes a non-staggered testing scheme. Performing test and maintenance activities simultaneously or sequentially, rather than a staggered scheme in which there is considerable time between activities, provides some conservatism in the failure probabilities (compared to using the staggered testing equations). Also, if multiple components are failed due to a CCF event, and if this type of failure were detectable by testing and inspecting, then staggering these activities would minimize the time that multiple components would be failed because of that CCF event. Thus, the average exposure time to an unrevealed CCF would be greater in a non-staggered testing scheme.

A common cause basic event is an event involving failure of a specific set of components due to a common cause. The common cause basic events were identified and incorporated into the system fault trees. Data used for CCF modeling are based NUREG/CR-5497 (Reference 19.1-61).

19.1.4.1.1.6 Software

The NuScale PRA was created in the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) code. SAPHIRE is used to model the response of a complex system to initiating events and to quantify the consequential outcome frequencies (or probabilities). For nuclear power plant applications, SAPHIRE can be used to identify important contributors to core damage and containment failure during a severe accident. In addition, it can be used for a PRA to model a reactor that is at full power or LPSD. The SAPHIRE code was developed by the NRC; its capabilities and limitations that could affect the results are included in the code documentation as presented in NUREG/CR-7039 (Reference 19.1-27). SAPHIRE has been demonstrated to generate appropriate results when compared to results from accepted algorithms, as indicated in NUREG/CR-7039.

Thermal-hydraulic modeling to support success criteria and accident progression modeling was performed with MELCOR and NRELAP5. Typically, NRELAP5 is used to confirm the success scenarios in the PRA, whereas MELCOR is used to simulate the core damage scenarios.

As described in Section 15.0, the NRELAP5 code is the NuScale proprietary thermal-hydraulics code developed from RELAP5-3D. The NRELAP5 model used for the PRA is a modification of the model that is used for design basis-LOCA and non-LOCA system transient calculations. The PRA model modifications provide for best estimate analysis and do not include several conservatisms that are employed in the design basis model. This model is intended for best estimate of module upset, beyond design basis transient analysis, evaluation of ATWS scenarios, and benchmarking the thermal hydraulics of the severe accident code, MELCOR.

A MELCOR model is developed and used with MELCOR Version 2.1. This model implements NuScale-specific code enhancements provided by Sandia National Laboratories under the auspices of the U.S. Department of Energy's cost sharing initiative to support the development and licensing of small modular reactor designs. The NuScale model is a set of text based input records that define the geometry and characteristics of the NPM. Using this input model and a user specified accident sequence, the MELCOR code simulates the progression of a severe accident. Starting from a nominal operating condition, the module state are advanced into severe accident space where phenomena such as cladding oxidation, core degradation, core relocation, and radionuclide release are evaluated.

The NRELAP5 code employs more sophisticated thermal-hydraulic models than MELCOR and is generally a superior tool for modeling the transient system performance prior to core degradation. As such, the approach for NuScale MELCOR simulations is to approximately match the progression of equivalent NRELAP5 simulations and then extend the analyses into severe accident space. The response of the MELCOR model with regards to severe accident phenomenology relies on the MELCOR code assessment to test data (Reference 19.1-28) and bestpractice recommendations for severe accident modeling from MELCOR code development staff and from published unique reactor consequence analyses (SOARCA) using MELCOR (Reference 19.1-29 and Reference 19.1-30). Because a design-specific benchmark for severe accident behavior of the NPM is not available, a line-by-line justification of the MELCOR inputs relevant to severe accident modeling is used. These aspects of the model include the detailed core nodalization, core component masses, radionuclide inventory and transport and hydrogen burn modeling.

19.1.4.1.1.7 Quantification

The quantification methodology encompasses two tasks: 1) quantification and analysis of sequences of events that could lead to core damage and 2) quantification and analysis of the potential containment response to the core damage sequences that could lead to a large release of radionuclides to the environment. Both of these tasks use the "fault-tree linking" approach.

The fault tree linking approach uses event trees that are developed for each initiating event. For the core damage analysis, the Level 1 event trees use branching decisions to question the success or failure of safety functions that are required to keep the core cooled and are organized in the event tree structure in a manner that defines the accident sequences that lead to core damage. The safety functions used in the event trees are modeled by fault trees that represent the potential for safety function failure. The fault trees model the safety functions as plant systems and include failure mechanisms that are modeled to the level of basic hardware failures and human action interface.

To evaluate the containment response to sequences that result in core damage, Level 2 event trees depict the possible sequence progressions after a core damage event. Core damage sequences are transferred from the Level 1 event trees to the Level 2 event tree. Fault trees are used to determine event probabilities. Both probabilistic and deterministic analysis techniques are used to understand and predict the containment response and magnitude of a potential radionuclide release.

Quantification of the PRA model was performed with the SAPHIRE code, which uses the following fundamental steps:

1) Link the fault tree models to the event tree sequences. SAPHIRE utilizes the fault tree linking approach whereby the fault tree logic is combined with the event tree logic (i.e. sequence logic) that results in accident sequence cutsets for each sequence in the event tree. Each of the 11 Level 1 event trees contain system top events that represent the mitigating systems that may be called upon in the mitigation of the initiating event in question.

2) Include quantification of operator actions and application of post-processing rules (e.g., elimination of mutually exclusive maintenance events).

3) Quantify the minimal cutsets with event data.

4) Determine the final set of accident sequences.

5) Partition the accident sequences into appropriate plant damage states (e.g., "CD" for a core damage state).

6) Perform sensitivity, importance, and uncertainty analyses on the accident sequences.

An appropriate truncation level ensures that dependencies and significant accident sequences are not eliminated from the evaluation. Consistent with the ASME/ANS PRA Standard, a convergence analysis was performed with SAPHIRE to evaluate the point at which less than a five percent change in CDF occurs after the truncation level is reduced by a factor of ten. Based on the convergence results, a truncation value of 1E-15 was used for the CDF.

Values of risk metrics such as CDF and LRF for each hazard are provided as statistical mean values. Because true mean values can be produced only by first generating a probability distribution, and it is not practical to comprehensively perform an exhaustive uncertainty analyses on all intermediate results, unless otherwise explicitly stated all results presented are generated by the point estimate quantification of the PRA logic model. Because the basic event point estimate values used in the PRA quantification are, infact, mean values, the point estimate results that are calculated are expected to be very close to the true mean values from the probability distributions that are produced from the full Monte Carlo simulations used to generate the probability distributions on the final results. However, while in theory, the propagation of mean values in a point-estimate quantification, should produce a final result of a mean value, in practice because of approximations used in the quantification and different probability distributions assumed for the basic events, there will be small differences between the mean value results produced via an uncertainty propagation process and those produced via a point estimate quantification.

19.1.4.1.1.8 Uncertainty

As discussed in NUREG-1855 (Reference 19.1-6), two general types of uncertainty should be considered in risk informed decision making. Aleatory uncertainty is due to the randomness of the nature of events or phenomena; the PRA model is an explicit model of the random processes and thus, addresses aleatory uncertainty by definition. Epistemic uncertainty is associated with the lack of knowledge about an event, system, phenomena, or model. Three types of epistemic uncertainty were then considered:

<u>Parameter Uncertainty</u> - Parameter uncertainty relates to the uncertainty associated with the computation of the parameter values (i.e., data) used to quantify the model. The data parameters include initiating event frequencies, component failure probabilities, CCF events and their alpha factors, and human error probabilities. The uncertainties associated with these parameters can be characterized by probability distributions that relate to the degree of belief in the confidence in their values. SAPHIRE has the built-in ability to perform an uncertainty analysis. After cutsets were generated in SAPHIRE, an uncertainty analyses was performed using the Latin Hypercube uncertainty sampling methodology.

<u>Model Uncertainty</u> - Model uncertainty is the uncertainty associated with assumptions made in the construction and quantification of the PRA model. A customary source of model uncertainty relates to an issue in which there is not a consensus approach or method to model a specific aspect and where the choice of approach or assumptions could affect the PRA. Another source of model uncertainty is associated with the limited functional knowledge of a design-phase NPM and plant. Model uncertainties are addressed through sensitivity studies or using realistic or best judgment assumptions. The guidance provided in EPRI TR-1016737 (Reference 19.1-7), was used to address the sources of model uncertainty.

<u>Completeness Uncertainty</u> - Completeness uncertainty pertains to the uncertainty regarding the risks that may have been excluded from the PRA model. These types of uncertainties may have significant impact on the risk insights of the PRA model. Examples of completeness uncertainty are:

- The scope of the PRA may have omitted certain initiating events or hazards.

- Specific system or phenomenological behavior may not fully be incorporated into the model.
- Detailed design features are not available at the design certification stage. Specific failure mechanisms, coupling mechanisms between modules, operator actions, or system behavior may not be fully understood and reflected into the model.

Because the scope of PRA is that of Design Certification Application submittal and the development of the PRA is based on design parameters and inputs rather than an as-built, as-operated plant, there are inherent completeness uncertainties associated with PRA.

19.1.4.1.1.9 Risk-Significance Determination

The PRA provides insights into the risk significance of SSC and operator actions with regard to core damage and large release frequencies. Importance measures provide a method to observe how significant a component is with respect to these risk metrics.

The process of calculating PRA system importance parameters has two aspects: 1) calculating the potential maximum risk increase and 2) calculating the overall percent contribution to the total risk. The first aspect is based on an absolute evaluation of the risk achievement worth (RAW) which considers the effect of complete unavailability of an SSC. The second aspect is based on the Fussell-Vesely (FV) importance measure which represents the fractional reduction in risk given perfect performance. As described in TR-0515-13952-A (Reference 19.1-8), "significance" for the NuScale Power Plant design was evaluated using an approach that reflects its very low calculated frequency of core damage. The very low calculated CDF implies that even exceedingly small changes in the calculated core damage or large release frequencies would be risk significant if traditional approaches based on relative changes were used. The approach provided in Reference 19.1-8 allows insights into the potential risk significance of SSC and operator actions with respect to safety goals without identifying small changes in a very low calculated risk metric as risk significant.

As summarized in Table 19.1-19, the criteria for determining SSC as candidates for risk significance are based on absolute rather than relative importance measures. The absolute importance measures are defined as the conditional core damage frequency (CCDF) and conditional large release frequency (CLRF). These absolute measures are used to evaluate risk significance instead of the traditional RAW evaluation based on a relative change in risk.

In addition to individual components, the FV importance measure is used to evaluate the risk significance of other basic events. This risk measure is used to identify basic events that have the largest fractional risk contribution, irrespective of the CDF or LRF value, by evaluating the reduction in risk if the basic event is assumed to be always successful. The FV importance measures are developed for contribution to core damage frequency (FVCDF) and contribution to large release frequency (FVLRF).

The importance measures are applied at a single module level. The absolute RAW thresholds apply to the aggregated risk across hazards, and the FV thresholds apply individually to each hazard group and mode of operation, and individually to CDF and LRF.

The SSC that were found to be "risk significant" by use of the importance measures are identified as candidates for inclusion in the Design Reliability Assurance Program, as discussed in Section 17.4.

19.1.4.1.2 Results from the Level 1 Probabilistic Risk Assessment for Operations at Power

This section provides results of the Level 1 PRA for full-power operation of a single module. Core damage frequency and insights on the significant contributors to the calculated CDF are presented. Uncertainties and sensitivity studies associated with the results are discussed.

Core Damage Frequency

The mean value of the uncertainty distribution on CDF due to internal events for a module during power operation is calculated to be 3.0E-10 per mcyr; the 5th and 95th percentile values are 1.0E-11 per mcyr and 1.1E-09 per mcyr, respectively. Module availability is assumed to be 100 percent, which results in a slight conservatism in the initiating event frequencies and the associated full-power CDF.

Significant Core Damage Sequences

The significant core damage sequences are provided in Table 19.1-17. The table provides the sequence identifier, the percentage contribution to the CDF, and a summary description of the sequence. The table illustrates that the dominant sequence is an RCS loss-of-coolant accident inside containment, which contributes 22 percent of the CDF. Loss-of-offsite power sequences contribute about 22 percent to the CDF and loss of DC power sequences contribute about 16 percent to the CDF.

Significant Core Damage Cutsets

Each accident sequence consists of a combination of an initiating event and basic events to form a cutset. The cutsets from the Level 1 internal events PRA that contribute individually more than one percent to CDF are presented in Table 19.1-18. As the table indicates, the most significant cutsets contributing the most involve incomplete ECCS actuations due to CCFs of the RRVs or RVVs to open.

Core Damage Frequency Contribution by Initiating Event

Figure 19.1-13 illustrates the contribution of each initiating event to the internal events point estimate CDF. The values provided in Figure 19.1-13 result from a point estimate calculation using mean values for basic events. The figure illustrates that the dominant contributing initiating event to core damage is an RCS loss-of-coolant accident inside containment. Loss of offsite power, loss of support systems, loss of DC power, a general transient, and CVCS line breaks outside of containment are measurable contributors to the CDF.

Risk Significance

As indicated in Section 19.1.4.1.1.3, the safety functions for the prevention of core damage are fuel assembly heat removal, reactivity control, and containment integrity.

The PRA provides insights into the risk significance of SSC and operator actions with regard to CDF. Importance measures provide a method to observe how significant a component is with respect to risk.

Table 19.1-20 identifies the candidate risk-significant SSC based on the Level 1 PRA for a module. The SSC identified by “Met” have an importance measure that meets the risk significance threshold value using the methodology described in Section 19.1.4.1.1.9. At the component level, the associated PRA basic event is also identified. There are no human actions that meet the risk significance thresholds based on the Level 1 PRA.

Key Assumptions

Table 19.1-21 summarizes the key assumptions associated with the Level 1, full-power internal events PRA. The table also provides the basis for the assumption.

Uncertainties

Section 19.1.4.1.1.8 summarizes the types and treatment of uncertainties associated with the Level 1 PRA. Parameter uncertainty is characterized by probability distributions associated with the calculated results. Table 19.1-15 summarizes important generic sources of model uncertainty, how those uncertainties were addressed and their effects on the model. Table 19.1-16 summarizes key design specific sources of model uncertainty, how those uncertainties were addressed and their effects on the model. Evaluating the effect of some uncertainties on PRA results required sensitivity studies.

Sensitivity Studies

To provide additional insights on the CDF and component importance measures, sensitivity studies were performed. The sensitivity studies investigated the importance of modeling assumptions and uncertainties. Table 19.1-22 summarizes such studies, the basis for the study and the associated results for the Level 1 full power PRA. The table includes sensitivity studies recommended by Reference 19.1-7 for generic uncertainties associated with human error probabilities and CCF as well as design-specific uncertainties. The table also includes results of a sensitivity study which credits only safety-related SSC to evaluate the need for including nonsafety-related SSC that require regulatory treatment through the regulatory treatment of nonsafety systems (RTNSS) program.

Key Insights

There are primarily two phenomena and three systems that underlie the very low risk of a NuScale module.

Key Phenomena

A large negative moderator temperature coefficient (MTC) and passive heat removal capability (from the RPV to the CNV and from the CNV to the reactor pool) are important phenomenological characteristics of the design.

At full power, the core exhibits a large positive moderator density coefficient (negative MTC), even at beginning of cycle conditions. As a result, the core is rendered subcritical shortly after a loss of normal feedwater, even without inserting control rods (i.e., an ATWS). The long-term ATWS response is unique because of the excess heat transfer capacity of the passive cooling systems. This excess heat transfer results from the relatively small core size, a large coolant-to-power ratio, and the efficient passive heat transfer systems. Return to power occurs only after passive heat transfer to the UHS has been established. The strong negative reactivity feedback and large coolant-to-power ratio ensure that the core fission power increases to meet the passive heat removal capacity, but does not exceed it. The resulting fission power is easily accommodated by the UHS, and the core is cooled. The effect of the strong negative reactivity feedback phenomena is reflected in the PRA model in that the event tree accident sequence structure is similar for both the success and failure of reactor trip.

Facilitating passive heat transfer to the UHS is the lack of insulating material on both the reactor vessel and the CNV. Following a LOCA or RSVs cycling, primary coolant collects in the containment to the point that the lower reactor vessel becomes submerged. For transients in which RSVs have cycled, the temperature inside the RPV is sufficiently high that heat transfer to the water collected in the containment becomes greater than decay heat levels. This condition occurs after roughly a dozen RSV cycles after which the RPV pressure subsides and RSV cycling stops. For the remainder of the event, decay heat is accommodated by transferring it passively (by conduction and convection) through the uninsulated vessel wall to the coolant that has collected in the containment. Similarly, heat is being transferred passively (by condensation, conduction and convection) to the UHS through the containment wall.

Key Mitigating Systems

The most important risk-significant SSC are the RSVs, the ECCS, and the CNTS.

As noted above, primary coolant system integrity is ensured by cycling RSVs during sequences in which secondary heat removal is not available or a failure to scram has occurred. While the primary purpose of the RSVs is RCS overpressure protection, an additional benefit of cycling RSVs is to provide steam that condenses on the CNV walls and collects in the lower portion of the CNV. Thus, operation of the RSVs facilitates the passive heat transfer from the RPV to the CNV by preserving the coolant inventory used for core heat removal and obviating the need for makeup to the RPV. This combination of cycling of RSVs and passive heat removal minimizes the importance of secondary heat removal by the steam generators. The primary role that secondary heat removal plays following a transient is to determine the path of heat from the core to the reactor pool (either through the steam generators and the DHRS heat exchangers or through the RPV wall to the CNV and then through the CNV wall to the pool). With or without secondary side cooling, heat ultimately is transferred to the reactor pool. The role DHRS plays in managing safety during transient conditions is diminished in this regard being limited to determining whether RSVs are demanded (i.e., DHRS operation alone is sufficient to maintain the core cooled, and RSV operation is not necessary).

An ECCS is provided that can mitigate the entire spectrum of inside-containment LOCAs. During a LOCA, primary coolant system conditions are lower in pressure and temperature than for transients and passive heat removal from the reactor to the CNV may not be sufficient to accommodate decay heat. There is a need to return inventory in the RPV that is lost during a LOCA in order to maintain core cooling. The ECCS provides this function. The ECCS consists of RVVs that are each large enough that the reactor pressure is reduced to near containment pressure and RRVs that are sufficiently large that the static head of coolant that has collected in containment flows back into the RPV to maintain core cooling. By steaming to containment (out the break and also through the RVVs), condensing and flowing back into the reactor (through the RRVs) through natural circulation, the ECCS provides adequate core cooling for all (inside containment) LOCA conditions without the need for external inventory makeup.

While rare, loss of primary coolant outside containment is considered in the PRA (e.g., SGTF, pipe breaks outside containment). The CNV and associated valves play a role in further reducing the significance of these accidents. Loss of coolant through a failed steam generator tube is terminated with main steam and feedwater isolation. Pipe breaks outside containment through CVCS is terminated through closure of isolation valves on the injection and discharge lines. It should be noted that all of the pipes connected to the RPV that have been identified as potential sources for pipe breaks outside containment are designed for full RCS pressure and temperature. Once isolated, the break flow is terminated and the accident proceeds in a manner very similar to a transient, requiring only passive heat removal from the reactor to the pool to maintain adequate core cooling.

Because safety-related mitigating systems are fail safe on loss of power, there is little need of support systems for managing risk for the NuScale design. Nevertheless, when power is available, portions of the MPS are needed to actuate these systems. This is largely limited to the actuation priority logic (APL) and the equipment interface modules (EIMs) for the ECCS and CNTS as both automatic and manual actuation are processed by these MPS components.

Approximately a dozen human actions are modeled in the PRA. These are limited to latent faults (e.g., mis-calibration errors) and recovery actions (e.g., manual backup of an automatic actuation). No operator actions are required for the nominal response to a design basis accident.

While derived considering internal initiating events, the above insights are generally applicable for internal floods, internal fires and external events. The key phenomena discussed above are dependent on only physical plant conditions and occur passively regardless of whether the initiating event is caused by a fault internal to the plant or by an external event such as high winds, external flooding or ground motion due to a seismic event. The key systems described above are protected from external events through the design of the systems themselves as well as protection provided by the seismic class 1 RXB. Therefore, the general insights summarized above are applicable to the mitigation of external events as well as internal events.

Table 19.1-23 summarizes these insights.

19.1.4.2 Level 2 Internal Events Probabilistic Risk Assessment for Operations at Power

The following sections describe the Level 2 PRA, which evaluates the potential for radionuclide release external to the plant from a severe accident in a module. Section 19.1.4.2.1 describes the Level 2 PRA for full-power operation; Section 19.1.4.2.2 provides the results of this evaluation.

19.1.4.2.1 Description of the Level 2 Probabilistic Risk Assessment for Operations at Power

The following sections address the methodology, data and analytical tool used to perform the full-power, internal events Level 2 PRA.

19.1.4.2.1.1 Methodology

A Level 2 PRA is performed to evaluate the potential for a severe accident progressing to the point of radionuclide release from the CNV. The design and operating characteristics of a NuScale module are such that the PRA is relatively simple, with few Level 1 end states. This allows the Level-2 event tree to be a direct transfer from the end state of the Level-1 event trees, without the need to perform an intermediate grouping or detailed "binning" of Level 1 core damage sequences; i.e., all core damage sequences identified in the Level 1 analysis are binned into the "CD" plant damage state.

The Level 2 event tree models the progression of a severe accident from core damage to the point of a potential release. The Level 2 event tree is also referred to as the containment event tree (CET). End states of the CET define the conditions that characterize the effect of the sequence on the environment, i.e., the potential radionuclide release. As such, end states reflect release characteristics such as timing and magnitude. Due to the simplicity of the design, only two CET end states are used to model radionuclide release. The end state “NR” is associated with a release that may be attributed to leakage from the boundary of an isolated containment; the end state “LR” is associated with a release from an unisolated containment. Each of these end states is assigned to a release category (RC) to represent the radionuclide source term.

19.1.4.2.1.2 Containment Event Tree

In the NuScale PRA, the CET is directly linked to the end state of the Level-1 event trees. Therefore, there is no development of plant damage states (PDS) to group sequences by similar characteristics. Instead, each core damage accident sequence that is not a success is directly linked to the CET by the transfer event LEVEL2-ET. As such, each core damage accident sequence is directly linked and propagated through the CET. As summarized below, most containment failure modes typically considered in Level 2 PRA analyses are demonstrated by analyses discussed in Section 19.2 not to challenge containment integrity in the NuScale design. As such, all Level 1 sequences that are classified as core damage (i.e., whose end state is not "OK") transfer to a single CET initiating event, Level2-ET, as illustrated in Figure 19.1-15.

Severe Accident Processes and Phenomena

Potential severe accident phenomena are evaluated to determine their applicability to the NuScale design. The evaluation considers phenomena listed in Section 19.0 of the Standard Review Plan, the ASME/ANS PRA Standard, NUREG/CR-2300 (Reference 19.1-38) and NUREG/CR-6595 (Reference 19.1-39).

The characteristics of the NuScale design provide an inherent degree of safety. As a result, severe accident phenomena that may challenge containment in currently operating plants are shown by analyses summarized in Section 19.2 to not challenge containment integrity in a postulated NuScale severe accident.

Thus, containment failure due to bypass or containment isolation valve failure is the only mode of containment failure depicted in the CET. The following severe accident processes were considered and are discussed in detail in Section 19.2, as indicated:

- Retention of core debris in RPV, external RPV cooling (Section 19.2.3.2.1 and Section 19.2.3.3.1)
- Retention of core debris in CNV (Section 19.2.3.2.2)
- Hydrogen deflagration and detonation (Section 19.2.3.3.2)
- High pressure RPV failure and associated phenomena (Section 19.2.3.3.4)
- Fuel coolant interaction and steam explosion (Section 19.2.3.3.5)
- Molten core-concrete interaction (Section 19.2.3.3.3)
- Containment bypass (Section 19.2.3.3.6)

The containment ultimate capacity is addressed in Section 19.2.4.

19.1.4.2.1.3 Success Criteria

The Level 2 PRA is bounding in that it does not credit mitigating systems or capabilities that are relevant only to a radionuclide release (e.g., a building spray system). The top event "CD-T01" in Figure 19.1-15 is simply a branch that allows quantification of the core damage probability that is developed from the transfer of Level 1 results to the CET. Thus, the only mitigating function that is modeled in the CET is containment isolation, as illustrated by top event "CNTS-T01" in Figure 19.1-15. Top event CNTS-T01 includes containment isolation failure, and resulting bypass, associated with fault tree events for:

- CES Containment Isolation Fails and Results in Bypass.
- CVCS Containment Isolation Fails and Results in Bypass.
- SGTF and Containment Bypass.

Section 6.2 describes CNV penetrations in detail. For evaluation in the Level 2 PRA, penetrations are grouped into three types: (1) piping connections, (2) bolted flange inspection ports, including electrical penetration assemblies, and (3) ECCS trip and reset pilot valve penetrations. Fluid system penetrations include at least two barriers in series so that a single failure or component malfunction does not result in a loss of isolation. The fluid system piping safe-ends and the penetration nozzle-to-safe end welds are part of the CNV. The boundary is at the end of the safe-ends furthest from the CNV shell. The pipe-to-safe-end welds are part of the attached piping. This applies to the FWS nozzles, MSS nozzles, CVCS nozzles, containment evacuation system (CES) nozzle, CFDS nozzle, reactor core cooling water system (RCCWS) nozzles, and DHRS nozzles.

The electrical penetration assembly boundary is at the face of the CNV flange surface for the penetration opening and includes the bolting (studs and nuts). There are eleven electrical penetration assemblies located on the CNV head. The electrical penetration assemblies provide a leak tight barrier against the uncontrolled release of radioactivity to the environment.

The three RVV and two RRV emergency core cooling system valve trip and reset pilot assembly safe-end penetrations are welded to the external side of the penetration nozzle. The safe-ends and the penetration nozzle-to-safe-end welds are part of the CNV. The valve assembly is welded to the penetration nozzle safe-end. The boundary is in the valve assembly-to-safe-end welds and the weld are part of the CNV. Each pilot valve has a double seal.

In a system line that is normally open, one valve needs to close for success in preventing radionuclide release from containment. Similarly, for sequences that involve an SGTF, one valve in each FWS and MSS containment isolation pathway needs to close for success. Although the design includes multiple containment isolation signals from a diverse set of sensors, only one sensor group is credited for initiating a containment isolation signal.

Because the CNV is maintained at a vacuum, so that CNV leaks or isolation failures can be readily detected and addressed, small penetration failures or leaks are not considered as contributors to containment isolation failure.

Table 19.1-24 summarizes containment penetrations, the isolation method and treatment in the PRA.

19.1.4.2.1.4 Release Categories

The Level 2 event tree, provided as Figure 19.1-15, is completed by defining the end state of each sequence. The figure provides three end states, "CD", "NR" and "LR." The end state "CD" allows quantification of the CDF as it summarizes the sequences transferred from the Level 1 event trees. The end state "NR" represents a core damage sequence with intact containment; for this end state, the potential radionuclide release is due to allowable leakage as defined by the Technical Specifications. The "LR" end state represents a large release. Due to the small core used in the design, additional release categories to reflect a range of release possibilities were judged to be unnecessary. The release categories are:

- RC1 is core damage with successful containment isolation.
- RC2 is core damage with containment bypass or failure of containment isolation.

The large release frequency (LRF) is the quantified result of the Level 2 PRA, and is used to demonstrate conformance with the safety goal promulgated in NRC policy statement (Reference 19.1-36). While various definitions of “large release” have been considered, there is not an established consensus definition. The definition used in the NuScale PRA is based on a threshold radionuclide dose that could result in early injuries.

Specifically, NUREG-0396 (Reference 19.1-9) specifies 200 rem whole body dose as the dose at which significant early injuries start to occur. This dose was used as the basis for defining a “large release” in terms of a hypothetical individual located at the site boundary; in the NuScale PRA, the “site boundary” is a best-estimate distance and is defined as one-half of the shortest site dimension, which is approximately 884 feet (0.167 miles).

Based on simulation results using the MACCS code (Reference 19.1-10), and following Steps 1 through 5 below, a release fraction of 2.9 percent of the iodine core inventory results in an acute 200 rem whole body (red marrow) mean dose over all weather trials at the site boundary. The mean MACCS plume dispersion relative radionuclide concentration results are equal to or greater than those provided by the ARCON96 code (described in Section 15.0.2) at and beyond the site boundary.

1) Radionuclide groups are scaled relative to iodine, consistent with Table 11 of SAND2011-0128 (Reference 19.1-63) for the gap release and in-vessel release phase based on PWR low burn-up uranium dioxide fuel, and released directly to the environment.

- The 69 radionuclides evaluated by the State-of-the-Art Reactor Consequence Analysis (SOARCA) (Reference 19.1-66) are considered in the release to the environment.
- The 69 radionuclides are grouped consistent with the SOARCA analysis.
- The initial core inventory of the 69 radionuclides is consistent with the best estimate core inventory provided in Table B-5 of the Environmental Report (Reference 19.2-16).

2) The release begins immediately following core damage; this maximizes radionuclide inventory by minimizing radioactive decay.

   - Fission product pipe deposition, building retention (i.e., building filtration system or biological shield), and reactor pool scrubbing are not considered.
   - The release is assumed to occur at the ground level from the short face of the RXB, which conservatively estimates the initial relative radionuclide concentration when building wake effects are considered.
   - An elevated release and plume buoyancy are not credited to decrease ground level air concentrations.
   - Plume meander at low wind speeds and stable atmospheric conditions is not credited to reduce the relative radionuclide concentration during plume transport and dispersion.

3) The release to the environment is assumed to have a two-hour duration which reduces the effect of wind shifts during the release.

   - The total release is divided into two equal one-hour segments. The release rate is constant throughout each segment (i.e., each hour of the release contains the same release fraction).
   - The hourly wind direction, wind speed, atmospheric stability, and precipitation rate are based on meteorological data described in Section B.1.6.3 of the Environmental Report.

4) Dose receptors are assumed to be present at all azimuthal directions on the site boundary; they are also assumed to remain stationary.

   - A 96-hour absorption window at the site boundary is assumed, corresponding to an upper bound for the range of time factors discussed in Environmental Protection Agency, "PAG Manual: Protective Action Guides and Planning Guidance for Radiological Incidents" (Reference 19.1-40).
   - Protective actions are not considered (e.g., dose receptors do not perform sheltering or evacuation).

5) The acute 200 rem whole body dose is the mean dose over one year of MACCS meteorological trials. For each trial, the reported dose is the peak dose on the spatial grid.

The 2.9 percent iodine group release fraction threshold is then used to distinguish between Release Categories 1 and 2.

RC1: core damage with successful containment isolation.

To ensure RC1 sequences are below the threshold of a large release, a bounding analysis is employed to envelope intact containment sequences. A calculation of the maximum possible iodine release fraction to the environment from a single module accident with intact containment, assuming the Technical Specification leak rate limit, is calculated to be 0.8 percent of the iodine core inventory; this is well below the threshold of a large release. The leakage is calculated for a 96 hour time period, with the following conservatisms:

- Radionuclide groups are scaled relative to iodine, consistent with Table 11 of SAND2011-0128 for the gap release and in-vessel release phase, based on PWR low burnup uranium dioxide fuel, such that the entire core inventory of iodine is released to containment (i.e., the SAND2011-0128 release fractions for all radionuclide groups are multiplied by approximately 3.3, with an upper bound of a 100 percent release for all radionuclide groups).
- The release to containment is assumed to remain airborne, and deposition in containment is not credited to reduce the airborne fraction of radionuclides in containment.
- All airborne radionuclides in containment are assumed to release directly to the environment (i.e., bypassing the RXB) at the Technical Specification limit of 0.2 percent containment air weight per day over the entire release duration.

RC2: core damage with containment bypass or failure of containment isolation

This RC represents the release associated with a core damage sequence that does not have successful isolation of the CNV, i.e., not categorized as “RC1.” These sequences have a Level 2 end state of RC2 and are associated with a "large" release.

19.1.4.2.1.5 Data Sources and Analysis

This section provides the sources of numerical data used in the Level 2 PRA. Initiating event frequencies, component failure rates, equipment unavailabilities, human error probabilities, and common-cause failure parameters are discussed.

Containment Event Tree Initiating Event Frequency

The frequency of the CET initiating event, "LEVEL2-ET", is the summation of contributions from all core damage sequences.

Component Failure Rates and Equipment Unavailability

Because the NPMs and plant do not have an operating history, failure rates are derived from generic data (i.e., based on industry information or other accepted practices and standards). The generic data sources to support quantification of top event CNTS-T01 are summarized in Section 19.1.4.1.1.5.

Because the CNV is maintained subatmospheric during power operation, to minimize heat loss, testing and maintenance on containment penetrations is expected to be performed during outages. As such, unavailability of the CIVs because of testing or maintenance is not included in the model. Unavailability because of testing or maintenance on the equipment providing the signals to close the valves is included in the model.

Human Error Probabilities

There is one post-initiator operator action modeled for containment isolation, CNTS--HFE-0001C-FTC-N. It is a recovery action following failure of the MPS auto-actuation of containment isolation. Valve position indication is provided in the control room, and the action is performed in the control room. No credit is given for repair of a CIV to accomplish this action.

Common Cause Failure Parameters

Common cause events are modeled in the Level 2 PRA. A CCF of the redundant CIVs to close is included in the Level 2 PRA. Common cause failure modeling is the same as described in Section 19.1.4.1.1.5.

19.1.4.2.1.6 Software

Quantification of the Level 2 PRA is performed with the SAPHIRE code as described in Section 19.1.4.1.1.6. Thermal-hydraulic modeling to support accident progression modeling is performed with NRELAP5 and MELCOR as described in Section 19.1.4.1.1.6.

19.1.4.2.1.7 Quantification

Linking of the Level 2 CET and system models to quantify the Level 2 results is performed using the SAPHIRE software in the same manner as is performed in the Level 1 analysis. By physically linking the Level 1 system models with the Level 2 system models, system dependencies are explicitly captured.

An appropriate truncation level ensures that dependencies and significant accident sequences are not eliminated from the evaluation. Consistent with the ASME/ANS PRA Standard, a convergence analysis was performed with SAPHIRE to evaluate the point at which less than a five percent change in LRF occurs when the truncation level is reduced by a factor of ten. Based on the convergence results, a truncation value of 1E-15 is used for the LRF.

19.1.4.2.1.8 Uncertainty

The types and treatment of uncertainty associated with the Level 2 PRA are the same as discussed in Section 19.1.4.1.1.8 for the Level 1 PRA.

19.1.4.2.2 Results from the Level 2 Probabilistic Risk Assessment for Operations at Power

This section provides results of the Level 2 PRA for full power operation of a single module. Large release frequency and insights on the significant contributors to the calculated large release frequency are presented. Uncertainties and sensitivity studies associated with the results are discussed.

Large Release Frequency

The mean value of the large release frequency for a single module due to internal events at-power for a module was calculated to be 2.3E-11 per mcyr; the 5th and 95th percentile values are 1.4E-13 per mcyr and 5.8E-11 per mcyr, respectively.

Conditional Containment Failure Probability

The conditional containment failure probability (CCFP), defined as the ratio of LRF to CDF, for full-power operation of a module is 0.06 for the internal events core damage sequences assessed in the PRA.

Significant Large Release Sequences

The significant core damage sequences that contribute to the LRF are provided in Table 19.1-25. The table provides the sequence identifier, the percentage contribution to the LRF, and a summary description of the sequence. The table illustrates that the large release frequency is dominated by sequences with a CVCS line failure outside of the CNV coupled with failures of the CIVs. The dominant core damage sequence involves operator failure to initiate CFDS injection to compensate for the loss of inventory.

Significant Large Release Cutsets

Each accident sequence consists of a combination of an initiating event and basic events to form a cutset. The significant cutsets from the Level 2 internal events PRA are presented in Table 19.1-26. As the table indicates, the cutsets contributing most to the LRF involve a CVCS line failure outside of the CNV coupled with CCF of the CIVs. The cutsets include operator and equipment failures associated with CFDS injection.

Large Release Frequency Contribution by Initiating Event

Figure 19.1-14 illustrates the contribution of each initiating event to the internal events point estimate LRF. (The values provided in Figure 19.1-14 result from a point estimate calculation using mean values for basic events.) The figure illustrates that the dominant contributing initiating event to a large release from a module is a CVCS line break outside containment which constitutes more than 90 percent of the LRF.

Risk Significance

The Level 2 PRA provides insights into the risk significance of SSC and operator actions with regard to large release frequency. The methodology for evaluating risk significance is described in Section 19.1.4.1.1.9.

As indicated in Section 19.1.4.1.1.3, the safety functions associated with the prevention of a large release are:

- Fuel assembly heat removal: The function to remove heat transferred from the RPV to the reactor pool (UHS)
- Containment integrity: The function to isolate containment and contain fission products within the CNV volume, preventing a post-accident release to the environment

Table 19.1-27 identifies the candidate risk-significant SSC based on the Level 2 PRA for a module. The SSC identified by "Met" have an importance measure that meets the risk significance threshold value using the methodology described in Section 19.1.4.1.1.9. At the component level, the associated PRA basic event is also identified.

As indicated in Table 19.1-27, one human action was found to be risk significant to prevention of a large release; it is operator failure to initiate CFDS injection.

Key Assumptions

Table 19.1-28 summarizes the key assumptions associated with the Level 2, full-power internal events PRA. The table summarizes the basis for the assumption and how the assumption was evaluated in the PRA model (e.g., conservative modeling).

Uncertainties

Section 19.1.4.2.1.8 summarized the types and treatment of uncertainties associated with the Level 2 PRA. Parameter uncertainty is characterized by probability distributions associated with the calculated results. Table 19.1-29 summarizes important generic sources of model uncertainty, how those uncertainties were addressed and their effects the model. Table 19.1-30 summarizes key design-specific sources of model uncertainty, how those uncertainties were addressed and their effects on the model. Evaluating the effect of some uncertainties on PRA results required sensitivity studies.

Sensitivity Studies

To provide additional insights on the LRF and component importance measures, sensitivity studies were performed. The sensitivity studies investigated the importance of modeling assumptions and uncertainties. Table 19.1-31 summarizes such studies and associated results for the Level 2 at-power PRA.

Key Insights

In the context of a potential radioactive release to the public, there is primarily one system and one phenomenon that underlies the very low risk of an NPM; specifically CNTS and passive heat transfer to the UHS, respectively.

Key Mitigating Systems

Containment isolation is modeled explicitly in the PRA and, if failed, is assumed to lead to a large release under severe accident conditions. The dominant contributors to CNTS failure are failure to close injection or discharge valves following a CVCS pipe break outside containment and failure to close MSIVs or FWIVs following an SGTF (either an initiating event or induced following a severe accident). More significant, however, is the role that the CNTS plays in ensuring that primary coolant inventory is preserved thereby retaining core debris in the RPV.

Key Phenomenon

When the containment is isolated, primary coolant is located in either the RPV or the CNV, or split between the two. If primary coolant is within the RPV, then the core is covered and cooling is available. If the core is not covered, then primary coolant must be in the CNV and has submerged the outside of the lower part of the RPV. With the RPV submerged, passive heat removal from the RPV to the CNV and from the CNV to the UHS results. This heat removal path cools debris within the RPV preventing the debris from penetrating the lower head thereby eliminating ex-vessel severe accident challenges to the CNV.

Severe Accident Challenges

Severe accident phenomena that can challenge the CNV include those that might occur with the core still in the RPV, those that could be a result of the core relocation from the RPV to the CNV, and those that might result regardless of the location of the core. Severe accident containment challenges are evaluated in the NuScale PRA and dispositioned either deterministically or modeled probabilistically:

- Hydrogen combustion within the containment is not a hazard to CNV integrity because power operation occurs with the CNV effectively evacuated; hence there is very little oxygen available to mix with generated hydrogen and produce a combustible mixture. The possibility of combustible gas mixtures is further reduced under severe accident conditions when the containment would be inerted with steam. Even in idealized hypothetical combustion scenarios, the minimal oxygen inventory limits the energetics such that the CNV is not at risk.
- Containment overpressurization due to generation of non-condensable gases cannot occur because there is no concrete within the containment with which molten-core debris could interact to produce non-condensable gases. The CNV

is not susceptible to overpressurization from steam generation because of the passive heat removal through the CNV wall. The CNV is partially immersed in the reactor pool (i.e., the UHS). The passive heat removal capability is not only greater than decay heat levels, but also greater than the expected power levels following a failure to scram, thus protecting CNV from being pressurized beyond its failure pressure.

- Molten core-concrete interaction is not a challenge to the CNV because there is not a concrete basemat within the CNV. The potential challenge of core debris in contact with the steel CNV shell has been evaluated.
- Primary coolant system overpressure failure would occur only if both safety-related RSVs failed to open during a transient with loss of heat removal through the steam generators (i.e., failure of both normal feedwater and of the DHRS). This extremely improbable scenario was addressed using a finite element structural analysis and shown to result in a slow-progressing asymmetrical flange separation on the pressurizer. Thermal-hydraulic simulations show that the resultant induced-LOCA does not pressurize the CNV beyond its ultimate failure pressure, and is therefore not considered a large release unless concurrent with failure of containment isolation. Furthermore, the induced-LOCA behaves like other severe accidents in that the RPV-CNV pressure differential decreases before core damage occurs, eliminating risk of a high-pressure severe accident and the associated containment challenges such as HPME and direct containment heating.
- Analysis of the potential for in-vessel steam explosions indicates that postulated steam explosions do not challenge the RPV. The design and materials of the core support structure are such that they are predicted to fail and relocate the core into the lower RPV head before temperatures in the core reach the fuel melting point. In addition, there would be only a small amount of water in the lower vessel head with which the core debris could interact.
- Although analysis indicates that ex-vessel containment challenges associated with sequences in which the core penetrates the RPV and enters the CNV do not occur, these events are considered from a defense-in-depth perspective. Such ex-vessel challenges would include HPME, ex-vessel steam explosion, and contact of core debris with the CNV lower head. The combination of successful containment isolation (which ensures primary coolant remains within the containment even under severe accident conditions) plus passive heat removal (from the RPV to the CNV and CNV to the UHS) ensures that core debris remains within the RPV and effectively precludes the potential for each of the postulated ex-vessel severe accident challenges.

Assessments of severe accident phenomena predict no CNV failure. However, even if the CNV were postulated to fail, there would not be a large release to the environment.

While derived considering internal initiating events, these insights are also generally applicable for internal floods, internal fires and external events. The passive heat removal phenomenon discussed above is dependent on only physical plant conditions and functions regardless of whether the scenario was caused by an internal initiating event or if an external event has occurred. The CNTS is protected from external events through the design of the system as well as protection provided by the structures in which it located. Therefore, the general insights summarized above are equally applicable to external events as well as internal events.

Table 19.1-32 summarizes these insights.

19.1.4.3 Level 3 Internal Events Probabilistic Risk Assessment for Operations at Power

The PRA Level 3 analysis is used to evaluate offsite consequences at a potential site. A Level 3 analysis has not been performed for design certification.

19.1.5 Safety Insights from the External Events Probabilistic Risk Assessment for Operations at Power

The external event hazards that may affect the NuScale risk profile are identified based on past studies and in a manner consistent with the requirements of ASME/ANS RA-Sa-2009. Once the hazards are identified for consideration, the guidance in ASME/ANS RA-Sa-2009 is used to implement a progressive screening process to identify which external events could be screened from detailed evaluation and those that required a quantitative hazard evaluation. The screening criteria are presented in Table 19.1-33. The table provides preliminary and bounding screening criteria using the approach discussed in Part 6 of ASME/ANS RA-Sa-2009.

Table 19.1-34 summarizes the external hazards identified for consideration in the NuScale PRA for operations at power. The table provides the screening disposition for each of the hazards.

The screening of some hazards was based on assumptions regarding siting requirements. A bounding analysis of high winds and external floods was performed and site characteristics should be compared to those assumed in the bounding analyses to ensure that the site is enveloped. The seismic hazard has been addressed by performing a seismic margin assessment (SMA). The external events that are not site-specific are internal fires and internal floods.

Section 19.1.5.1 through Section 19.1.5.5 address seismic, internal fire, internal flood, external flood and high-winds hazards, respectively.

COL Item 19.1-7: A COL applicant that references the NuScale Power Plant design certification will evaluate site-specific external event hazards (e.g., liquefaction, slope failure), screen those for risk-significance, and evaluate the risk associated with external hazards that are not bounded by the design certification.

19.1.5.1 Seismic Risk Evaluation

Evaluation of the risk due to seismic events for a NuScale plant is performed using PRA-based SMA. Section 19.1.5.1.1 describes this assessment and outlines the manner in which the SMA is performed. Section 19.1.5.1.2 summarizes the results obtained from the PRA-based SMA for the NuScale design.

The scope of the SMA is the evaluation of seismic fragilities for SSC associated with a single module. A ground motion representing high confidence of low probability of failure (HCLPF) is derived for each SSC. Accident sequences from the PRA are solved to produce the combinations of seismic and random failures (cutsets) that could lead to core damage and large releases. Cutset level and plant level HCLPFs are then derived using the MIN-MAX method.

The SMA covers full power and LPSD operating conditions and includes Level 1 (core damage) and Level 2 (large release) consequences.

19.1.5.1.1 Description of the Seismic Risk Evaluation

There are two main tasks associated with performing a PRA-based SMA: seismic fragility analysis (structures and components), and seismic plant response analysis (accident sequence analysis and plant level response). The following sections summarize the SMA approach:

- Seismic Analysis Methodology and Approach (Section 19.1.5.1.1.1).
- Seismic Input Spectrum (Section 19.1.5.1.1.2).
- Seismic Fragility Evaluation (Section 19.1.5.1.1.3).
- Systems and Accident Sequence Analysis (Section 19.1.5.1.1.4).

19.1.5.1.1.1 Seismic Analysis Methodology and Approach

The PRA-based SMA for the NPM (single module) is performed in accordance with the applicable NRC guidance from DC/COL-ISG-020 (Reference 19.1-56) and with the applicable PRA-based SMA guidance in Part 5 of ASME-ANS Ra-Sa-2009 as endorsed by RG1.200. As discussed in DC/COL-ISG-020, the purpose of a PRA-based SMA is to provide an understanding of significant seismic vulnerabilities and other seismic insights. Consistent with DC/COL-ISG-020, the seismic margin is evaluated with respect to a review level earthquake (RLE). The RLE spectral shape is defined relative to the certified seismic design response spectra (CSDRS) as provided in Figure 3.7.1-1, with a scaling factor of 1.67. The peak ground acceleration of the CSDRS is the safe shutdown earthquake (SSE).

19.1.5.1.1.2 Seismic Input Spectrum

Structure, system, and component fragility is referenced to the peak ground acceleration of the CSDRS, which is the SSE (0.5g).

Component and structural fragility calculations are evaluated with in-structure response spectra (ISRS) produced at relevant SSC locations using the CSDRS as input. Based on available component design information, ISRS is used in lieu of required response spectra for fragility calculations.

19.1.5.1.1.3 Seismic Fragility Evaluation

A seismic fragility analysis is completed as part of an SMA. Fragility describes the probability of failure of a component under specific capacity and demand parameters and their uncertainties. All SSC modeled in the internal events PRA were included in fragility analysis, with the exception of basic events that are not subject to seismically-induced failure (e.g., phenomenological events, filters, control logic components). No pre-screening was performed to establish a seismic equipment list (SEL) or safe shutdown equipment list (SSEL). The terminology "PRA-critical" is used to denote SSC that contribute to the seismic margin. Contributing SSC are determined by applying the MIN-MAX method and the screening assumption described in Section 19.1.5.1.2 and Table 19.1-40.

The HCLPF ground motion for PRA-critical structures and components modeled in the SMA are obtained by performing fragility analysis using the separation of variables and conservative deterministic failure margin (CDFM) methods, as endorsed by DC/COL-ISG-020. Separation of variables, described in EPRI 103959 (Reference 19.1-57), is a best-estimate methodology to determine SSC fragility parameters (median capacity, randomness, and modeling uncertainty) as a combination of several independently determined factors (e.g., strength, ductility). The fragility parameters are then used to calculate the HCLPF. The CDFM method, described in EPRI NP-6041-SL (Reference 19.1-21), uses conservative input parameters (e.g., seismic demands, material properties) to calculate the HCLPF directly. For non-critical components, fragilities are evaluated using generic capacity values and design-specific response spectra to calculate the demand.

The controlling failure mode of the structural events and their direct consequences are shown in Table 19.1-35. For components, seismic failures are either considered functional failures (all modes) or mapped to specific equivalent random failures (such as a valve failing to open on demand). Information for component fragilities is provided in Table 19.1-38.

Seismic Structural Events

Fragilities for structural failures are modeled as basic events in the SMA model with median failure accelerations and uncertainty parameters. For each structural fragility, boundaries are defined such that relevant seismically-induced failure mechanisms are accounted for (e.g., failures to supporting sections, intersecting structures, nearby structures). Seismically-induced structural failures are then assumed to lead directly to core damage and large release without opportunity for mitigation. This is a simplifying assumption for modeling catastrophic failure mechanisms. Structural events differ from component failures in that they do not correspond to a random event in the internal events PRA. In all cases, the consequences of structural events are assumed to lead to both core damage and large release without opportunity for mitigation. This is a simplifying assumption for modeling catastrophic failure mechanisms.

The selection of structural failures to model is based on a qualitative assessment of the external mechanisms that can damage the NPM. Structures selected for analysis meet one of the following criteria:

- Structures directly in contact with the NPM: This applies to the NPM base support and module lug support system;
- Structures directly connected to the module interface: The reactor bay walls, pool wall, and basemat; or
- Structures located above the module, where collapse could lead to physical damage to the module. These include the Reactor Building crane (RBC) and the bioshield.

Figure 1.2-5 provides perspective on the locations of structural failures included in the SMA.

Reactor Building Crane

The RBC is located over the reactor pool and is suspended by girders. It runs the length of the reactor pool and is used primarily for raising and transporting NPMs to and from the refueling bay.

The crane is designed with seismic restraints. As illustrated in Figure 19.1-42, bridge girder failure cannot lead to catastrophic collapse without failure of the bridge seismic restraints. Failure of the bridge seismic restraints is the controlling failure mode by comparison to yielding of the bridge girder itself. The bounding consequence of crane failure is a collapse of the crane structure, which is assumed to impact the top of the module, and lead to core damage and large release. This modeling simplification is conservative because the bioshield, CNV, and RPV integrity are not credited following a crane collapse.

Reactor Building

The fragility of the RXB as a whole is modeled by separate fragility analyses of each of the wall types, as well as the RXB roof, and basemat:

- the four exterior RXB walls
- the four RXB pool walls
- the RXB crane support structure
- the pool bay walls
- the RXB roof
- the basemat

The locations experiencing maximum loading (combined seismic and non-seismic) for each of the above groups of structures, were evaluated. Failure is assumed to lead to building collapse, core damage, and large release. The controlling failure mode is determined to be out-of-plane shear cracking at the base of the exterior east-west walls.

NuScale Power Module Supports

The NPM supports are comprised of two support interfaces between the NPM and the RXB: the NPM passive support plates assembly and the NPM lug restraint. The NPM passive support plates assembly provides lateral support to the NPM at the pool floor. The NPM lug restraint provides support to the NPM via interfaces with the RXB pool walls and the bay walls. The design of the NPM passive support plates assembly is discussed in Section 3B.2.7.3. The design of the NPM lug restraint is discussed in Section 3B.2.7.4.

Results of the fragility calculation for the NPM supports are shown in Table 19.1-35.

Bioshield

Each NPM is covered by a removable bioshield that rests over the module during normal operation. The bioshield consists of a concrete slab attached by anchor bolts to the bay walls.

During refueling, the bioshield of the refueled module is placed on top of an adjacent module. Any operating module, therefore, may have two bioshields stacked over it. A separate fragility calculation is performed for two stacked bioshields and is included in the SMA.

Potential bioshield failure modes were identified:

- Vertical bioshield failure;
- Horizontal shear flexure;
- Bay wall anchor bolt shear.

Bioshield failure is expected to cause the entire horizontal slab section to collapse on top of the NPM, causing core damage and a large release.

Vertical bioshield failure has been screened from analysis because of the bounded consequences of failure. The controlling failure mode would involve detachment from its lower supports against the bay wall, its upper connection to the horizontal bioshield slab, and then sufficient flexing of the bay walls to allow the vertical section to separate from the rest of the bioshield and twist inwards to strike the CNV. Because bay wall twisting and shear cracking failure is evaluated by a separate fragility calculation, this fragility is screened from the analysis.

Results of fragility calculations for bioshield failure modes are shown in Table 19.1-35.

Components

Similar to fragilities developed for structural failures, fragilities for component failures are modeled as basic events with median failure accelerations and uncertainty parameters. For each component fragility, component boundaries are defined such that relevant seismically-induced failure mechanisms are accounted for (e.g., anchorage failure, structural collapse affecting component function). Seismically-induced component failures are then mapped to existing random component failure modes from the internal events PRA. Seismic failures of components are modeled in one of two ways:

- By design-specific fragility analysis. This analysis method uses the material properties and geometry specified by design documents to model the component capacity. It uses ISRS data for the seismic demand to calculate the response and safety factors using the separation of variables method.
- By using NuScale-specific response factors derived from clipped ISRS, the methodology outlined in EPRI 103959, and generic spectral acceleration capacities developed from EPRI 3002000507 (Reference 19.1-59) and NUREG/CR-2680, NUREG/CR-3558, NUREG/CR-4659, and NUREG/CR-7040 (Reference 19.1-18, Reference 19.1-19, Reference 19.1-20 and Reference 19.1-25, respectively).

The first modeling approach is used for PRA-critical components, such as active components located inside the NPM.

For components located outside the NPM (e.g., diesel generators), or components that, if failed, would not directly affect safe shutdown, the second method was used. This allows for the use of design-specific ISRS data and generic spectral acceleration capacities to determine the component fragilities.

Components sharing common type, location, and elevation within a building are similarly impacted by earthquakes. Because of this, components sharing seismically relevant characteristics are grouped together. Seismic failures are assigned to groups named seismic correlation classes and are modeled as basic events within the SMA model. For the purposes of seismic correlation class grouping, components of the same type in the same building (or general area) with the same elevation class are considered 100 percent correlated. Individual seismic correlation classes are then treated as independent of other seismic correlation classes.

Table 19.1-36 lists the locations identified for grouping components into seismic correlation classes in the SMA model. Table 19.1-37 lists the component types used in the SMA and their descriptions. Table 19.1-38 contains characteristics for each seismic correlation class, including name, component type, location, and fragility parameters. The median seismic capacity for the seismic correlation class is chosen such that plant-specific information is utilized wherever possible in conjunction with available ISRS nodes. ISRS nodes and descriptions are provided in Table 19.1-39. Any ISRS node labeled as "Site" in the "Location" column of the table is referenced to ground acceleration from the CSDRS, rather than a location within the RXB.

Fragilities and High Confidence of Low Probability of Failure

The seismically induced failure probability of a component (fragility) is a function of its median capacity (A_m), median capacity uncertainty (β_U), and fragility randomness (β_r).

Separation of variables fragility analysis was performed on PRA-critical SSC and SSC for which the NuScale Power Plant design is different from operating plants. These SSC are structures or active components inside the NPM. Generic capacities and NuScale-specific response factors were used for components either located outside the module or components that do not show a substantial impact on the plant risk profile.

For generic capacity fragility calculations, a spectral acceleration capacity was used. This capacity describes the spectral acceleration level (in g) where a component is expected to fail at a 50 percent probability. To convert this value to a peak ground acceleration (PGA)-grounded capacity, the nominal value is divided by a demand response factor.

Demand response factors convert peak ground accelerations to the accelerations experienced by components at different locations. For components assigned generic capacities, the local equipment seismicity is scaled up from the peak ground acceleration by using a demand response factor. This factor is calculated by dividing the peak clipped spectral accelerations by the corresponding CSDRS values in the frequency range of interest, and selecting the maximum ratio. As a result, the implicit safety factors used in the evaluation of the generic spectral acceleration capacity are compared with the design-specific ISRS in evaluating SSC fragility.

In fragility development summaries and implementation guides, fragility is calculated based on floor response. This means SSC fragility is referenced to the peak ground acceleration of the seismic input spectrum (CSDRS), the SSE (0.5g). Component fragility is then determined as a function of equipment design loads, equipment placement, and site response.

The HCLPF is then defined as the acceleration level where there is a 95 percent confidence of less than 5 percent failure probability. The HCLPF can also be approximated as the acceleration with a one percent probability of failure on the mean fragility curve.

19.1.5.1.1.4 Systems and Accident Sequence Analysis

Plant response analysis maps the consequences of seismic initiators combined with seismic and random failures. This analysis produces event trees with seismically induced initiating events, component and structural events, and non-seismic unavailability.

The SAPHIRE computer code is used for quantification of the logic models utilized in the NuScale SMA.

Seismically-Induced Initiators

Plant response after a seismic event is mapped using seismically-induced initiating events, as illustrated in Figure 19.1-16. These events are modeled using similar logic to corresponding random internal events PRA initiating events. Plant response is modeled only for earthquakes with a non-negligible probability of causing a reactor trip.

The seismic hazard for the NuScale design SMA is partitioned into fourteen seismic event trees. The underlying logic for each event tree is identical; however, each event tree represents a different ground motion acceleration (each seismic event tree represents a portion of the ground motion range from 0.005g to 4.0g). In the SMA, the use of multiple ground motions provides insights into the relative contributions of both seismic and random failures at different ground motions. Figure 19.1-16 is a representative seismic event tree, corresponding to a range of peak ground accelerations from 0.005g to 0.1g. The thirteen remaining event trees represent ground motion ranges spaced accordingly up to 4.0g (0.1g to 0.2g, 0.2g, to 0.4g,..., 2.0g to 2.5g,..., 3.0g to 4.0g). Component failure probabilities are then evaluated at the mid-point of each range (0.0525g for a range of 0.005g to 0.1g, for instance). In each event tree, the initiating event frequency is set to unity in the SMA to allow for an evaluation of the conditional probability of core damage and large release at each ground motion.

Seismic event trees are initiated by the failure of a single component or structural event. Sequences containing these failure events transfer from Figure 19.1-16 to other seismic event trees that represent plant response to breaks outside containment (Figure 19.1-17), LOCAs inside containment (Figure 19.1-18), SGTFs (Figure 19.1-19), and losses of offsite power (Figure 19.1-20). Figure 19.1-17 and Figure 19.1-19 include a transfer to a loss of DC power event tree (Figure 19.1-20a) to reflect battery depletion at 24 hours. These trees are modified from existing internal events PRA event trees to remove credit for the availability of AC power or for offsite power recovery.

Offsite power loss is the most likely induced initiator (a LOOP would occur from lower ground motions than are expected for other induced initiators). As such, credit for offsite power has been removed from the seismic event trees during consideration of the other seismically-induced initiating events (i.e., LOCAs inside and outside containment, SGTFs, and structural failures). In the event of a LOOP, as illustrated in Figure 19.1-20, credit is considered for the CTG and BDGs. If either survives along with the DC buses, the response to a general reactor trip is considered, as indicated by the transfer "TGS---TRAN--NPC-ET" (Figure 19.1-11). If neither survives, offsite and onsite power has been lost and a station blackout exists. Because backup power is fragile relative to the valves and steam generator tubing for the other seismically-induced initiating events, the existence of power in those situations is not considered. If backup power is unavailable due to the seismic event (Sequence 5 of Figure 19.1-20), a transfer is made to the internal event LOOP event tree (Figure 19.1-9), as indicated by the transfer "EHVS--LOOP----ET".

The lowest threshold for seismically-induced initiators is a LOOP, which has a median failure capacity of 0.3g. A seismically-induced LOOP credits AC power recovery from the CTG or the BDGs (A_m = 0.65g for both). If both the turbine and the diesels fail to restore power, the ECCS valves open after the DC power holding the valves closed is removed, and the DHRS or the reactor safety valves (RSVs) depressurize the RPV to the point where the IAB allows the ECCS valves to open.

Seismically-induced SGTF is then modeled with a median failure capacity of 2.9g (failure of tube supports leads to failure). The logic is mapped similarly to a randomly occurring SGTF. Other induced failures include LOCAs inside containment (e.g., spurious opening of RSVs, ECCS valves), breaks outside containment (e.g., CVCS regenerative heat exchanger failure) and (most severely) structural events.

Seismic Accident Sequences

In developing the SMA, system fault trees also are modified. Seismic failure modes for structures and components are incorporated by inserting transfer gates for each seismic correlation class into each existing fault tree alongside existing randomly occurring events (failure modes). This ensures that cutsets produced by evaluating the SMA model contain both random and seismic failures. Events representing failure modes without a seismically-relevant equivalent remain in the SMA. Once complete, the SMA is representative of seismic failures of different component groups located throughout the plant as well as original random failures. Updated fault tree logic is transferred through the logic of each seismic event tree. Because fourteen event trees are utilized to define the seismic hazard, the appropriate ground motion demand corresponding to each event tree is applied with "house" events. These events coincide with the ground motion acceleration modeled with each individual seismic event tree. Project level linkage rules are used to turn house events “true” or “false” in order to solve each seismic event tree at the corresponding ground motion.

In the seismic event trees, sequences involving core damage end with "Level2-ET." This indicates a transfer to the containment event tree (Figure 19.1-15), which contains the radionuclide release categories.

In summary, the SMA event trees terminate in:

- OK: No core damage
- Transfer to another event tree
- Transfer to the Level 2 event tree.

19.1.5.1.1.5 Effects of Seismically Failed SSC on Surviving SSC

Potential failures of seismically qualified components due to physical interaction with a nonseismically qualified SSC are evaluated consistent with the definition of “spatial interaction,” as defined by the ASME/ANS PRA standard:

a) Proximity effects

   Safe shutdown of an NPM is ensured by opening of the RSVs, combined with successful passive ECCS valve operation, when there is not a loss of coolant outside the containment boundary. These components have very high seismic capacities and are physically shielded from nonseismically qualified SSC by the seismically qualified CNV. These components fail safe on loss of power and are not located in proximity to nonseismically qualified components.

b) Structural failure and falling

   The potential for failure and falling interactions between surviving seismically qualified SSC and seismically failed SSC is limited by the nature of the NuScale design. The NPM is physically protected by the pool water, pool walls, bay walls, and, during power operation, the bioshield. Seismically-induced damage to the bay walls and bioshield is modeled in the SMA; the SMA demonstrates that these structures have higher HCLPF values than potential components that could fail due to a seismic event. Thus, these structures would provide a physical barrier between potentially failed components and the NPM.

   When the bioshield is removed from an operating bay prior to NPM transport for refueling, piping penetrations atop the CNV, as well as the DHRS piping and heat exchangers on the side of the NPM, could be impacted by a falling or swinging object. However, the module is shut down and flooded prior to its bioshield being removed. In this configuration, safe shutdown is maintained by conduction from the RPV through to the CNV and reactor pool.

c) Flexibility of attached lines and cables

   Seismically-induced pipe breaks outside containment are modeled in the SMA and encompass the effects of pipe leaks caused by stresses induced by structural displacements or failing objects.

   The NPM is not precluded from achieving safe shutdown as a result of a loss of electrical power or signaling logic. As such, the SMA model does not credit systems requiring electrical power at ground motion levels sufficient to cause both loss of offsite power and failure of backup power sources.

19.1.5.1.2 Results from the Seismic Risk Evaluation

Seismic risk is evaluated in terms of a plant-level HCLPF g-value and a review of SMA accident sequence cutsets for risk insights.

The plant-level HCLPF is determined by examining the cutset results from all fourteen seismic event trees. All cutsets are reviewed to screen those that are not relevant to the determination of the plant-level HCLPF. Per the MIN-MAX screening assumption addressed in Table 19.1-40, cutsets are screened out if the combined probability of random failures is less than one percent. This is appropriate because the conditional probability of failure corresponding to the HCLPF (i.e., given an earthquake ground motion equal to the plant-level HCLPF) is required to be greater than or equal to one percent (using the mean fragility curve). Therefore, even if all seismically induced failure probabilities of a particular cutset were 100 percent, the probability of core damage from non-seismic random failures must be greater than or equal to one percent for the cutset to be a relevant contributor to the HCLPF calculation. If the combined random failure probability of the cutset is below one percent, the cutset would not be a relevant contributor to the HCLPF calculation. The MIN-MAX method is then applied to the remaining cutsets to determine the SSC with the limiting HCLPF for each cutset. The limiting SSC identified for each cutset contributes to the seismic margin. Of all the seismic margin contributors, the SSC with the smallest HCLPF value provides the plant-level HCLPF. To demonstrate acceptably low seismic risk at the design certification stage, as indicated by DC/COL-ISG-020, the resultant plant-level HCLPF must be greater than or equal to 0.84g, which is the plant-level HCLPF requirement of 1.67 times the SSE.

All cutsets associated with the corresponding peak ground acceleration HCLPF g-value are reviewed for seismic risk insights. That is, cutsets are not screened from the review process so that all cutsets are considered for potential risk insights.

Plant Level HCLPF

Implementation of the screening process described above results in a plant-level HCLPF for the NuScale design of 0.88g. Structural events are the leading contributor to the seismic margin because of their immediate consequences and relatively low PGA-grounded median capacities as compared to component failures. Table 19.1-35 summarizes the fragility analysis for each of the structural events. Each of the structural event parameters has been calculated using design specific fragilities. The SMA assumes that failure of major structures leads to sufficient damage to the modules such that core damage and a large release would result.

Significant Sequences

This section provides brief descriptions of the significant contributors to risk as determined by a review of all SMA accident sequence cutsets.

Structural events are by far the leading contributor to the seismic margin. The bounding structural event is weldment failure on the crane bridge seismic restraints, which is modeled to lead directly to RBC collapse, core damage and large release.

A single SMA sequence contains all structural events and represents 99.8 percent of the large release conditional failure probability after a HCLPF-level earthquake. In accordance with the MIN-MAX method, the lowest HCLPF value between cutsets in the same sequence is controlling. This is why only the RBC event HCLPF shows up at the sequence level.

Risk Significance

Potentially risk significant structures, components and operator actions are discussed below.

Significant Structural Failures

Table 19.1-35 lists the structures and associated failure modes for which structural fragilities are calculated. All structural fragilities are assumed to lead directly to core damage and large release. As such, all structural fragilities modeled in the SMA contribute to the seismic margin.

Significant Component Failures

The NuScale unique passive safety features limits the risk associated with failure of active components (such as pumps, compressors and switches) to perform during or after a seismic event. In addition, mitigating systems are largely fail safe, resulting in their actuation on loss of power or control. As such, very few component failures have the potential to contribute to seismic risk.

Moreover, component fragilities reported in Table 19.1-38 show very low seismic failure probabilities. The fail-safe design of PRA-critical components means that the only credible seismic failures of the valves required to achieve safe shutdown involves physical deformation of the valves themselves, which only occurs under extreme stresses. As a result, component failures (either seismic or random) do not contribute significantly to the potential for core damage or releases following a seismic event. Rather, similar to the internal events PRA, CCF of key functions have the most potential for controlling risk, for example, common cause events leading to failure of reactor trip, ECCS valve CCFs and failures to isolate containment (in response to seismically induced SGTF or breaks outside containment).

Significant Operator Actions

The SMA model implements HFE probabilities in the same manner as the internal events PRA. Individual system-specific HFE events are first inserted into cutsets using sequence logic; no seismic-specific operator actions were added to the SMA models.

The internal events human error probabilities of each HFE in the SMA models are multiplied by a factor of 5 for the SMA to account for the assumed "extreme stress" environment associated with a seismic event (per SPAR-H methodology, NUREG/CR-6883). This is performed regardless of ground motion, meaning the HEPs at lower ground motion levels are conservative.

The NuScale design incorporates passive safety features, requiring no operator intervention to initiate or maintain operation. As a result, seismic cutsets containing HFEs also include other seismically-induced or random failures that limit the importance of operator actions. Recovery actions are not credited in the SMA. Although the HEPs are increased for the SMA, operator actions do not play a substantial role in contributing to, or mitigating, the conditional core damage probability (CCDP) results for the SMA.

Key Assumptions

Table 19.1-40 summarizes the key assumptions associated with the SMA.

Uncertainties

Parameters representing aleatory and epistemic uncertainty are used directly in evaluating the plant-level HCLPF. Each SSC in the SMA is modeled with a lognormal uncertainty distribution using randomness (β_r) and uncertainty (β_u) parameters. For PRA-critical SSC that are the subject of detailed fragility evaluations, uncertainty parameters are also assigned to each sub-factor that contributes to the overall safety factor. The determination of these uncertainty parameters for each fragility calculation sub-factor is performed in accordance with EPRI TR-103959 and EPRI TR-1019200 (Reference 19.1-58).

The SMA contains uncertainty from many sources, including:

- Ground motion variability
- Uncertainty in soil-structure interaction
- Uncertainty in structural response factors
- Spectral shape (motion frequency) uncertainty
- SSC capacity uncertainty (material strength and inelastic energy absorption)

The modeling of seismic uncertainty is divided into two composite factors, β_r and β_u. Both β_r and β_u are included in each seismic event, along with the median capacity A_m.

In addition to parametric uncertainty, the completeness of the selection of SSC is a consideration in the performance of the SMA.

With respect to evaluation of structures, the SMA specifically considers the capacity and effects of failure of:

- Structures directly in contact with the NPM
- Structures directly connected to the module interface
- Structures located above the module

After the plant-level HCLPF is determined, uncertainty analysis is performed by setting the seismic demand to the HCLPF level, sampling each event in the SMA (fragilities and random events), and re-calculating the CCDP. Results are compared to the HCLPF definition (95 percent confidence of less than 5 percent probability of failure or 1 percent failure probability on the mean fragility curve).

The CCDP uncertainty distribution demonstrated agreement between the controlling failure HCLPF (seismic restraint weldment) evaluated with the MIN-MAX method. Results from the uncertainty analysis confirm that the HCLPF value is reasonable.

Sensitivity Studies

No sensitivities were performed for the SMA.

Key Insights

The SMA shows that the current design meets the regulatory HCLPF requirement of 1.67 times the SSE (i.e., 0.84g). A structural failure sequence involving collapse of the RBC is the most important contributor to the seismic margin (and such collapse is relevant only if the RBC is under load within the operating module area of the RXB pool). Other sequences include one or more random failures after the seismic event. These failures occur among the same general components and sequences that lead to core damage in the internal events PRA. An examination of operating nuclear power plant data shows that the seismic survivability of the NuScale design is high because of the low core damage contribution from losses of offsite power. The only significant cutsets contain structural events leading directly to core damage and large release. All other seismically-induced initiating events require multiple seismic or common-cause random failures for core damage. This is largely a consequence of the low degree of reliance on electrical power for achieving safe shutdown. The passive actuation features of safe shutdown functions also imply a low degree of reliance on operator intervention to mitigate a severe accident.

19.1.5.2 Internal Fires Risk Evaluation

An internal fire probabilistic risk assessment (FPRA) for at-power operations has been performed for a single NuScale module. Section 19.1.5.2.1 describes key aspects of the evaluation including methodology and modeling. Section 19.1.5.2.2 provides key results including the CDF, LRF, and CCFP due to internal fire events.

19.1.5.2.1 Description of Internal Fire Risk Evaluation

The internal fire risk evaluation addresses the potential fire events that may originate within the plant boundary and that affect a single module. The FPRA is based on the Level 1 internal events PRA model, which is supplemented by fire-specific failure modes. Because detailed layout information (e.g., cable routing) is not available, detailed fire modeling is not performed.

The internal FPRA applies the methodology provided in NUREG/CR-6850 (Reference 19.1-42); the methodology consists of 16 interrelated tasks. The tasks are implemented as summarized in the following discussion. The discussion addresses assumptions, estimation of fire initiation frequencies, and module response.

Task 1: Global Boundary and Partitioning

For the FPRA, the initial activity associated with partitioning of the module fire areas is establishing the "global" boundary of a module. The intent of this activity is to identify locations that could contribute to the fire risk. This activity is performed by review of a 12-module site plan based on the locations of SSC that are associated with normal or emergency reactor operating or support systems.

Partitioning of the locations of potential fire risk is used to define "fire compartments." Fire compartments are defined in NUREG/CR-6850 as well defined volumes within a plant that are expected to substantially contain the effects of a fire. Fire "areas" that are defined in the fire hazards analysis (FHA), presented in Appendix 9A, are retained as fire compartments without further partitioning. Thus, for the FPRA, fire compartments are defined with the following criteria:

- Fire compartments for buildings where fire areas are defined in the FHA, are mapped one-to-one with fire areas.
- The entire building for buildings that are not within the scope of the FHA,
- Other elements, which are not located inside of a building, are broadly grouped into one fire compartment, unless substantial fire barriers are identified that separate the element from adjacent areas.

Task 2: Component Selection

Components considered in the FPRA are determined by consideration of the Level 1 internal events PRA discussed in Section 19.1.4 and the Fire Safe Shutdown Plan presented in Appendix 9A. Table 19.1-42 summarizes the applicability of the initiating events used in the internal events PRA to the FPRA; components associated with mitigation of these initiating events were evaluated in the FPRA. The Fire Safe Shutdown Plan generally requires the same equipment as needed to respond to a general reactor trip. However, the plan also considers challenges to safe shutdown that result from multiple spurious operations (MSOs). The MSO analysis is consistent with the approach outlined in NEI 00-01, Rev 2 (Reference 19.1-43). Table 19.1-41 identifies the applicable MSOs derived from the generic list provided in NEI 00-01, Rev 3 (Reference 19.1-44).

Task 3: Cable Selection

The intent of this task is to establish which cables, if damaged by a fire, are capable of preventing a component identified in Task 2 from performing its function. In general, these failures result either from cable damage causing a loss of control (loss of control or motive power) or by causing spurious operation of the component.

Detailed associated cable configuration and routing information are not established for design certification. However, components identified in Task 2 are controlled by one or more of the following control systems:

- module control system (MCS), which uses fiber optic cable

- the plant control system (PCS), which uses fiber optic cable
- the MPS, which uses fiber optic and copper cable
- the plant protection system (PPS), which uses fiber optic and copper cable

The passive nature of the module safety systems generally reduces the effect that a fire can have on a safety component because a loss of control or power to the component would result in the component failing in the desired position, rendering it nominally available to perform its safety function. Thus, a minimal number of control and motive power supplies is needed for component operation; specifically, the only equipment that requires control or motive power in the context of the FPRA is the equipment associated with establishing a makeup path through the CVCS and CFDS makeup lines and the ECCS valves from the perspective that a fire may result in an ECCS demand for reasons other than a response to a LOCA.

Given the required components and associated component control and power supply, a cable routing is assumed based on physical location of equipment and engineering judgment.

Task 4: Qualitative Screening

This task identifies fire compartments that can be demonstrated to have little risk significance without quantitative analysis. Fire compartments are screened if:

- The compartment does not contain equipment (and their associated circuits) identified in Tasks 2 and 3, and
- The compartment is such that fires in the compartment do not lead to:
  - An automatic trip, or
  - A manual trip as specified in fire procedures or plans, emergency operating procedures, or other plant policies, procedures or practices, or
  - A mandated controlled shutdown as prescribed by Technical Specifications because of invoking a limiting condition of operation.

Task 5: Fire-Induced Risk Model

The fire-induced risk model illustrates the module response to a potential fire. The starting point of the model is an assessment of potential initiating events associated with a fire. The internal events PRA was reviewed to identify faults that could be induced by a fire. Table 19.1-42 summarizes this review. For example, as indicated in the table, the potential for a fire to induce pipe breaks or vessel failures is judged to be not credible, which eliminates internal events initiators such as SGTF (IE-MSS---ALOCA-SG-) from consideration in the FPRA.

The resulting initiators can be categorized based on common characteristics in terms of effect on a module. If a fire has the potential for causing more than one type of event, it is assumed to cause the most serious limiting challenge based on the following ranking:

- Fire-Induced transient: This is the base case for internal fire events. Two of the initiating events from the internal events PRA that can be induced by a fire are transients with and without support systems available.
- Fire-Induced LOOP: This case is a fire that results in a loss of the normal AC power. The event progression is similar to the LOOP initiator in the internal events PRA except that credit is not taken for the recovery of offsite power.
- Fire-Induced ECCS demand: This case is an extension of the transient case where there is a fire-induced failure that also actuates the ECCS valves. This event also includes initiating events caused by the loss of DC power.
- Fire-Induced LOCA inside containment: This case is an extension of the transient case where there is a spurious operation signal sent to the CVCS makeup pumps resulting in the potential to overpressurize the RPV and challenge the RSVs.

The fire compartments identified in the FHA that were not screened in Task 4 are mapped to the initiating events based on the failures that may be caused by fire damage to equipment or associated cable in the compartment. Twenty-nine fire initiating events are identified, as summarized in Table 19.1-44. The fire initiating events are then mapped to the internal events PRA initiating events as indicated in the 4^{th} column of Table 19.1-44. If more than one initiator could be associated with a fire, the most limiting challenge is assumed to occur using the following priority:

1) Fire-Induced LOCAs inside containment are the most limiting given that DHRS actuation is not adequate to avoid core damage. ECCS actuation is needed but is not part of the initiating event.

2) Fire-Induced ECCS demands are the second most limiting given that DHRS actuation is not adequate to avoid core damage. ECCS actuation is needed and is part of the initiating event.

3) Fire-induced LOOP are the next most limiting event. DHRS cooling is potentially compromised by an incomplete ECCS actuation, which can occur after the EDSS module-specific (EDSS-MS) battery depletion.

4) Fire-induced transients are the least limiting because they are mitigated by the widest array of systems, including the DHRS.

There is one transfer event tree corresponding to each of the 29 fire initiating events. Each of the transfer trees has a similar structure to one of the trees provided as Figure 19.1-21 through Figure 19.1-24 based on which of the four fire initiator types is applicable. As with the internal events PRA, fault trees, supplemented by additional fire failure modes are used to quantify the top events. Fire-induced failures are considered for the components identified in Task 2. The failures of "fails due to fire," "spurious hot short," and "spurious hot short, short fails to clear" are added to the internal events fault trees to reflect the additional failure modes associated with a fire.

Task 6: Fire Ignition Frequencies

Potential fire ignition sources are identified by review of the general arrangement drawings. Frequency estimates for the ignition sources were developed using the generic frequencies provided in NUREG-2169 (Reference 19.1-45). In NUREG-2169, fire ignition frequencies are presented by grouping failures according to location and equipment type or "bins" as summarized in Table 19.1-43. The bins that are applicable to the design are indicated in the table. The table also indicates the total number of each fixed ignition source that is associated with a 12-module plant and the NUREG-2169 generic frequencies. The fixed ignition frequencies for each fire compartment used in the FPRA are developed from the generic frequencies considering the number of components and their locations to determine the portion of the generic frequency allocated to each compartment. The transient ignition frequencies for each fire compartment are based on the NUREG-2169 generic frequencies. The initiation frequencies for each of the 29 fire initiating events, as provided in Table 19.1-43 were developed from the summation of ignition frequencies associated with the fire compartments assigned to each fire initiating event.

Task 7: Quantitative Screening

Quantitative screening of fire compartments or scenarios based on their risk contribution is not included in the FPRA. Areas that include components associated with the FPRA have been evaluated.

Task 8: Scoping Fire Modeling

Screening may be performed to screen out fixed ignition sources that do not pose a threat to targets within a specific fire compartment. The FPRA does not screen ignition sources.

Task 9: Detailed Circuit Failure Analysis

A simplified approach to detailed circuit analysis is implemented in the development of the FPRA model. Two general considerations were given to potential circuit failures: material of construction of fire-affected cable and separation requirements of RG 1.189 as required by the FHA.

With regard to cabling material, fiber optic control cables are not considered to be capable of causing a spurious component operation, that is, a "hot short" as described in NEI 00-01. Therefore, potential fire damage to fiber optic cable is modeled only as a loss of control of the component controlled by the cable. Fire-induced spurious operation of circuits involving copper cabling is considered in the model.

Separation of redundant safe shutdown equipment and cabling is achieved as discussed in Fire Safe Shutdown Plan, described in Section 9A.6.

Task 10: Circuit Failure Mode Likelihood Analysis

This task considers the relative likelihood of various circuit failure modes. Fire-induced failures other than spurious actuation are assigned a probability of 1.0. However, for spurious operations, circuit failure mode likelihood is determined by several factors: the type of component that is being controlled, the type of material composition of control cabling, and the control power sources are critical factors in establishing spurious failure probabilities.

Components requiring consideration for spurious operation are identified in Table 19.1-41; the components involve failures that can be categorized as ungrounded DC control circuits or temperature sensitive electronics.

Spurious operations of solenoid-operated valves powered by ungrounded DC supplies, have been assigned a probability of 7.7E-2 based on NUREG/CR-7150 (Reference 19.1-46). This probability is applicable to solenoids which require double break hot shorts from intra-cable and ground fault equivalent sources. If a spurious operation can be withstood for longer than 7 minutes, a value of 2.2E-2 is assigned as the probability for the hot short to persist for longer than 7 minutes, based on NUREG/CR-7150; this probability allows for the possibility for a hot short to clear after it occurs. No credit is taken for hot shorts to clear when they affect the inventory in the DHRS heat exchangers. If the feedwater lines and main steam lines do not isolate quickly enough, the inventory in the DHRS heat exchangers may be lost resulting in a failure of that system. Alternatively, failure to isolate the main feedwater pumps could result in overfilling the DHRS heat exchangers which fails the system.

The CVCS makeup pumps are controlled by the module control system primarily by fiber-optic cables, which are not susceptible to fire-induced spurious operation. However, spurious operation of these pumps is considered in the area where the pumps and their associated control cabinets are located because of the possibility of a fire or smoke damaging the controller(s) for the components. In this situation, the probability of spurious operation has been assumed to be 1.0.

Task 11: Detailed Fire Modeling

Fires postulated in a NuScale design are grouped into the following categories and evaluated with assumptions regarding fire growth:

- General Compartment: Within individual fire compartments, credit is not taken for automatic or manual fire suppression. If fire growth occurs, these fires are conservatively assumed to damage the equipment in the room. The potential for fire growth, (i.e., the probability of a fire spreading) was modeled with probability distributions.
- Main control room: Fires in the MCR, including fires affecting the main control board, are conservatively assumed to damage the equipment in the room. Should a fire result in conditions that challenge control room habitability or equipment controls, operators can take control of the module from outside of the MCR.

- Multi-Compartment: A multi-compartment fire is a fire which originates in one fire compartment and subsequently spreads into a second compartment due to the failure of a fire barrier. The frequency of a multi-compartment scenario is computed as the product of the ignition frequency, the severity factor, the probability of non-suppression, and the fire barrier failure probability.
  - Ignition frequency: If fire growth occurs, ignited fires in the originating compartment are conservatively assumed to result in a challenge to fire compartment boundaries, such as by the formation of a hot gas layer.
  - Severity factor: Similar to single compartment scenarios, a fire growth factor is used to characterize fire growth.
  - Probability of non-suppression: Given that it is both assumed and necessary that each ignited fire progresses to the point that a hot gas layer is formed in order to progress into a multi-compartment scenario, a factor of 0.01 is judged to be a conservative probability of non-suppression. Each fire compartment is protected by a reliable suppression system that is adequate for the unique fire hazards in the compartment; this factor is intended to capture both the automatic and manual suppression capabilities.
  - Fire Barrier Failure Probability: Once a fire produces a hot gas layer, the last feature considered in developing a multi-compartment fire scenario frequency is the failure probability of the fire barriers separating adjacent compartments. Fire barriers include various features including fire doors, penetration seals, fire walls, and other structures. Given the uncertainty associated with the number of fire barrier penetrations, this probability has been modeled with a screening value of 0.1 using a lognormal distribution with an error factor of 10 to conservatively model the potential for fire propagation.

Task 12: Fire Human Reliability Analysis

There are no additional operator actions postulated to respond to a fire beyond those that are considered in the internal events PRA model (failure to initiate manual suppression efforts is evaluated as part of the non-suppression factor discussed in Task 11). For the FPRA, the "post-initiator" actions identified in Table 19.1-14 are included in the model with the exception of "CVCS--HFE-0002C-FOP-N," which is not applicable because use of CVCS injection during a partial loss of DC power is not credited in the FPRA. The method of evaluating the modeled operator actions is the same as used for the internal events PRA. The timing, stress, or complexity of modeled actions in the FPRA do not result in a difference in the evaluation of the operator action HEPs applicable to the internal events PRA because the actions are already modeled as "high stress" in the internal events PRA.

Task 13: Seismic-Fire Interactions

A qualitative assessment of the risk associated with a seismically induced fire has been performed consistent with NUREG/CR-6850. A planned shutdown using safety-related equipment would mirror a shutdown following a fire alone. No fire hazards unique to seismic events were identified; the most likely source of a seismically induced fire in the RXB or Control Building (CRB) is a fire originating in an electrical cabinet. The fire protection system is robustly designed in accordance with NFPA standards, as described in Section 9.5.1. Safety related equipment and equipment credited in the safe shutdown plan are protected from flooding caused by spurious actuations of the fire suppression system or breaks in fire suppression system piping. There are generally multiple entrance and egress points to support manual firefighting activities.

Task 14: Fire Risk Quantification

The fire scenarios postulated were quantified using the SAPHIRE code with a truncation frequency of 1E-15, as was done with the internal events PRA.

Task 15: Uncertainty and Sensitivity Analyses

Analogous to the internal events PRA model, parametric and modeling uncertainties are evaluated for the FPRA. The SAPHIRE code is used to perform parameter uncertainty analysis. The uncertainty in the FPRA risk metrics are characterized by various percentiles of the underlying probability distributions, such as 5^{th}, 95^{th} and mean values. The uncertainty results are calculated for the model using Latin Hypercube sampling. Model uncertainty arises because different approaches exist to represent module response to a fire even if necessary, these uncertainties may be addressed through sensitivity studies using different models or assumptions.

Task 16: Documentation

Documentation of the FPRA has been performed and maintained consistent with the guidance in ASME/ANS RA-Sa-2009.

19.1.5.2.2 Results from the Internal Fire Risk Evaluation

This section provides results of the FPRA for full-power operation of a single module. Risk metrics and insights are presented. Uncertainties and sensitivity studies associated with the results are discussed.

Core Damage Frequency for Internal Fires

The mean value of the CDF for a module due to internal fires is calculated to be 9.7E-10 per mcyr; the 5^{th} and 95^{th} percentile values are 7.4E-12 per mcyr and 3.1E-09 per mcyr, respectively.

Large Release Frequency for Internal Fires

The mean value of the LRF for a module due to internal fires was calculated to be 4.3E-11 per mcyr; the 5^{th} and 95^{th} percentile values are 8.9E-14 per mcyr and 1.4E-10 per mcyr, respectively.

Conditional Containment Failure Probability for Internal Fires

The CCFP for a module due to internal fires is 0.05.

Significant Core Damage and Large Release Sequences

There are numerous sequences contributing to the core damage frequency, with each being a relatively small contributor. The most significant sequences involve failures of the ECCS, including both random and fire-induced failures. The ECCS is demanded through both spurious actuation as the initiating event and as a mitigation function. A LOCA results if an RSV is demanded and the RSV fails to close. Core damage occurs following a failure of an operator to establish RCS makeup from the CVCS.

The LRF is dominated by a multi-compartment scenario that results in a failure of both divisions of ESFAS. Given failures of ESFAS, DHRS is not available for heat removal. Random CCF of both RSVs results in RPV overpressurization which cannot be mitigated by CFDS and leads to core damage. With both divisions of CIVs failed, these sequences progress to a large release.

Significant Cutsets

Table 19.1-45 provides the cutsets that contribute more than one percent of the CDF and LRF associated with an internal fire. The table indicates that the internal fires risk is dominated by fire-induced transients and induced ECCS operation. The most significant cutsets for CDF involve failure of ECCS vent or recirculation valves to function successfully. The most significant cutsets for LRF involve failure to isolate containment due to a multi-compartment fire affecting both ESFAS divisions.

Risk Significance

Applying the methodology referenced in Section 19.1.4.1.1.9, the following SSC are identified as risk significant candidates in the FPRA, as summarized in Table 19.1-64:

- ECCS (reactor recirculation valves and reactor vent valves)
- RSVs
- CVCS containment isolation valves
- MPS

No human actions are identified as risk significant.

Key Assumptions

Table 19.1-46 summarizes the key assumptions associated with the FPRA.

Uncertainties

Parameter uncertainty is characterized by probability distributions associated with the calculated results. Section 19.1.4.1.2 identifies sources of uncertainty in the internal events model. Model uncertainties that are unique to the internal fire PRA include the initiating event frequencies (e.g., fixed and transient ignition sources) and lack of design detail on protective and mitigative features (e.g., cable routing, fire suppression). Model uncertainties associated with the internal fire PRA are addressed with assumptions or sensitivity studies as indicated in the following section.

Sensitivity Studies

Given the lack of detailed spatial data regarding fire compartment layout, the growth of fires is modeled with wide probability distributions. To characterize the significance of this uncertainty, two sensitivity studies are performed that evaluate changes in SSC risk significance as the potential for fire growth is varied.

In the first sensitivity case, fire growth is minimized such that the modeled fires grow to the point of causing a reactor trip, but do not damage other mitigating equipment. In this case, the CDF and LRF are reduced as compared to the base case FPRA results; the dominant core damage sequence results mirror those from the transient initiators in the internal event model. The DHRS also becomes risk significant.

In the second sensitivity case, fire growth is maximized such that the modeled fires grow to the point where they damage all targets in a given fire compartment or multiple compartments in the case of a multi-compartment fire scenario. In this case, the CDF and LRF increase in comparison to the base case, but remain several orders of magnitude smaller than safety goals. This sensitivity case shows a significant increase in the relative significance of the fire-induced LOOP sequences and the multi-compartment scenario that fails both divisions of ESFAS.

Key Insights

The FPRA results show that even using conservative and bounding assumptions, the risk from a fire is extremely low, indicative of the passive features of the NuScale Power Plant design.

19.1.5.3 Internal Flooding Risk Evaluation

Consistent with ASME/ANS RA-Sa-2009, an internal flood is considered an external hazard, but it is a flood that is initiated from within the plant boundary. An internal flooding PRA for full power operations has been performed for a single module. Section 19.1.5.3.1 describes key aspects of the evaluation including methodology and modeling. Section 19.1.5.3.2 provides key results including the CDF, LRF, and CCFP due to internal flood events.

19.1.5.3.1 Description of Internal Flooding Risk Evaluation

The scope of the internal flooding evaluation is potential events originating within the plant boundary; such events include pipe breaks, storage tank rupture and heat exchanger failure. The internal flooding PRA is based on the Level 1 internal events PRA model supplemented by flood-specific modeling assumptions. The evaluation is based on information at the design stage; thus, assumptions and bounding modeling approaches are used to assess internal flood risk.

The internal flooding PRA applies the methodology provided in Part 3 of ASME/ANS RA-Sa-2009 with consideration of the review clarifications provided in DC/COL-ISG-028. The methodology consists of five elements. The following discussion addresses these elements and summarizes assumptions, estimation of flood initiation frequencies and module response. The elements of the internal flooding evaluation are part of an iterative process that is used to develop risk metrics. As such, the totality of information resulting from each task is used to identify flooding scenarios that depict the nature of the challenge that an internal flood presents. Transfer event trees for internal flooding initiating events are then linked to the internal hazard event trees to evaluate the module response.

<u>Internal Flood Plant Partitioning</u>

For the internal flooding PRA, a "plant partitioning" activity is performed to evaluate the design and establish physical boundaries in which the effects of flooding can be contained. These boundaries define "flood areas", which consist of a building, a room within a building or other defined area. The partitioning activity is performed by review of a 12-module site plan with consideration of the locations of safety-related, risk-significant, and regulatory required SSC.

Buildings and areas that do not contain flood sources or components that could cause a reactor trip if flooded, are not considered in the internal flood PRA model. Examples of areas that are not included in the PRA model because they do not contain flood sources are the switchyard and power distribution centers. Examples of areas that do not contain components that could cause a reactor trip are the electric firewater pumphouse building and diesel firewater pumphouse building. If an area contains components that could cause a reactor trip, but flood protection features are required by design, and there is no flood source within the area protected by the flood control features, the area is removed from consideration in the PRA model. The CRB contains equipment that may result in a plant trip if flooded, but areas containing this equipment are protected from internal flooding (and there are no flood sources that would circumvent that protection). Thus, the CRB is not included in the internal flooding PRA model. Table 19.1-47 identifies the buildings and areas that are included in the model. As indicated in the table, only the RXB houses components associated with mitigating equipment.

<u>Internal Flood Source Identification and Characterization</u>

Potential sources of internal flooding are identified by review of equipment lists and system descriptions. Flooding from fluid-containing components may be initiated by:

- Failures that include leaks and breaks in piping; leaks and ruptures of tanks; and leaks and catastrophic failures of gaskets, joints, fittings, and seals.
- Human-induced mechanisms which can lead to overfilling tanks, diversion of flow-through openings created to perform maintenance, or inadvertent action of fire-suppression systems.

Table 19.1-48 identifies systems that could be internal flooding sources, characterizes their relative significance and provides their locations.

Internal Flood Scenarios

Internal flooding scenarios are developed to assess the effect of potential flooding in an area on the equipment in that area. The potential scenarios consider propagation pathways, mitigation factors, and the affected equipment.

Flood protection features that are considered in the internal flooding PRA include:

- Installation of flood doors, which is effective at ensuring a flood does not originate in an adjacent area and propagate into an area containing risk significant equipment.
- Mounting equipment above postulated flood depths,
- Appropriately sizing sumps and drains in areas, and
- Qualifying electrical equipment for submergence, for example, National Electrical Manufacturers Association (NEMA) Type 6 enclosures

Flood-induced failure of some types of equipment can be caused by immersion or other flood-induced failure mechanisms such as spray, jet impingement, pipe whip, humidity, condensation, and temperature concerns. Electrical equipment is assumed to be susceptible to flood damage; the most likely failure mechanism for flood water damage is an electrical short to ground, which typically results in an open-circuit failure mode. Failure is generally assumed to occur instantaneously when the lowest portion of the equipment is submerged, and includes:

- electrical switchgear, motor control centers (MCC), electrical cabinets
- pumps, fans, air conditioning units
- motor operated valves, which are assumed to fail 'as-is'
- air and solenoid-operated valves, which are assumed to fail in the de-energized position

Passive components such as piping, tanks, heat exchangers, manual valves, check valves, relief valves, strainers, and filters, which do not require control to operate, are not considered susceptible to flood damage.

Equipment located inside the CNV is designed to operate in harsh environments, including during potential floods in the area; therefore, flooding effects are not considered for equipment inside the CNV.

The analysis accounts for equipment 'failure' position. In this aspect, the passive nature of the NuScale design is unique in that the onsite AC power system does not interface directly with plant safety-related equipment; the design does not have safety-related AC loads. Similarly, the onsite DC power systems are not required for nuclear safety-related SSC to perform their safety function. In the NuScale design, mitigating engineered safety features are designed to "fail safe" on a loss of power. As such, safety systems are projected to go to their fail-safe position in response to a loss of power.

Flooding of areas containing equipment included in the PRA model was evaluated for the potential to damage equipment. Table 19.1-49 summarizes this evaluation.

Internal Flood-Induced Initiating Events

Determining the flood-induced initiating events involves identifying the applicable initiator(s) from the internal events PRA, the frequency of the initiator(s) and the potential flooding effect on mitigating systems.

Consideration of the potential effects that an internal flood could have on equipment and of the PRA initiating events indicates that an internal flood cannot initiate a LOCA, steam line break, or feedwater line break because passive components are not affected by flood damage. An internal flood also cannot initiate a LOOP or LODC because no internal flooding sources are associated with an area containing EDSS or EHVS switchgear. However, an internal flood could initiate a transient due to potential effects on pumps, control panels or equipment. Thus, as summarized in Table 19.1-50, the internal event initiators "TGS---TRAN--NSS" and "TGS---TRAN--NPC" are applicable to internal flooding.

The frequency of the internal flooding contribution to the transient initiator is assessed by comparing of the design to generic data provided in NUREG/CR-2300. Based on similarities in the location and types of equipment in various buildings, the internal flood frequency is estimated from industry data. Specifically, the NuScale RXB is judged to be similar to the Auxiliary Building of current nuclear plants and the Turbine Generator Building (TGB) is comparable to typical turbine buildings. Other buildings, such as the central utilities building, that are capable of inducing a plant trip elicit a similar plant response to a flooding event in the TGB. However, the frequency of a flood in the TGB is judged to dominate the flooding frequencies associated with other structures. Areas of other buildings that could experience a flood and to induce a plant trip are included in the TGB group. Table 19.1-51 provides the generic flooding frequencies and illustrates the data grouping to produce the frequencies for the NuScale RXB and TGB. The error factors presented were calculated as the square root of the 95th percentile divided by the 5th percentile frequencies.

The potential effect on mitigating systems is determined by evaluating the effect of flooding areas containing equipment modeled in the PRA on the top events associated with event trees TGS---TRAN--NSS and TGS---TRAN--NPC. The results of the evaluation are summarized in Table 19.1-52. As seen in the table, the RXB is the only area in which components modeled in PRA mitigating systems are located. The table also indicates that, because of the passive component design or their fail-safe position when deenergized, only the CVCS and the CFDS components are affected by internal flooding.

There are no operator actions that are unique to the internal flooding PRA, with the exception of actions that may be taken to isolate the flood. Operator actions are credited to mitigate an equipment failure (e.g., as a backup to failure of automatic ECCS operation). If a flooding event has the potential to challenge the equipment necessary to perform an operator action, in addition to challenging the potential travel routes to perform an action, the action is not credited.

Based on this evaluation, unique event trees were not required for the internal flooding PRA. Figure 19.1-25 and Figure 19.1-26 are used to indicate a pass-through from the internal flooding initiating events in the RXB and TGB to the TGS---TRAN--NSS and TGS---TRAN--NPC event trees, respectively.

Internal Flood Accident Sequences and Quantification

Quantification of the internal flooding PRA was performed in the same manner as the internal events PRA, as discussed in Section 19.1.4.1.1.7 using a truncation frequency of 1E-15.

19.1.5.3.2 Results from the Internal Flooding Risk Evaluation

This section provides results of the internal flooding PRA for full-power operation of a single module. Risk metrics and insights are presented. Uncertainties and sensitivity studies associated with the results are discussed.

Core Damage Frequency for Internal Floods

The mean value of the CDF for a module due to internal floods is calculated to be 6.1E-11 per mcyr; the 5th and 95th percentile values are 2.0E-13 per mcyr and 2.1E-10 per mcyr, respectively.

Large Release Frequency for Internal Floods

The mean value of the LRF for a module due to internal floods was calculated to be less than 1.0E-15 per mcyr.

Conditional Containment Failure Probability for Internal Floods

Due to the very small ratio of calculated LRF to CDF, the CCFP for a module due to internal floods is much less than 0.1.

Significant Core Damage and Large Release Sequences

Core damage due to internal floods is dominated by sequences associated with transients in which DHRS cannot depressurize the RPV quickly enough to preclude cycling of the RSVs. After the initial opening, the valve randomly sticks open resulting in a steam release into the containment; the sequences progress to core damage though failures of ECCS actuation and makeup from the CVCS. Aside from the initiating event, these sequences do not involve flood-specific failures. An additional significant contribution is a reactor trip with random failures of the DHRS and RSVs, resulting in overpressurization of the RPV.

The potential for a flood-induced large release sequence was calculated to be so small that discussion of such sequences is not meaningful from a risk perspective.

Significant Cutsets

Table 19.1-53 provides the top CDF cutsets associated with the internal flooding risk evaluation. The top four cutsets contribute more than 70 percent of the CDF associated with internal flooding. The table indicates that failure of RSVs to function correctly is associated with the top cutsets. There are no LRF cutsets with a calculated frequency greater than the truncation frequency of 1E-15.

Risk Significance

Applying the methodology referenced in Section 19.1.4.1.1.9, the internal flooding PRA identified the following SSC as risk significant candidates, as summarized in Table 19.1-64:

- ECCS (reactor recirculation valves)
- RSVs
- DHRS (inlet, actuation valves)
- MPS

No human actions were identified as risk significant.

Key Assumptions

Table 19.1-54 summarizes the key assumptions associated with the internal flooding PRA.

Uncertainties

Parameter uncertainty associated with the internal flooding PRA is characterized by probability distributions associated with the calculated results. Section 19.1.4.1.2 identifies sources of uncertainty in the internal events model. Model uncertainties that are unique to the internal flooding PRA include the initiating event frequencies (i.e., pipe routing), and the lack of design detail on protective and mitigative features. Model uncertainties associated with the internal flooding PRA are addressed with assumptions or sensitivity studies as indicated in the following section.

Sensitivity Studies

A sensitivity study is performed to assess the impact of the modeling assumption made in the internal flooding PRA where a flood in the RXB prevents operators from establishing makeup from the CVCS or CFDS. Adding credit for CVCS and CFDS makeup reduces the risk associated with internal flooding. The CDF reduces to 1.1E-12 per mcyr; the LRF is below the truncation value.

Key Insights

The internal flood PRA results show that even using conservative and bounding assumptions, the risk from internal floods is extremely low, indicative of the passive nature of the NuScale Power Plant design.

19.1.5.4 External Flooding Risk Evaluation

An external flooding PRA for full power operations has been performed for a single NuScale module. Section 19.1.5.4.1 describes key aspects of the evaluation including methodology and modeling. Section 19.1.5.4.2 provides key results including the CDF, large release frequency, and CCFP due to potential flooding events from external sources.

19.1.5.4.1 Description of External Flooding Risk Evaluation

External flooding considers potential events originating from outside of the plant boundary. The external flooding PRA is based on the Level 1 internal events PRA model, which was supplemented by flood-specific failure modes.

The external flooding PRA applies the methodology provided in Part 8 of ASME/ANS RA-Sa-2009 with consideration of the review clarifications provided in DC/COL-ISG-028. The methodology is consistent with NEI 16-05 (Reference 19.1-47). The external flooding methodology encompasses hazard analysis, fragility evaluation and module response as summarized in the following discussion.

Hazard Analysis

The hazard analysis involves an evaluation of the frequency of occurrence of an external flood. The hazard analysis typically is based on an occurrence frequency for different external flood severities using site-specific data. The frequency of an external flood includes consideration of potential site-specific causes, including:

- Extreme local precipitation (including snow melt),
- Extreme river flooding, including floods due to single or cascading dam failures,
- Extreme ocean flooding (coastal and estuary),
- Extreme lake flooding (including seiches),
- Extreme hurricane and tsunami flooding (including seismic- induced),
- Flooding caused by failure of a dam, levee, or dike.

Based on a range of probable maximum flood frequencies cited in ASME/ANS RA-Sa-2009, a flood frequency of 2.0 E-3 with an error factor of 10 is assumed to estimate the likelihood of exceeding the plant grade elevation.

External flood hazards generally occur after significant warning time or develop over a long enough time period to allow the operating staff to take precautionary measures. For 90 percent of flood events, operators are assumed to cease refueling and crane operations, and perform a controlled shutdown prior to potential external flood-induced equipment impacts (e.g., due to LOOP), when forecasts or conditions indicate the potential for SSC susceptibility to an external flood. The remaining 10 percent of floods are assumed to result in a LOOP while the plant is still at power, with the result that AC power is lost to plant transformers and power production loads such as the feedwater pumps and condensate pumps. Temporary flood protection measures such as sandbags are not credited.

Fragility Evaluation

The fragility evaluation considers the susceptibility of SSC to an external flood. It includes consideration of flood protection features that prevent floodwaters from affecting key SSC. Flood-caused equipment failure is typically due to immersion. Electrical equipment is assumed to be susceptible to flood damage; the most likely failure mechanism for flood water damage is an electrical short-to-ground, which typically results in an open-circuit failure mode. Failure is assumed to occur instantaneously when the lowest portion of the equipment is submerged, and includes:

- Electrical switchgear, MCCs, electrical cabinets, etc.
- Pumps, fans, air conditioning units
- Motor operated valves (assumed to fail "as-is")
- Air and solenoid-operated valves

The analysis accounts for the fail-safe on loss-of-power design of safety system components. The NuScale design does not include safety-related AC power loads. Similarly, DC power is not required to place a component in its desired position. Thus, safety-related components move to their fail-safe position in response to a loss-of-power, which could be associated with an external flooding event. Passive components, such as piping, tanks, heat exchangers, manual valves, check valves, relief valves, strainers, and filters, which do not require control to operate, are not considered susceptible to flood damage. Equipment located inside the CNV is designed to operate in harsh environments, and, therefore flooding effects are not considered for equipment inside the CNV.

As indicated in Chapters 2 and 3, site buildings are designed to withstand flooding associated with the probable maximum flood. Because of the inherent capability of safety-related buildings, flooding exceeding the design basis flood level is assumed not to structurally damage the Seismic Category I RXB.

Module Response

The module response, based on the internal events full power PRA model, analyzes the plant and system response to an external flood and quantifies risk metrics CDF, LRF and CCFP. Determining the module response to an external flood event involves identifying the applicable accident progression from the internal events PRA and adding the potential flooding effect on mitigating systems.

Review of the internal events PRA indicates that an external flood cannot initiate a LOCA, steam generator tube failure, or steam or feedwater line break because passive components are not affected by flood damage. An external flood could initiate a transient due to potential effects on pumps, control panels or equipment. An external flood could initiate a LOOP or LODC because of flooding in areas containing EDSS or EHVS components. A LOOP bounds the LODC initiator because the LOOP event tree captures the loss of power and de-energization of the ECCS solenoid valves. The LOOP also bounds a transient and support system loss when considering the equipment that is not available due to a loss of power. Thus, the limiting plant response and accident progression model for an external flood is the LOOP event tree. Table 19.1-55 summarizes the applicability of the initiating events used in the internal events PRA to the external flooding PRA.

The potential effect on mitigating systems is determined by evaluating the effect of flooding areas containing equipment modeled in the PRA. The results of the evaluation are summarized in Table 19.1-56. As seen in the table, the AC and DC power components can be directly affected by flooding, which causes safety related components to move to their safety position on loss of power.

Based on the susceptibility of the CRB (which houses the MCR) and RXB (which houses the remote shutdown station) to an external flood, operator actions that could potentially mitigate an external flood are not credited in the analysis.

Based on this evaluation, unique event trees are not required for the external flooding PRA. Figure 19.1-27 is used to indicate a pass-through from the external flooding initiating event to the EHVS-LOOP event tree. The figure includes an event (EXT-FLD-LOOP) that accounts for the fraction of external floods for which there is insufficient warning time for the operating staff to initiate a controlled shutdown.

External Flood Accident Sequences and Quantification

The system models that represent the top events in the external flooding PRA take into account additional failure modes that are associated with external flooding. Quantification of the external flooding PRA was performed in the same manner as the internal events PRA, as discussed in Section 19.1.4.1.1.7.

19.1.5.4.2 Results from the External Flooding Risk Evaluation

This section provides results of the external flooding PRA for full-power operation of a single module. Risk metrics and insights are presented. Uncertainties and sensitivity studies associated with the results are discussed. An evaluation of external flooding was also performed for LPSD operations. Based on the limited time a module is in any POS, the results conclude that external flooding risk during LPSD conditions is negligible.

Core Damage Frequency for External Floods

The mean value of the CDF for a module due to external floods was calculated to be 8.7E-10 per mcyr; the 5^{th} and 95^{th} percentile values are 4.7E-12 per mcyr and 3.5E-09 per mcyr, respectively.

Large Release Frequency for External Floods

The mean value of the LRF for a module due to external floods was calculated to be 7.9E-14 per mcyr; the 5^{th} and 95^{th} percentile values are 6.4E-17 per mcyr and 3.2E-13 per mcyr, respectively.

Conditional Containment Failure Probability for External Floods

Due to the very small ratio of calculated LRF to CDF, the CCFP for a module due to external floods is much less than 0.1.

Significant Core Damage and Large Release Sequences

Core damage due to external floods is dominated by sequences that involve an incomplete ECCS actuation; the EDSS batteries and switchgear are below grade and the loss of power results in an ECCS demand. An incomplete ECCS actuation causes water to transfer from the RPV to the CNV, which results in core uncovery and eventually core damage due to the incomplete recirculation path for RCS fluid between the RPV and CNV.

Dominant large release sequences are similar to those for core damage, but also include failures of containment isolation. The containment isolation failures include CCF of both CES isolation valves to close, and CCF of both CVCS isolation valves to close.

Significant Cutsets

Table 19.1-57 provides the top CDF and LRF cutsets associated with the external flooding risk evaluation. The top CDF cutsets account for over 99 percent of the total risk due to external flood. The LRF cutsets shown in the table account for 100 percent of LRF cutsets with frequencies above the 1E-15 truncation limit. The majority of external flood risk is associated with flood-induced LOOP followed by an incomplete ECCS actuation. Incomplete ECCS actuations are the result of CCFs of both RRVs or all three RVVs following the flood-induced failures of the switchgear and batteries. The most significant cutsets for LRF also involve CCF of the containment evacuation system CIVs or CCF of the chemical and volume control system CIVs to close.

Risk Significance

Applying the methodology referenced in Section 19.1.4.1.1.9, the results of the external flooding PRA were reviewed to identify candidate risk significant SSC. Based on the review, the following SSC are risk significant, as summarized in Table 19.1-64:

- CVCS and CES containment isolation valves
- ECCS
- MPS

For the situations in which a controlled shutdown has not been completed by the operators prior to external flooding (i.e., ten percent of the external flooding initiating events) operator actions are not credited. Therefore, operator actions are not identified as risk significant in the external flooding evaluation. In addition, because flooding penetrations (e.g., doors) are not credited in the external flooding analysis, none were identified as risk significant.

Key Assumptions

Table 19.1-58 summarizes the key assumptions associated with the external flooding PRA.

Uncertainties

Parameter uncertainty associated with the external flooding PRA is characterized by probability distributions associated with the calculated results. Section 19.1.4.1.2 identifies sources of uncertainty in the Level 1 internal events model and Section 19.1.4.2.2 identifies sources of uncertainty in the Level 2 internal events model. Model uncertainties that are unique to the external flooding PRA include the external flooding initiating event frequency and the lack of design detail on protective and mitigative features for flooding. Model uncertainties associated with the external flooding PRA are addressed with assumptions; as indicated in the following section, sensitivity studies are judged unnecessary.

Sensitivity Studies

The external flooding PRA for design certification is based on conservative, bounding assumptions. No sensitivity studies were performed.

Key Insights

The external flood PRA results show that even using conservative and bounding assumptions, the risk from external floods is extremely low, indicative of the passive nature of the NuScale design.

19.1.5.5 High-Wind Risk Evaluation

A high-wind risk assessment for at power operations has been performed. Consistent with Part 7 of ASME/ANS RA-Sa-2009, wind hazards whose only effect on the site is to induce a loss-of-offsite power, are considered in the internal events PRA model. The internal events PRA includes a LOOP initiating event due to 1) extratropical straight wind (e.g., thunderstorms, squall lines, weather fronts); 2) tornadoes defined on the Enhanced Fujita (EF) scale as EF0 and EF1 (i.e., wind speed ≤ 110 mph); and 3) Saffir-Simpson scale Category 1 and Category 2 hurricanes (i.e., wind speed ≤ 110 mph). Thus, the high-winds PRA addresses hazards from extreme high winds, specifically tornadoes and hurricanes that exceed the conditions associated with an internal event initiator.

Section 19.1.5.5.1 describes key aspects of the evaluation including methodology and modeling. Section 19.1.5.5.2 provides key results including the CDF, large release frequency, and CCFP due to high-wind events.

19.1.5.5.1 Description of High-Wind Risk Evaluation

The high-wind events considered in this evaluation are considered extreme high winds which exceed those evaluated in the internal events PRA. Winds or tornadoes can affect plant structures if: (1) wind forces exceed the load capacity of a building or other external structures, causing damage or collapse of the walls or framing, or (2) the wind is strong enough to lift materials and propel them as missiles against structures that house safety-related equipment.

The wind events considered in the high-winds PRA are:

- Tornadoes with a wind speed exceeding 110 mph. Wind speeds ≤ 110 correspond to Enhanced Fujita (EF) scale ratings EF0 and EF1 are considered to be contributors to weather-related LOOP events in the internal events PRA. Thus, EF2 through EF5 tornadoes are addressed in the high-winds risk evaluation.
- Hurricanes with a wind speed exceeding 110 mph. Hurricanes having wind speeds ≤ 110 correspond to Saffir-Simpson Hurricane Wind Scale Categories 1 and 2 are considered to be contributors to weather-related LOOP events in the internal events PRA. Thus, Category 3 through Category 5 hurricanes are addressed in the high-winds risk evaluation.

Methodology

The high-wind PRA applies the methodology provided in Part 7 of ASME/ANS RA-Sa-2009 and includes a hazard analysis, fragility evaluation, and plant response. The hazards analysis involves an evaluation of the frequency of occurrence of high-winds events. The fragility evaluation considers the susceptibility of plant SSC to high winds and wind-generated missiles. The plant response model analyzes the plant and system response to a high-winds event and quantifies CDF and LRF. The high-winds plant response model is based on the internal events model for full power conditions and adapted to incorporate aspects of the high-wind hazard.

The frequency of occurrence of high-winds events considers the regions of the U.S with the highest tornado intensity and the highest occurrence of hurricanes to provide bounding inputs for potential NuScale sites. A single tornado initiating event frequency for EF2 through EF5 tornadoes and a single hurricane initiating event frequency for hurricanes greater than Category 3 are determined. The fragility portion of the analysis evaluates the NuScale structural response to the wind speeds and pressure drops of the tornadoes and hurricanes evaluated to determine the structures and systems susceptible to high winds.

The event trees from the internal events PRA model are reviewed for applicability to high winds. As indicated in Table 19.1-59, only the LOOP event tree EHVS--LOOP---ET is considered in the high-winds PRA because (i) systems or components whose failure would otherwise result in an initiating event are located in Seismic Category I structures, and would therefore not be affected by high winds, (ii) other initiators, such as a feedwater line break outside the RXB, are unlikely and mitigated by closing isolation valves inside the RXB, or (iii) the effects of the initiating event are bounded by the LOOP event.

Figure 19.1-28 and Figure 19.1-29 are the full power high-winds event trees; the event trees are simply a transfer to the internal events LOOP event tree. There are separate transfer trees for extreme winds associated with a tornado and a hurricane.

Quantification is similar to that performed for the internal events models with rules relevant to a high-wind event, for example, assuming systems located outside of the RXB are unavailable.

High-Wind Hazard

The initiator frequency associated with the high-winds PRA is derived from the frequency of high winds exceeding 110 mph, due to either tornadoes or hurricanes. Because a specific site is not identified for design certification, a bounding analysis is performed to assess the high-wind occurrence frequency. The high-wind initiating event frequencies for various operating modes are developed from the high-wind strike frequencies and the time the module is in a specific mode. For full power operation, the initiating event frequency conservatively assumes 100 percent module availability.

<u>Tornado Strike Frequency</u>

To assess the tornado frequency, the methodology provided in NUREG/CR-4461 (Reference 19.1-48) is applied. Using the "point structure" model, the probability of the wind speed exceeding a given value at a site is dependent on the total area affected by tornadoes in the region of interest divided by the total area of the region of interest over the time period under consideration. Using the “life-line” model for a tornado striking a large structure, the probability of the wind speed exceeding a given value affecting a large structure is dependent on the size of the structure and the total length of tornado paths within the region over the time period under consideration. The total tornado strike frequency of a structure is the sum of the point structure and life-line strike probabilities.

The tornado hazard frequency is based on the region of the U.S. with the highest tornado intensity, central U.S. region 1, using data from NUREG/CR- 4461. The tornado initiating event for full power operations is the overall strike frequency adjusted by the module availability factor. As stated, the availability factor is conservatively assumed to be one (i.e., the module operates at 100 percent power for a full year). The frequency of the tornado initiating event, IE-TORN--EF2-5-FP, for EF2 through EF5 tornadoes is calculated as 2.1E-04 per year with an assumed lognormal distribution and error factor of 10.

Hurricane Strike Frequency

The methodology for estimating a hurricane strike is based on the number of hurricane events near United States commercial operating plants that are at risk for hurricane damage, divided by the operating time for those at-risk reactors. The wind maps in ASCE 7-19 (Reference 19.1-49) for the region of the United States with the highest occurrence of hurricanes are used to determine the hurricane wind speed hazard near at-risk reactors. Plants where a maximum wind speed greater than that of a Category 2 hurricane (i.e., > 111 mph) could occur, are considered. Hurricane events and undefined high-wind events that resulted in a LOOP are obtained from NUREG/CR-6890. The number of events is then divided by the sum of the years of operation for the at-risk reactors to determine the strike frequency. The hurricane initiating event for full power operations is the overall strike frequency adjusted by the availability factor. As stated, the availability factor is conservatively assumed to be one, that is, the module operates at 100 percent power for a full year. The frequency of the hurricane initiating event, IE-HURR-CAT3-5-FP, for hurricanes of Category 2 or greater is calculated as 1.5E-03 per year with an assumed lognormal distribution and error factor of 10.

High-Wind Fragility Evaluation

The distinction between high winds that are considered in the internal events model, that is, those for which the only effect is a LOOP, and those considered in the high-winds evaluation, is based on building design capability to withstand such wind speeds without significant damage. Damage to equipment from extreme high winds can occur due to pressure differentials, wind generated missiles, or direct damage due to dynamic wind loadings. The fragility of SSC is evaluated using a bounding approach based on the seismic classification of structures. Table 19.1-60 summarizes NuScale building capacity to withstand high winds. The table illustrates, for example, that Category I structures are not damaged enough by tornado winds categorized up to and including EF5 to cause damage to SSC located within the structures.

Given the structural response to high winds provided in Table 19.1-60, a review of the top events in the LOOP and Level 2 event trees is performed for susceptibility to high winds.

Plant Response: Recovery of Offsite Power

To assess the potential for recovering power within 24 hours (to prevent a demand for the ECCS), data from NUREG/CR-6890 were reviewed; it includes data with the probabilities of exceedance versus duration for a LOOP. Based on these data, there is a 1.1E-01 probability, given a weather-related LOOP, that the duration will be longer than 24 hours. Therefore, a weather-related LOOP non-recovery probability of 1.1E-01 (with an error factor of 10) was applied to tornado and hurricane events. Event EHVS--SYS-0002X-FOP-N is added to cutsets that include recovery of offsite power. This event is a multiplier used to increase the probability of failure to recover offsite power for tornadoes and high winds from that included in the internal events PRA model.

High-Wind Operator Actions

The high-winds PRA included a review of the HFEs in the internal events PRA. Two operator actions that are credited in the internal events PRA but were judged not to be possible following a high-wind event are:

- operator starts and loads the CTG due to the potential for significant damage to the combustion turbine
- operator starts and loads the BDGs due to the potential for significant damage to the building housing the BDGs

The other operator actions occur within the Seismic Category I RXB and CRB, which are not susceptible to high-wind damage. Due to the additional stress on the operators during a high-wind event, HFEs in high-wind cutsets were multiplied by a factor of five to account for the assumed "extreme stress" environment.

19.1.5.5.2 Results from the High-Wind Risk Evaluation

This section provides results of the high-winds PRA for full-power operation of a single module. Risk metrics and insights are presented. Uncertainties and sensitivity studies associated with the results are discussed.

<u>Core Damage Frequency</u>

The mean high-wind CDFs for a single module operating at full power from tornadoes of EF2 or greater and from hurricanes of Category 3 or greater, using a 1E-15 truncation, are:

- tornado CDF = 9.9E-11 per mcyr; 5th and 95th percentile values are 3.9E-13 per mcyr and 3.9E-10 per mcyr, respectively
- hurricane CDF = 7.2E-10 per mcyr; 5th and 95th percentile values are 2.9E-12 per mcyr and 2.8E-09 per mcyr, respectively

The results for core damage are dominated by sequences that involve an incomplete ECCS actuation; if AC power is not restored within 24 hours, ECCS valves are demanded to move to their fail-safe position on loss of power. A CCF of both RRVs or all three RVVs transfers reactor coolant from the CNV to the RPV, but without recirculation, core uncovery and eventual core damage results.

Large Release Frequency

The mean high-wind LRFs for a single module operating at full-power operation are:

- tornado LRF = less than 1E-15 per mcyr
- hurricane LRF = 6.4E-14 per mcyr; 5th and 95th percentile values are 3.8E-17 per mcyr and 2.5E-13 per mcyr, respectively

The dominant sequences for the large release are similar to those for CDF, but also include a failure of containment isolation. The containment isolation failures include CCF of both CES isolation valves or both CVCS isolation valves to close.

Conditional Containment Failure Probability for High Winds

Due to the very small ratio of calculated LRF to CDF, the CCFP for a module due to high winds is much less than 0.1.

Significant Cutsets

Table 19.1-62 and Table 19.1-63 provide the top CDF and LRF cutsets associated with the hurricane and tornado high-wind risk evaluation, respectively. The top hurricane CDF cutsets comprise approximately 96 percent of the risk. There are only eight hurricane LRF cutsets above the 1E-15 truncation limit. The top tornado CDF cutsets are similar in content to the hurricane cutsets and also comprise about 96 percent of the tornado risk. There are no tornado LRF cutsets with a calculated frequency greater than 1E-15 per mcyr. The most significant cutset for the high-winds CDF involves incomplete ECCS actuation due to CCF of the RRVs to open following failure to restore offsite power within 24 hours. The most significant cutset for LRF also involves failure of the CES containment isolation valves to close.

Risk Significance

Applying the methodology referenced in Section 19.1.4.1.1.9, the results of the high-winds PRA were reviewed to identify candidate risk significant SSC. Based on the review, the following SSC are risk significant, as summarized in Table 19.1-64:

- CES and CVCS containment isolation values
- ECCS (reactor recirculation valves, reactor vent valves, reactor pool)
- MPS

None of the operator actions considered in the high-winds PRA are risk significant.

Key Assumptions

Table 19.1-61 summarizes key modeling assumptions for the high-winds PRA.

Uncertainties

Parameter uncertainty associated with the high-winds PRA is characterized by probability distributions associated with the calculated results. Section 19.1.4.1.2 and Section 19.1.4.2.2 identify sources of uncertainty in the internal events model. Model uncertainties that are unique to the high-winds PRA include the initiating event frequencies and the lack of design detail on protective and mitigative features. Model uncertainties associated with the high-winds PRA are addressed with assumptions or sensitivity studies as indicated in the following section.

Sensitivity Studies

The high-winds PRA analysis is based on conservative, bounding assumptions so as to encompass all potential domestic (U.S.) sites. Because of the low risk associated with high winds, the only sensitivity performed is to alter the probability of recovering offsite power. Increasing the failure to recover offsite power from 1.1E-01 to 5.0E-01 increases the hurricane CDF by almost an order of magnitude. Similarly, the hurricane LRF increases. Because the dominant sequences involve failure to recover power, changes in risk track almost linearly with the probability of recovering power. Tornado CDF and LRF respond similarly with the change in probability of recovering offsite power.

Key Insights

The results of the high-winds evaluation indicate that, even using bounding assumptions, the risk associated with a high-winds event is extremely low. The high-wind hazard evaluation does not identify additional SSC as risk significant that were not identified in the internal events PRA. Equipment failures after the high wind-induced LOOP are due to random failures and are independent of the initiator. The passive design features and redundant systems ensure safe shutdown, core cooling, and containment integrity.

19.1.6 Safety Insights from the Probabilistic Risk Assessment for Other Modes of Operation

The risk associated with full power operations is discussed in Section 19.1.4, which addresses internal events, and Section 19.1.5, which addresses external events. This section addresses the risk associated with other modes of operation which is assessed by the LPSD probabilistic risk assessment. The LPSD probabilistic risk assessment addresses risk associated with modes other than full power operation, including low power operation, refueling outages, hot shutdown, and flooded and unflooded maintenance shutdowns.

Section 19.1.6.1 describes the LPSD probabilistic risk assessment. Section 19.1.6.2 provides results for the risk associated with internal events at LPSD. Section 19.1.6.3 provides results for the risk associated with external events at LPSD.

19.1.6.1 Description of the Low Power and Shutdown Operations Probabilistic Risk Assessment

An LPSD evolution is defined in the ANS/ASME Low Power and Shutdown PRA Standard (Reference 19.1-50) as "a series of connected or related activities such as a reduction in power to a low level or plant shutdown followed by the return to full-power plant conditions." Thus, the LPSD probabilistic risk assessment addresses the risk associated with Technical Specification Mode 2 (Hot Shutdown), Mode 3 (Safe Shutdown), Mode 4 (Transition) and Mode 5 (Refueling). The LPSD probabilistic risk assessment quantitatively analyzes the risk for a nominal refueling outage. The 24-month refueling cycle corresponds to a refueling frequency of 0.5 per year, and a nominal refueling outage is projected last approximately 10 days.

A scheduled outage begins by increasing the boron concentration in the primary coolant and inserting control rods to reduce power in preparation for shutdown. When the power reaches the minimum turbine load, the turbine is tripped and the turbine bypass valve is used to adjust the steam flow to maintain the power level. A short time later the control rods are fully inserted to terminate fission power. Motive power to the control rod drive mechanisms is removed to prevent unintentional withdrawal. Normal secondary cooling is used to reduce primary coolant temperature and pressure to allow the CNV to be flooded. The CFDS is used to fill the CNV with water from the reactor pool to approximately the level of the pressurizer baffle plate, establishing passive cooling by conducting heat through containment to the reactor pool.

If the module is to be refueled, disconnection begins after the RVVs and RRVs are open. Disconnection involves removing the bioshield, disconnecting piping and instrumentation, installing material exclusion covers on pipe flanges, and connecting the RBC and module lifting adapter to the module.

Module transport involves using the RBC to lift the module out of its operating bay, transport it to the refueling area, and lift it into the containment flange tool (CFT).

Module disassembly begins after the module is placed into the CFT. With the module still connected to and supported by the RBC, the CNV flange is unbolted and the RPV and upper CNV are lifted out of the CFT and moved to the reactor flange tool (RFT) while the lower portion of the CNV remains in the CFT. The RPV flange is unbolted and the upper CNV and the upper RPV, which includes the upper RPV internals, are moved to the dry dock area while the lower head of the RPV, which includes the core, remains in the RFT. After securing the upper vessels in the dry dock the RBC returns to the refueling area to remove the lower riser assembly and allow access to the fuel.

The fuel handling machine is used to move fuel assemblies between the core and the fuel storage racks. Maintenance and inspections are carried out on the upper vessels and RPV internals in the dry dock area during this time, and remote inspections are performed on the lower RPV and lower CNV in the refueling area.

The module is reassembled after maintenance activities are completed and proper fuel loading is verified. The RBC replaces the reactor vessel internals, then aligns the upper vessels for reassembly in the RFT. The RPV flange bolts are tensioned and the assembly is lifted out of the RFT and moved to the CFT. The RBC aligns the CNV for reassembly and the CNV flange bolts are tensioned.

Module transport involves using the RBC to lift the module out of the CFT, transport it to the operating bay, and lower it into the seismic restraints. The RBC is disconnected from the module.

Module reconnection involves restoring instrumentation and power connections, and reconnecting all piping.

Restart begins with steam generator cleanup by establishing flow through the steam generators using the feedwater, main steam, and condensate systems. Flow is established through the CVCS to close the RVVs and RRVs and begin coolant cleanup and boron dilution. The CNV is drained and RPV heatup begins as heat conduction to the reactor pool is reduced. Heat is added primarily by passing CVCS flow through the startup heater, with some assistance from the pressurizer heaters. Feedwater flow is adjusted to establish coolant circulation within the RPV, and control rods are withdrawn to establish criticality. When the power level reaches the minimum turbine load, the turbine is brought online and heatup continues. When the turbine is synchronized with the electrical grid, the module exits the scope of the LPSD probabilistic risk assessment and enters that of the full-power PRA.

The nominal refueling outage is modeled as a series of seven plant operating states (POSs) that cover each arrangement of the module between shutdown and start-up. In addition to module arrangement, POSs are defined based on the activity being performed and availability of systems which can cause or be used to mitigate an initiating event. Each POS is described in detail below.

POS1: Shutdown and Initial Cooling: The module enters POS1 when the control rods are inserted and the module becomes subcritical. Normal secondary cooling through the turbine bypass is used to reduce the temperature of the primary coolant to a level that allows the CNV to be flooded, and the CVCS functions to both borate and cleanup coolant chemistry. Containment flood begins and the main steam and feedwater systems are removed from service. The module exits POS1 when CNV flooding is complete.

POS2: Cooling Through Containment: The module enters POS2 when the CNV flood is complete. Decay heat is passively conducted through the flooded CNV to the reactor pool, and cooling remains passive for the duration of the outage. If the module is not being transported, the module can be maintained in POS2 indefinitely without electric power or operator action. If the module is being transported, it exits POS2 when it is lifted by the RBC, and if it is not being transported it exits POS2 when the CNV drain begins in preparation for restart.

POS3: Transport and Disassembly: The module enters POS3 when the module is lifted by the RBC. This POS includes transport to the refueling area and disassembly and ends when the RBC moves the upper RPV and CNV into the dry dock area.

POS4: Refueling and Maintenance: The module enters POS4 when the RBC moves the upper RPV and upper CNV into the dry dock. While in POS4, the core remains in the RPV lower head while the upper vessels are far enough from the refueling area that the core is not affected by an RBC failure. The module exits POS4 when the upper vessels are brought out of the dry dock in preparation for module reassembly.

POS5: Reassembly, Transport, and Reconnection: The module enters POS5 when the upper vessels are brought out of the dry dock in preparation for module reassembly. The upper RPV and upper CNV are aligned with the RPV lower head in the RFT and the

RPV flange is tensioned and leak tested, then the assembly is moved to the CFT, where it is aligned with the CNV lower head and the CNV flange tensioned and leak tested. After transport to the operating bay piping and power connections are restored, instrumentation is transferred back to its operating configuration, steam generator cleanup begins, and the RVVs and RRVs are closed in preparation for draining the CNV. The module exits POS5 when CNV drain begins.

POS6: Heatup: The module enters POS6 when CNV drain begins. CVCS flow bypasses the module until the RPV is sufficiently pressurized, then CVCS flow through the RPV is established. This POS includes CNV drain, alignment of secondary coolant flow, and completion of testing required to withdraw control rods. Active systems credited in the full power PRA are available. The module exits POS6 when control rods are withdrawn to criticality.

POS7: Low Power Operation: The module enters POS7 when control rods are withdrawn and the core reaches criticality. Systems credited in the full power PRA are nominally available, with the only difference in configuration being that the turbine is bypassed. During startup, core power is increased following procedural limits until it reaches the minimum turbine load allowing turbine synchronization with the grid. The turbine is synchronized with the grid, at which time the module exits POS7. The configuration of POS7 also includes extended low power operation in which the module is critical but the power level is below the minimum turbine load, and the turbine is, therefore, bypassed.

Table 19.1-65 summarizes plant operating states and the time in each POS.

19.1.6.1.1 Low Power and Shutdown Methodology

In the same manner as is done for the full power PRA, the LPSD probabilistic risk assessment is constructed by first developing a representative spectrum of potential initiating events. The spectrum of initiating events was developed by identifying the safety functions that are required during LPSD. The LPSD safety functions are:

- decay heat removal: maintaining adequate heat transfer so that the fuel cladding temperature remains below 2200 degrees Fahrenheit
- coolant inventory control: maintaining sufficient inventory in the RCS to cover the fuel and ensure decay heat removal
- RCS integrity: maintaining the reactor coolant pressure boundary
- reactivity control: maintaining k_{eff} in the desired regime
- core orientation: maintaining the core in an upright configuration to enable natural circulation of coolant. This is a safety function unique to NuScale.
- low temperature overpressure protection (LTOP): preventing brittle fracture of the RPV

The initiating events identified in the full power PRA are reviewed to determine if their occurrence would challenge a safety function for each POS. Applicable initiating events are then linked to the full power event trees for quantification, with event tree logic modified to reflect LPSD conditions. Fault trees are used to quantify top events of the event trees. The system success criteria used for LPSD probabilistic risk assessment are the same as those used for the full power PRA.

19.1.6.1.2 Low Power and Shutdown Initiating Events

Initiating events considered in the LPSD probabilistic risk assessment are those that are considered in the full power PRA and those that may be unique to the LPSD configuration. EPRI TR-1021167 (Reference 19.1-55) was also reviewed for applicability to confirm that the initiators are appropriately reflected in the model.

Initiating Events Common to the Full Power Probabilistic Risk Assessment

The full power initiating events were reviewed for applicability to each POS and screened as appropriate for module conditions. If an initiating event is precluded due to the configuration of the module during a POS, or if the initiating event does not challenge a safety function, the event is screened as not applicable to the POS. For example, during POS1, POS6, and POS7, the configuration of the module is similar to normal operation, and initiating events considered for full power are applicable to LPSD.

By contrast, most at-power initiating events can be screened for the remaining plant operating states. The flooded CNV allows "LOCA inside containment" events to be screened. Also, normal secondary cooling is out of service, allowing the screening of general transients, secondary line breaks, SGTFs, loss of DC power, and LOOP. In POS4, the module is disassembled and the core is open to the reactor pool, which passively provides both decay heat removal and inventory control; thus, all internal initiating events are screened. In POS3 and the transport portion of POS5, the module is completely disconnected and unaffected by any at-power initiating events. Coolant recirculation by CVCS is in place for the beginning of POS2 (until just before the RVVs and RRVs are opened) and the end of POS5 (beginning shortly before the RVVs and RRVs are closed). When CVCS is in service, line break outside containment events are retained, and screened when it is out of service.

Table 19.1-66 summarizes the full power initiating events and their applicability during LPSD.

Initiating Events Unique to Low Power and Shutdown

Low temperature overpressurization could be caused by an uncontrolled coolant injection (e.g., inadvertent CVCS injection) or heat addition (e.g., inadvertent pressurizer heater actuation) at low RCS temperature. Low temperature overpressure protection is enabled when the RCS pressure is below the LTOP enable temperature and ECCS valves are closed. The LTOP function is performed by automatic opening of one or more RVVs to relieve pressure.

Low temperature overpressure events are screened based on the number of failures that must occur in order for a pressurization event to occur, the short time period in which the pressurization event could occur when LTOP is enabled, the amount of time that the pressurization event must continue before the RVVs would be demanded to open due to the pressurizer not being water-solid, the presence of automatic MPS signals and alarms, and the high reliability of the RVVs to open on demand.

Module transport is a unique step in the NuScale refueling process, as discussed in Section 1.2.2.1.2 and Section 19.1.6.1.

Given the unique nature of the refueling process, initiating events "IE-RBC-DROP-OP-FTS" and "IE-RBC-DROP-RF-FTS" associated with failure of the RBC are included in the LPSD risk assessment. An RBC failure initiating event is applicable to POS3 and POS5 and is used to depict potential drops in the operating area and refueling area. Module drops in the operating area could involve damage to multiple modules; a drop in the refueling area could affect only a single module. Table 19.1-68 provides the initiating event frequencies for POS3 and POS5 for the operating and refueling areas. The initiator frequencies provided in Table 19.1-68 were determined by multiplying the module drop probability per lift by the frequency with which a lift occurs. A module is lifted once per POS, and enters each POS 0.5 times per year, therefore the initiating event frequency is found by multiplying the module drop probability for each location by 0.5 times per year. A lognormal uncertainty factor of 10 is assumed, which is consistent with internal initiating events.

To develop the module drop probability per lift, an evaluation of the RBC was performed to identify combinations of failures that could lead to a module drop. Initiating events for this evaluation were identified using an FMEA, supplemented by operating experience in NUREG-0612 (Reference 19.1-51). For each module drop initiating event, an event tree is developed to account for potential mitigating features (e.g., detection capability, emergency stops) which could prevent the initiating event from progressing to a module drop. Three types of drops were initially considered, based on the assembled configuration of the module during RBC movements:

- The first type of module drop reflects the possibility of dropping an assembled module. The module is in this configuration when transported between the operating bay and the CFT. In a fully assembled module, the CNV is intact, flooded, and the RVVs and RRVs are open. Module drops in this configuration are considered for POS3 and POS5.
- The second type of module drop reflects the possibility of dropping a partially assembled module, without the lower CNV. The module is in this configuration when the RBC lifts the upper CNV and the RPV out of the CFT and places it into the RFT. In this configuration, the water in the RPV communicates freely with the reactor pool through the open RVVs and RRVs. If a module were dropped in this configuration, pool water would flow in through the open RVVs and RRVs to keep the fuel covered and prevent core damage. Thus, a drop of a partially assembled module is not considered further in the LPSD probabilistic risk assessment.
- The third type of module drop reflects the possibility of dropping the upper vessels (i.e., the upper portions of the RPV and CNV) as they are moved to or

from the dry dock area. Because the fuel is in the lower RPV, which remains in the RFT, the primary hazard in this situation is the physical impact of the RBC dropping the upper vessels onto the stationary core. While this configuration is not included as a potential contributor to CDF because it involves potential mechanical fuel damage rather than inadequate heat removal, the radiological dose calculation of potential radionuclide release due to damaged fuel indicates that a large release does not occur due to this type of module drop. Thus, a drop of the upper vessels is not considered further in the LPSD probabilistic risk assessment.

Table 19.1-67 summarizes the module drop initiating events associated with an RBC failure and the mitigating features. Figure 19.1-30 is a representative event tree for evaluating potential NPM drops. The representative event tree is used to evaluate a full module drop based on the overload (OL) module drop initiating event (Item 7 in Table 19.1-67), in which the load exceeds the rated capacity of the RBC. As indicated on the event tree, a module drop occurs based on combinations of detection and safety system features, for example, Sequence 6 of Figure 19.1-30 involves failure of the weigh circuit in the hoist control system to detect the overload (DET-OL) and failure of the motor overload protection to stop the motor (OL-PROT), which results in a module drop (MD) end state. The top events of the event trees are evaluated using fault trees. Quantification of the event trees associated with the module drop initiators identified in Table 19.1-67, and accounting for the time that a module is being moved in either the refueling area and operating area, produced probabilities of module drop in each of these areas for POS3 and POS5 as summarized in Table 19.1-68, as well as the determination of the initiating event frequencies that are used in the LPSD probabilistic risk assessment.

19.1.6.1.3 Low Power and Shutdown Accident Sequence Determination

The accident sequences modeled in the LPSD probabilistic risk assessment are represented by the various "paths" through the event trees that were developed to depict the module response to initiating event. The changes in the module configuration between full power and LPSD configurations are not significant with regard to success criteria as no new systems are brought online to aid in shutdown cooling or other LPSD functions. For these systems, the LPSD success criteria are bounded by those established for full power condition. The LPSD plant operating states exhibit lower decay heat levels than the full power PRA due to the module being shut down or operating at low power at the time of the initiating event and the systems modeled for mitigation of full power initiators are sufficient for decay heat levels. Thus, for most LPSD initiating events, an LPSD transfer event tree is used to transfer to the full power event trees with the following modifications to the sequence logic to reflect each POS configuration:

- RTS-T01: The RTS is assumed to succeed for the POS in which the module is subcritical (i.e., POS1, POS2, POS3, POS4, POS5, and POS6).
- CFDS-T01: The containment flooding system is assumed to succeed for the POS in which the CNV is already flooded (i.e., POS2, POS3, POS4, and POS5).

- DHRS-T01: The DHRS is not necessary in POS2 and POS5, for which the safety function of decay heat removal is achieved by passively conducting heat to the UHS through the flooded containment.
- RCS-T05: The RCS reactor safety valve demand to open is questioned following actuation of DHRS in transient event trees, when the RCS pressure may rise high enough to open the RSV before sufficient heat has been removed to reduce the pressure. Because the module is already shutdown, it is unlikely that the pressure increases enough to open the RSVs when DHRS is successful.

A representative LPSD transfer event tree is provided as Figure 19.1-31. The tree is used to transfer the initiating event of a CVCS charging line LOCA occurring in POS1 to the full power event tree CVCS-ALOCA-CIC for evaluation of the mitigating system response. Similar transfer trees are used for each of the unscreened LPSD events indicated in Table 19.1-66.

Additional event trees are developed to account for the design-specific RBC failure initiating events in POS3 and POS5. Module drop scenarios are those that may lead to core damage due to inadequate cooling caused by uncovering the fuel. This occurs in the case of a horizontal or nearly horizontal module, in which the coolant inventory in the CNV is not sufficient to cover the fuel; due to uncertainty in calculations of peak cladding temperature (PCT), core damage is assumed to occur. Module drop scenarios in which the module comes to rest in such a way that the fuel remains covered are assumed not to result in core damage due to inadequate heat removal. Module drop scenarios are defined by whether the drop could occur in the operating area or refueling area of the reactor pool. The specific locations of a postulated drop are selected to maximize the probability that a tipping module would strike another operating module, and the lowest probability that a dropped module comes to rest partially upright on a structural portion of the RXB.

A module dropped in the operating area is dropped from a maximum height of one foot; a drop from this low height leaves a possibility that the containment support skirt may not fail and the module may remain upright. Due to uncertainty in the parameters of such a module drop, the probability of the module remaining upright is assigned by engineering judgment. A module dropped in the refueling area is assumed to not remain upright. The transfer event trees provided as Figure 19.1-32 through Figure 19.1-35 are used to link the module drop initiating event frequencies provided in Table 19.1-68 to the event trees used to evaluate the end state of a module drop event; these event trees are provided as Figure 19.1-36 and Figure 19.1-37.

Figure 19.1-36 depicts the possibility of a module drop in the operating area. The initiating event shown in the figure, IE-RBC-DROP-OP-FTS, is a placeholder, and the initiating event frequency is added through the POS-specific transfer event trees shown in Figure 19.1-32 and Figure 19.1-34. The top event RBC-T01 depicts the possibility of the module tipping if dropped. If the module remains upright, cooling from natural circulation and conduction through the flooded CNV is unaffected and the module remains cooled. If the module remains upright, no core damage occurs and the sequence results in an "OK" end state. If the module falls over, core damage occurs, and the sequence is assigned the end state "MD-CD." It is further conservatively assumed that the CNV is damaged in a manner that provides a radionuclide release path, but does not allow inflow of water that would prevent core damage. Analysis shows that the offsite dose consequences of core damage in a horizontal module with a damaged CNV results in a radionuclide release that is a small fraction of that associated with a large release. The radionuclide release is limited because of the scrubbing effect of the reactor pool. The practice of pressurizing the CNV in preparation for module transport as identified in Section 9.3.6, or the gas used for pressurization, does not affect the potential for core damage or radiological consequences of postulated module drop accidents, as modeled in the PRA.

Figure 19.1-37 illustrates the possibility of a module drop in the refueling area. The initiating event shown in the figure, IE-RBC-DROP-OP-FTS, is a placeholder, and the initiating event frequency is added through the POS-specific transfer event trees shown in Figure 19.1-33 and Figure 19.1-35. Module drops in the refueling area are assumed to result in core damage because the module is dropped from a height greater than one foot.

19.1.6.1.4 Low Power and Shutdown Data Sources and Analysis

Data sources used in the LPSD probabilistic risk assessment are similar to those discussed for the full power PRA. Differences from the full power PRA are:

- The initiating event frequency from the full-power PRA is adjusted to account for the duration and frequency for each POS.

  The equation used to adjust the frequency is

  $$f_{\mathrm{LP}} = f_0 f_{\mathrm{RF}} \frac{t}{8760}$$

  where,

  f_{LP} = frequency used in LPSD probabilistic risk assessment, per calendar year,

  f_0 = full power frequency of event, per mcyr,

  f_{RF} = refueling outage frequency, per calendar year,

  t = time during which the initiating event is applicable, hours, and

  8760 = number of hours per year

- The LOOP frequency is assumed to be the same as that used for the full-power PRA although operating experience sources provide a different frequency for LOOP during shutdown, primarily due to maintenance activities. The electrical distribution systems have been designed with high redundancy and to have maintenance performed online to allow minimal disruption to operating modules. Therefore, the plant configuration when one module is in refueling is not substantially different than when all modules are operating, justifying the use of the same event frequency.

- The RBC used for module moves is designed to the single-failure proof criteria described in NUREG-0612 and NUREG-0554 (Reference 19.1-52), thus is highly reliable. The generic data from NUREG-0612, NUREG/CR-6928, IEEE STD 500-1984 (Reference 19.1-53) and the Quanterion Automated Database (Reference 19.1-54) are used to quantify the module drop fault trees supporting the top events of the module drop event trees, as discussed in Section 19.1.6.1.3.
- The probability of module tipping if dropped is represented by top event RBC-T01. When dropped from a height of one foot or less, the probability that a module tips is 0.5, with uncertainty uniformly distributed between 0 and 1. When dropped from a height exceeding one foot, the module is assumed to tip.

19.1.6.1.5 Low Power and Shutdown Software

Consistent with the full-power PRA, the LPSD probabilistic risk assessment is produced using the SAPHIRE computer code.

19.1.6.1.6 Low Power and Shutdown Quantification

Quantification of the LPSD probabilistic risk assessment model is performed with the SAPHIRE code in the manner described in Section 19.1.4.1.1.7 for the full power PRA. A cutset truncation level of 1E-15 was used to be consistent with other hazard analyses.

19.1.6.2 Results from the Low Power and Shutdown Operations Probabilistic Risk Assessment

This section provides the results of the risk associated with LPSD due to internal events. The risk metrics are presented in terms of (1) risk due to internal events other than module drop, and (2) the risk associated with module drop alone. This presentation provides useful insights given that a conservative evaluation of potential module drop results in an LPSD risk that is several orders of magnitude greater than the risk associated with internal event initiators. Even with the conservatisms, both risks were calculated to be very small.

<u>Core Damage Frequency</u>

The mean value of the CDF due to internal events for a module during LPSD conditions is calculated to be 4.9E-13 per calendar year; the 5th and 95th percentile values are 1.4E-14 per calendar year and 1.7E-12 per calendar year, respectively.

The mean CDF due to module drop, MD-CD, is calculated to be 8.8E-08 per calendar year; the 5th and 95th percentile values are 1.5E-08 per calendar year and 2.5E-07 per calendar year, respectively. This frequency is equally divided between POS3 and POS5.

Large Release Frequency

The mean value of the large release frequency due to internal events for a module during LPSD conditions is calculated to be 2.0E-14 per calendar year; the 5th and 95th percentile values are 2.1E-16 per calendar year and 7.4E-14 per calendar year, respectively.

Analysis shows that the scrubbing effect of the water in the reactor pool reduces the offsite dose to only a small fraction of the large release definition, and therefore precludes a large release following a module drop. Thus, a dropped module event does not contribute to the large release frequency.

Significant Core Damage and Large Release Sequences

The significant CDF sequences contain three initiating events: spuriously open ECCS valve, loss of DC power, and reactor coolant system LOCA inside containment. All of the significant sequences involve an incomplete ECCS actuation. The increased significance of the spurious ECCS valve opening initiator in the LPSD probabilistic risk assessment is because the IAB is not credited for reducing the frequency of a spurious ECCS valve opening in POS1 or POS6, which increases the initiating event frequency for those POSs by several orders of magnitude.

The significant LRF sequences involve an unisolated CVCS pipe break outside containment in POS1, POS6, or POS7, followed by a series of failures that prevent the CVCS or CFDS from injecting coolant into the CNV. These sequences are not significant in POS2 and POS5 due to the short duration of applicability for these initiating events.

Module drop sequences are significant only in POS3 and POS5.

Significant Cutsets

Table 19.1-69 provides the top ten CDF and LRF cutsets for internal initiating events during LPSD operating modes. The cutsets for internal event initiators indicate that risk is distributed over a range of initiators and random failures. The cutsets associated with module drop contain very few events, reflecting the fact that mitigating actions are not credited.

Risk Significance

As discussed for the full-power operational mode, the PRA for LPSD provides insights into the risk significance of SSC and operator actions with regard to CDF for the low power/shutdown mode. Table 19.1-70 summarizes the candidate risk significant components and operator actions associated with internal event initiators.

Key Assumptions

Key assumptions for the LPSD probabilistic risk assessment relate to containment capability, reactor shutdown status, initiating event frequency, system availability and operator actions. The key assumptions, applicability to each POS and basis for the assumption are summarized in Table 19.1-71.

Uncertainties

As with the full power PRA, parameter uncertainty for the LPSD probabilistic risk assessment is characterized by probability distributions associated with the calculated results. Uncertainty distributions associated with internal initiating events are the same as used in the full-power model. Uncertainty distributions associated with module drop are lognormal with an error factor of 10, consistent with the internal events distribution.

Model uncertainties that are unique to the LPSD probabilistic risk assessment are:

- Duration of each POS -- The duration of each POS is based on engineering assumptions without operating experience. Actual POS durations, especially in early refueling outages, may be longer. Initiating event frequencies, and consequently the CDF and LRF, are proportional to POS durations.
- Damage to a dropped module -- There is considerable uncertainty regarding the potential damage to a module in the unlikely event of a drop.

Sensitivity Studies

The uncertainty associated with POS durations is accounted for in the conservative error factors used the initiating event frequencies. The uncertainty associated with damage to a module, if dropped, is addressed by simplified modeling of potential damage which accounts for location of components, movement paths and design capabilities.

The values of CDF and LRF reported in Section 19.1.6.2 are truncated at 1E-15, which is consistent with other hazard analyses. A sensitivity study is performed to determine an appropriate truncation level for the LPSD hazards consistent with the requirement stated in Section 19.1.4.1.1.7 and Section 19.1.4.2.1.7 that each successive decade reduction does not result in an increase to CDF or LRF of more than five percent. To meet this criterion, a truncation level of 1E-18 is applied. At this truncation, the point estimate of the CDF is 6.7E-13 per calendar year, and the LRF is 3.9E-14 per calendar year.

Key Insights

Key insights from LPSD internal events PRA are:

- Module drop accidents are the dominant contributors to core damage. The calculated probability of such events is low and a large release does not occur from a dropped module, even if the containment is damaged, due to radionclude scrubbing by the reactor pool.
- Passive decay heat removal and the absence of reduced inventory in POSs preclude potential accident initiators associated with drain down events, reduced inventory conditions, and failure of a residual heat removal system.
- Plant operating states with the longest durations, POS 2 and 4, have the lowest risk because safety functions are achieved passively and the core directly interfaces

with reactor pool water. As a result, the module is not susceptible to internal and external initiating events.

19.1.6.3 Safety Insights from the External Events Probabilistic Risk Assessment for Low Power and Shutdown Operation

The external events evaluations discussed in Section 19.1.5 for at-power operation, are also considered for LPSD risk. Section 19.1.6.3.1 through Section 19.1.6.3.5 address seismic, internal fire, internal flood, external flood, and high-winds external events, respectively.

19.1.6.3.1 Seismic Risk during Low Power and Shutdown

The SMA covers both fullpower operation and LPSD states. A nominal refueling outage for a single module is provided in Table 19.1-65 and occurs every two years. Using this information results in a 1.4 percent probability that the module is in a state other than fullpower operation. This percentage does not account for outages that do not involve refueling. The LPSD probabilistic risk assessment is limited to a nominal refueling outage and does not address expected frequency or duration of other LPSD evolutions.

The module is therefore approximately two orders of magnitude more likely to be at fullpower than LPSD during the occurrence of an earthquake. As such, the risk of the LPSD configuration can be screened out for contribution to seismic risk whenever the potential seismic consequences during LPSD are bounded by the full power consequences.

For seismic events, the only potential specific risk to an NPM during LPSD is during the transport phase before and after refueling, when the RBC is bearing the load of the module. When the RBC is not bearing the load of the module, stresses on crane supports and seismic restraints from earthquake loadings are less, resulting in more margin to failure. At other times during refueling, the module reactor and containment are open to the pool, with lower decay heat levels. Failure of the bridge seismic restraints is the failure mode corresponding to the controlling RBC fragility as discussed in Section 19.1.5.1.1.3.

Considering the nominal outage duration outlined in Table 19.1-65, the transportation time to the refueling area, and the transportation and reconnection time after refueling, the RBC is under load for about 30 percent of a nominal outage duration, resulting in a probability of one specific module being suspended by the RBC of 4.0E-3 during the two year operating cycle. As such, the relative seismic risk to a module suspended by the RBC in a LPSD configuration is low.

Furthermore, because the RBC fragility analysis was performed considering a loaded module, seismic risk is overestimated for a condition when the RBC is unloaded. The specific seismic risk to the module being transported is bounded by the risk of a loaded RBC seismic failure during normal operation. It therefore follows that there is no additional specific seismic risk to the NPM during LPSD conditions.

19.1.6.3.2 Internal Fire Risk during Low Power and Shutdown

In the same manner as described in Section 19.1.5.2 for full power operation, the evaluation of LPSD fire risk is developed using the LPSD model for internal events and adapting the model to incorporate aspects of fire that differ from the corresponding aspects of the internal events model.

An evaluation of each POS during LPSD operations is performed and presented in Table 19.1-72, along with its susceptibility to an internal fire. The analysis for the internal fire risk during LPSD concludes that because of the limited time (frequency and duration) that the module is in each POS during LPSD operations, as discussed in Section 19.1.6.1, and the fail-safe nature of the safety systems, internal fire contributes insignificantly to the risk when in LPSD modes.

19.1.6.3.3 Internal Flood Risk during Low Power and Shutdown

As described in Section 19.1.5.3 for full power operation, the evaluation of internal flood risk associated with LPSD is developed using the LPSD model for internal events and adapted to incorporate aspects of internal floods that differ from the corresponding aspects of the internal events model.

An evaluation of each POS during LPSD operations is performed and presented in Table 19.1-73 along with its susceptibility to an internal flood. The analysis for the internal flood risk during LPSD concludes that because of the limited time (frequency and duration) that the module is in any POS during LPSD operations, as discussed in Section 19.1.6.1, and the fail-safe nature of the safety systems, internal flood contributes insignificantly to the risk associated with LPSD. Thus, CDF and LRF for internal floods during LPSD are not calculated.

19.1.6.3.4 External Flood Risk During Low Power and Shutdown

As described in Section 19.1.5.4 for full power operation, the evaluation of external flood risk associated with LPSD is developed using the LPSD model for internal events and adapted to incorporate aspects of external floods that differ from the corresponding aspects of the internal events model.

Similar to the analysis for full power operation outlined in Table 19.1-55, the LOOP event tree bounds potential external flooding effects during LPSD. An evaluation of each POS during LPSD operations is performed and presented in Table 19.1-74 along with its susceptibility to an external flood. The analysis for the external flood risk during LPSD concludes that because of the limited time (frequency and duration) that the module is in any POS during LPSD operations, as discussed in Section 19.1.6.1, and the fail-safe nature of the safety systems, external flood contributes an insignificant amount to the risk when in LPSD modes. Thus, a CDF and LRF for external floods during LPSD are not calculated.

19.1.6.3.5 High-Wind Risk during Low Power and Shutdown

As described in Section 19.1.5.5 for full power operation, the evaluation of high-wind risk associated with LPSD is developed using the LPSD model for internal events and adapted to incorporate aspects of the high-wind hazard. As was the situation with the full power high-wind evaluation, and outlined in Table 19.1-59, the LOOP event tree bounds potential high wind effects during LPSD.

The susceptibility of equipment damage due to an extreme high-wind event is summarized in Table 19.1-75. Following the hazard methodology presented in Section 19.1.5.5.1, the overall strike frequency during LPSD operations is calculated by adjusting the frequency for each applicable POS based on the duration in the POS. The hurricane strike frequency for LPSD was also adjusted for events that occurred during shutdown conditions.

Core Damage Frequency

The point estimate CDF values for extreme high winds during LPSD are:

- tornado in POS1: 7.5E-14 per mcyr
- tornado in POS7: 6.8E-14 per mcyr
- hurricane in POS1: 5.4E-13 per mcyr
- hurricane in POS7: 4.9E-13 per mcyr

In POS 1 and POS 7, risk is dominated by sequences that involve a failure to recover power before an ECCS actuation and an incomplete ECCS actuation.

Large Release Frequency

The point estimate LRF values for extreme high winds during LPSD are:

- tornado in POS1: <1E-15 per mcyr
- tornado in POS7: <1E-15 per mcyr
- hurricane in POS1: <1E-15 per mcyr
- hurricane in POS7: <1E-15 per mcyr

Dominant risk sequences associated with the high-wind LRF frequency during LPSD are not identified because of their exceedingly low calculated frequency.

Significant Cutsets

Cutsets are not included for LPSD because the results are similar to those associated with full power operation, as indicated in Table 19.1-62, but are not explicitly listed because of the exceedingly low calculated frequency.

Risk Significance

Risk significant SSC were identified in the high-wind evaluation at full power. There are no unique risk significant SSC or high-wind related operator actions for LPSD.

Key Assumptions

Key assumptions specific to the LPSD risk assessment for high winds are:

- an extreme high wind is assumed to result in a LOOP
- the duration of each POS is as defined in Table 19.1-65

Table 19.1-61 provides key assumptions associated with the full power evaluation, which are also applicable to the LPSD evaluation.

Uncertainties

The LPSD mode does not introduce uncertainties that have not been identified in the full power evaluation of high winds. Parametric uncertainty associated with the LPSD evaluation is reflected in parametric ranges on the risk metrics. There is no model uncertainty that is unique to the LPSD evaluation of high winds.

Sensitivity Analyses

There are no sensitivity cases associated with the high winds evaluation for LPSD.

19.1.7 Multi-Module Risk

The risk associated with operation of a single module is discussed in Section 19.1.4 through Section 19.1.6. This section addresses the risk associated with operation of multiple modules. Section 19.1.7.1 describes the internal events risk evaluation of multiple module operation. A systematic process, illustrated in Figure 19.1-38, was used to evaluate the design capability and identify risk significant human errors. Section 19.1.7.2 provides results for the risk associated with internal events for full power operation. Section 19.1.7.3 provides insights regarding the risk associated with external events for full power operation. Section 19.1.7.4 provides insights regarding the risk associated with LPSD operation.

19.1.7.1 Description of the Multiple-Module Risk Evaluation

The Level 1 PRA for a single module provides the basis for evaluating the risk associated with a multiple module plant; the intent of the multiple module (multi-module) PRA is to identify and quantify postulated accident sequences that lead to core damage in multiple modules. The multi-module (MM) modeling approach described in this section does not identify the specific module or set of modules involved in an accident sequence. Rather, the methodology identifies the characteristics and associated risk to two or more modules given an accident involving one module.

The MM PRA uses the single module PRA accident sequence logic and makes parametric adjustments to single module basic events to account for MM configurations and the associated likelihood of extension to multiple modules. The intent is to identify the possible ways in which modules could be coupled from a risk perspective. The simplest coupling of multiple modules could occur through a shared system. Less obvious coupling could be caused by characteristics such as like-manufacturer, similar manufacturing techniques, similar testing and maintenance activities, and operation in similar environments.

The parametric adjustments to the single module model are made at the cutset level using multi-module adjustment factors (MMAFs) and multi-module performance shaping factors (MMPSFs). An MMAF is a conditional occurrence or failure probability that an event which has occurred in one module occurs in more than one module. Each MMAF is assigned a value between zero and one. An MMPSF is a multiplicative factor that is greater than or equal to one. An example is a human error for a single module that does not directly affect another module. Rather, the occurrence of the error for one module increases the likelihood that such an error could occur in additional modules. The MMPSF accounts for the added complexities associated with an MM plant configuration not nominally considered in the base model analysis.

Coupling factors are applied to initiating events and to basic events.

19.1.7.1.1 Initiating Event Coupling

The initiating events associated with the multi-module evaluation are the same as those considered for a single module. Potential mechanisms that could couple an initiating event in one module to multiple modules are:

- age-related degradation (e.g., wear, chemistry effects)
- manufacturing defects
- similar phase transformations
- harsh environmental conditions
- common upset conditions (e.g., shared system events)
- site-wide conditions (e.g., external events such as flooding)

However, each characteristic does not apply to each initiating event. Table 19.1-77 summarizes the coupling characteristics, the associated MMAFs and their bases for initiating events. For example, as indicated in the table, an MMAF of 1.0 is assigned to each sequence cutset containing the site-wide initiating event of loss-of-offsite power. This implies that for a loss of off-site power event, the effects are wide spread throughout the plant and affect all modules. Conversely, age-related degradation is applied only to the initiating events associated with pipe failure. The MMAF of 0.01 implies that, given there is a pipe break in one module, there is a one percent chance that a similar pipe break occurs in at least one additional module relatively close in time (i.e., within the same 72-hour mission time).

19.1.7.1.2 Basic Event Coupling

A basic event represents a failure mode of a piece of equipment, human action or phenomena. Each basic event in the single module PRA is evaluated in terms of a multiple module “classification” to assign an MMAF for the multiple module PRA.

- Single Failure -- A single failure refers to a single SSC for an individual NPM being in a state in which it cannot perform its designed function for either a specific demand or specified mission time. Single failures are independent of other single failures; however, with any independent event, there is the possibility that coupling mechanisms are present that could propagate a specific failure to other modules. Single failures also include test and maintenance unavailability. The MMAF for a single event represents the conditional probability of a failure event occurring in two or more modules given occurrence in one module. An MMAF of ten percent is assigned to each single failure basic event based on engineering judgment.

- Common Cause Failures -- The failure of two or more like components performing a redundant function during a short period of time due to a single shared cause. The MMAF for CCFs represents the extension of existing CCF events in the single PRA model for one module to other modules. An estimate of thirty percent is applied as a conditional probability of CCF extended to two or more modules given a CCF in one module using engineering judgment.
- Shared SSC (Single failure)-- Represents the potential for a failure due to a shared component affecting multiple modules. An example of a common system is the CFDS, which is shared among six modules; an example of a shared structure is the reactor pool, which is common to all modules. To be classified as a shared SSC for the MM PRA, the failure event must nominally affect two or more modules simultaneously, not necessarily all twelve. Basic events in representing shared equipment are assigned an MMAF of 1.0. Table 19.1-76 summarizes the effect of a system failure for each of the systems shared by multiple modules. Systems associated with only a single module and systems used for LPSD operations or security are excluded from the evaluation. The postulated failure is considered to be the complete inoperability or unavailability of all functions of that system.
- CCF of Shared SSC -- In the same manner as MMAFs were developed for single failures of shared equipment failure, there is an MMAF equal to 1.0 for the CCF of shared redundant SSC.
- Human Failure Events -- Represents an SSC equipment, function, or initiation unavailability due to the action (or inaction) of a human. An MMPSF is applied to account for the added complexity of servicing a multiple module plant configuration compared to a single module.
- Shared Human Events -- Some HFEs involve operator actions on shared systems (e.g., the operator action to start the CTG, the operator action to align a CFDS train after maintenance or testing). An MMAF of 1.0 applies to these actions.
- Similar Plant Response -- Represents a similar (or same) sequence of events which would affect multiple modules simultaneously, hence a similar response for the multiple module analysis. In the PRA, there is one event with a similar response characteristic: recovery of offsite power prior to depletion of backup battery power. The response to recover offsite power is modeled as the same for every module and an MMAF of 1.0 is assigned.
- Physical parameters -- A physical parameter is a deterministic design parameter for SSC design, Technical Specifications, or expected performance (e.g., an RSV

setpoint). Assuming the same conditions exist for all modules, the same physical response is expected for all modules, hence an MMAF of 1.0 is applied.

- Passive Safety System Reliability ECCS Events -- Basic events are included in the single module PRA to account for passive failure of the ECCS due to thermal-hydraulic uncertainty. The dominant contributor for the ECCS passive safety system reliability events is reactor pool temperature. As the reactor pool is a shared system an MMAF of 1.0 is used.
- Passive Safety System Reliability DHRS Events -- Basic events are included in the single module PRA to account for passive failure of the DHRS due to thermal-hydraulic uncertainty. As the DHRS passive safety system reliability events are predominantly defined by module-specific constituent parameters, an MMAF of 0.1 is used.
- Testing and maintenance events are assigned the same MMAFs as the events defined for other equipment failure modes. For example, if a piece of equipment is shared among multiple modules, the test and maintenance event for that component is also a shared event with the associated MMAF.
- SGTF events are assigned a value of 0.1. This is an order of magnitude higher than the MMAF for pipe break initiators. The value is based on engineering judgment of the uncertainty to which steam generator chemistry and environmental conditions may have a comparable effect on multiple modules.
- CVCS Pipe Break Location/Size events are assigned as a physical parameter MMAF with a value equal to 1.0. The event models the possibility that a LOCA flow rate is insufficient to engage the CVCS excess flow check valve to isolate containment.
- RSV Demand Probability Event considers the probability that an RSV is demanded to open. It is assigned as a physical parameter event with a MMAF of 1.0 because the condition causing an RSV demand in one module is assumed to be the same in multiple modules.

Table 19.1-78 summarizes the coupling characteristics, the associated MMAFs and their bases for basic events. For example, as indicated in the table, a shared SSC fault affects all modules as indicated by an MMAF of 1.0.

19.1.7.1.3 Quantification of Multiple Module Risk

As indicated earlier, the multi-module model is built directly from the single module PRA model. Changes to base case data, logic flag sets, linking rules, event tree and fault tree logic are not required to apply the multi-module methodology. The coupling factors are applied with post-processing rules to the single module PRA results. Thus, The CDF for two or more modules was quantified using the single module internal events PRA and applying multi-module post processing rules to add the coupling factors to each cutset. Quantification was performed with the SAPHIRE code using a 1.0E-15 truncation level.

The MMAFs and MMPSFs do not account for the specific number of modules, that is, the resulting risk metrics of MM-CDF and MM-LRF are judged to be bounding regardless of whether two or twelve modules are being considered.

Further, timing of multiple events is not explicitly addressed in the methodology. For example, a pipe failure in multiple modules, even if it were to occur, would likely not occur at the same time for all modules. This would afford time for diagnostic and mitigating measures that are not credited.

Another consideration with this methodology is the correlation with regards to module component location. Assumed coupling mechanisms are likely to be highly dependent on location. For instance, the RVVs in one module are not likely to be closely coupled to the RVVs in another module, even for adjacent modules. This is because the RVVs are attached to different reactor pressure vessels and reside in separate containment vessels. While the design of two modules is similar, it is unlikely that environmental conditions would propagate in such a way to produce high correlation.

19.1.7.2 Results of the Multiple Module Risk Evaluation at Full Power

Core Damage Frequency

The multi-module core damage frequency is defined as "MM-CDF." It is conservatively assumed that, if more than one module is affected, all modules in the plant are affected. Thus, when evaluating the risk from multiple module operation, the calculated MM-CDF applies to a two-module configuration up to, and including a twelve-module configuration.

The mean value of the MM-CDF due to internal events for multiple modules was calculated to be 4.1E-11 per mcyr, that is, on the order of ten percent of the CDF calculated for a single module. The 5th and 95th percentile values are 7.2E-13 per mcyr and 1.5E-10 per mcyr, respectively. Figure 19.1-39 provides the point estimate MM-CDF by internal event initiator. As indicated in the figure, over half of the MM-CDF is associated with the site-wide LOOP initiating event.

Large Release Frequency

As defined in Section 19.1.4.2.1.4, a large release is defined as a release producing 200 rem at the site boundary fence for a single module. Using the same definition of "large release,", multi-module large release frequency (MM-LRF), is the frequency of a single module large release accident from two or more modules.

The mean value of the MM-LRF due to internal events for multiple modules was calculated to be 1.7E-13 per mcyr; the 5th and 95th percentile values are 2.4E-16 per mcyr and 5.2E-13 per 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 make up 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 make up 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 19.1-79 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 the 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.

Risk Significance

Consistent with the risk significance determination methodology described in TR-0515-13952-A, 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.

Key Assumptions

Key assumptions for the MM-PRA are:

- MMAF values are based on engineering judgment.
- 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.
- The 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 due to an initiating event.

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

A sensitivity study was performed to evaluate the effect of variation in the MMAF coupling values.

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 (Loss of RCS inventory, pipe break) provided in Table 19.1-77 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, in comparison to the single-module CDF.
- MM-LRF is reduced by approximately an order of magnitude, in comparison to the single-module LRF.
- 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.

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; safety-related systems are module-specific and functionally independent of shared systems and other modules. Further, the MM LRF is nearly two orders of magnitude less than the base model results. 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, operator actions are not 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.

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, 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 19.1-81 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 was identified in which a fire could affect the DHRS for multiple modules if multiple hot shorts occur. Thus, an additional contribution to the DHRS unavailability for the multiple module evaluation is included in the PRA model to reflect this possibility. Conversely, no internal flood was found that could affect the RSVs for multiple modules. Thus, there is not a contribution to RSV unavailability from internal flooding for the multiple module evaluation.

Seismic events

Earthquakes, by their nature, affect multiple modules 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 module core damage scenario as applying to all modules 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 module, as well as multiple modules, approaches 1.0. At lower severity earthquakes, differences among modules 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 modules affected.

A plant level HCLPF is provided in Section 19.1.5.1.2. The bounding structural event is weldment failure on the crane bridge seismic restraints; the crane is assumed to be bearing load for the calculation of this fragility. Although the physical footprint of the crane structure spans multiple modules, catastrophic crane bridge collapse into the reactor pool with resultant damage to multiple modules is highly unlikely based on the following:

- A postulated earthquake's peak acceleration is generally too short in duration relative to the period of seismic loading necessary to significantly affect the crane bridge structure.
- The crane bridge is a large structure with varying weight distributions (depending on the location of the module lifting adapter); thus, simultaneous failures of multiple seismic restraints is unlikely.
- The length of the crane bridge girders is greater than the width between opposing pool walls; thus, the girders would remain on the wall ledge in the event of a seismically-induced crane collapse.

Structural events potentially affecting all modules require low likelihood seismic events with high ground acceleration. The seismic capacities of the walls and other structures evaluated for the SMA are higher than that of the crane weldment.

<u>Internal Fire</u>

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 modules. 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 module to shut down, but given the fail-safe design of the decay heat removal system, 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 module.

<u>Internal Flood</u>

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 modules. 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 flooding event is through the nonsafety-related makeup systems, CVCS and CFDS. Neither of these systems are credited in the building where this flood would need to occur.

An internal flood may create the demand for more there one module to shut down, but given the fail-safe design of the decay heat removal system, 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 module.

External Flood

In terms of initiating an upset to steady-state operations, operators are expected to perform a controlled shutdown on all operating modules when thresholds are reached that indicate an external flood could affect plant SSC. If there were insufficient warning, a LOOP initiating event at full power could occur for all modules.

The system insights show that the only common susceptibility to an external flood is on the EDSS support system. Although the EDSS is a module-specific system, the EDSS subsystems for all modules are located on the 75' and 86' elevations of the RXB. When flood levels reach the EDSS equipment, solenoids on safety-related systems de-energize and associated valves go to their fail-safe position.

The common MCR and common remote shutdown station are both susceptible to an external flood. However, because of the passive nature of the DHRS, ECCS, and CIVs, once these systems have been successfully actuated, there is no further need for electric power or operator actions.

The effect of an external flood is essentially that of a station blackout following a loss of power, which is also analyzed in the full-power internal-events PRA. An external flood affects all modules. A review of mitigating systems shows that there is no indication of coupling mechanisms that would affect the ability of multiple modules to safely shut down in response to an external flood. Given the fail-safe design of the decay heat removal system, ECCS, and CIVs, there are no multi-module dependencies that result in an elevated conditional probability of core damage or large release given core damage in the first module.

High Winds

In terms of initiating an upset to steady-state operations, a high-wind event results in a LOOP including loss of the EHVS and result in the MPS initiating a reactor trip on all modules.

The system insights show that the only susceptibility to a high-wind event is a loss of AC power and reactor trip. In cases where power is not restored within 24 hours, safety systems go to their fail-safe position. Because of the passive nature of the decay heat removal system, ECCS, and CIVs, once these systems have been successfully actuated, there is no further need for electric power or operator actions.

The effect of a high-wind event is basically that of a reactor trip and loss of power, which is analyzed in the full-power internal-events PRA. A high-wind event affects all modules with a demand to respond. A review of mitigating systems shows that there is no indication of coupling mechanisms that would affect the ability of multiple modules to safely shut down in response to a high-wind event. Specifically, a high-wind event would create the demand for all modules to shut down, but given the fail-safe design of the decay heat removal system, 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 module.

19.1.7.4 Insights Regarding Low Power and Shutdown for Multi-Module Operation

Evaluation of full-power multiple module operation provides insights into the risk associated with LPSD. The full-power evaluations of internal and external initiating events indicate that modules are largely independent. In a twelve-module configuration, and a two-year fuel cycle, one module enters a LPSD configuration for refueling every two months. As discussed in Section 19.1.6.1, the module being refueled is moved to the refueling area of the reactor pool and use of the personnel and equipment involved in the refueling (and maintenance activities that are not performed on-line) does not interfere with the operation of other modules.

The unique LPSD activity that potentially affects multiple modules is associated with module movement. Section 19.1.6.1.2 provides the initiating event frequencies applied to a potential module drop during LPSD operation. To consider the possibility that a dropped module could affect multiple modules, potential drop scenarios were evaluated:

- Single module accident -- The dropped module falls toward the centerline of the reactor pool, either directly, or after striking a bay wall. The module comes to rest horizontally on the floor.
- Two-module accident -- The dropped module strikes an operating module at the platform level, resulting in damage to both the dropped module and the operating module. The leftmost three dropped modules in Figure 19.1-41 illustrate this.
- Three-module accident -- The dropped module falls toward an operating module, striking it at the platform level. The bottom of the dropped module then slides across the floor and strikes a third module on the other side of the reactor pool. The rightmost dropped module in Figure 19.1-41 illustrates this.

A three-module accident, illustrated on the right side of Figure 19.1-41, requires that the dropped module first strike an operating module at a sufficient inclination to begin sliding backwards after the contact. The dropped, sliding module may then contact a second operating module at its base. The other operating bays present a smaller visible angle and make it less likely that the bottom of the dropped module is able to slide into a module across the pool. Additionally, a three-module accident is judged to be not credible if the module drop occurs in the refueling area, because its base is angled away from the operating area and would slide farther from the operating modules.

If the dropped module remains partially upright, such as if it is supported by another module or RXB structure, it is assumed that core damage is avoided; conversely, if it is not supported and falls to the floor core damage is assumed to occur.

The effects of a module being struck by a dropped module are determined by engineering judgment. Automated signals are not generated by a dropped module. An automated signal is generated for an operating module only if the drop creates a condition that reaches a safety setpoint. It is anticipated that operators will monitor a module transport and respond to the effects of a dropped module by ensuring that the appropriate automatic functions occur for the conditions and taking follow-up manual actions, as needed (e.g., tripping an operating module).

If the module is struck near the top, the DHRS piping or heat exchangers may be damaged, rendering one or both trains unavailable. If the operating module platform is struck with sufficient force, additional pipe breaks may occur, leading to a CVCS line break outside containment. If the module is struck near the bottom, as in a three-module accident, the collision is expected to cause a torque about the module support lugs, resulting in similar stresses to the piping on top of the operating module. In both cases, the CNV is unlikely to be breached due to the relatively low velocity of impact, caused by the dropped module falling only a short distance through a resistive medium (i.e., the water in the reactor pool).

A struck module being dislodged from its operating bay is not judged to be credible as the module supports limit horizontal motion, and the weight of the module and downward angle at which it is struck prevents it from being lifted high enough to escape its bay.

Thus, it is assumed that a dropped module event could result in the dropped module incurring core damage and the struck modules incurring an initiating event at full power. The dropped module is assumed to also incur damage which fails its CNV. In such an occurrence, a radionuclide release is assumed. However, as the event occurs under a minimum of 50 feet of water in the reactor pool, a large release would not occur due to the scrubbing effect of the reactor pool water.

19.1.8 Probabilistic Risk Assessment-Related Input to Other Programs and Processes

The PRA supporting the design certification has been used to support the NuScale design and provides a basis for COL applicant development of a site-specific PRA. The following sections summarize the uses of the PRA.

19.1.8.1 Probabilistic Risk Assessment Input to Design Programs and Processes

As discussed in Section 19.1.1.1 the uses of the PRA during the design phase are summarized in Table 19.1-1, which also indicates the applicable section in which the PRA application is discussed. The following sections address specific applications of the PRA, several of which rely on the updated site-specific PRA.

19.1.8.2 Probabilistic Risk Assessment Input to the Maintenance Rule Implementation

The Maintenance Rule, prescribed by 10 CFR 50.65, is implemented by the licensee. Use of the site-specific PRA in supporting the Maintenance Rule is determined by the program for monitoring the effectiveness of maintenance, which is addressed in Section 17.6.

19.1.8.3 Probabilistic Risk Assessment Input to the Reactor Oversight Process

The Reactor Oversight Process, the NRC program to assess the safety of an operating commercial nuclear power plant, is based in part on risk insights. At the design certification stage, the Reactor Oversight Process is not applicable. However, the PRA developed for the design certification provides the basis for an as-built, as-operated PRA for a specific operating site. The site-specific PRA is used to support the Reactor Oversight Process, including specific safety and performance metrics.

19.1.8.4 Probabilistic Risk Assessment Input to the Reliability Assurance Program

The Reliability Assurance Program, as described by SECY-94-084 (Reference 19.1-33), SECY-95-132 (Reference 19.1-34) and related guidance, has been implemented at the design certification stage to support development of the Design Reliability Assessment Program, as discussed in Section 17.4.

19.1.8.5 Probabilistic Risk Assessment Input to the Regulatory Treatment of Nonsafety-Related Systems Program

The PRA is used to support the identification of nonsafety-related SSC that are within the RTNSS scope at the design certification stage. The scope, criteria and process to determine SSC within the RTNSS program are discussed in Section 19.3.

19.1.8.6 Probabilistic Risk Assessment Input to the Technical Specifications

The PRA provides input to the technical specifications from several perspectives:

- Criterion 4 of 10 CFR 50.36(c)(2)(ii)(D) requires that a limiting condition of operation be established for an SSC which operating experience or PRA has shown to be significant to public health and safety. The design certification PRA is used to identify SSC meeting this criterion by applying the quantitative criteria discussed in Section 19.1.4.1.1.9. (See Section 16.1.1.)
- Surveillance frequencies in the technical specifications are consistent with assumptions made in the design certification PRA.
- The PRA may be used to support development of Risk Managed Technical Specifications, as described by NEI 06-09 (Reference 19.1-5).
- The PRA may be used to support development of a Surveillance Frequency Control Program as described by NEI 04-10 (Reference 19.1-4).

19.1.9 Conclusions and Findings

Key insights from the Level 1 and Level 2 PRA for internal events and external events, full-power and LPSD modes, as well as single and multiple module operation were provided in earlier sections. The analysis demonstrates that the NuScale Power Plant design incorporates features that produce an exceedingly low risk to public health and safety. Key results of the analysis and additional risk perspectives are provided in this section, specifically:

- conformance with safety goals

- perspective of the NuScale small core with respect to safety goals
- focused PRA insights
- unique system capability

19.1.9.1 Conformance with Safety Goals

The safety goal policy statement and subsequent guidance provide quantitative objectives for evaluating conformance with the qualitative goals associated with public health and safety. The quantitative results of the PRA, summarized in Table 19.1-80, demonstrate that the risk associated with operation of an NPM is substantially less than defined by the safety goals. The table also indicates that additional risk associated with multiple module operation is small. As indicated in the table:

- the mean value of the CDF of an NPM is 3.0E-10 per mcyr as compared to the CDF safety goal of 1.0 E-4 per reactor year.
  - The ATWS contribution to CDF is 2.2E-11 per mcyr, significantly less than the target of 1.0E-5 per reactor year provided in SECY 83-293 (Reference 19.1-65).
  - With regard to a multi-module configuration, the MM-CDF is about 10 percent of the CDF.
- the mean value of the LRF of an NPM is 2.3E-11 per mcyr as compared to the LRF safety goal of 1.0 E-6 per reactor year.
  - With regard to a multi-module configuration, the MM-LRF is about one percent of the LRF.
- the composite CCFP of a module is less than the safety goal of 0.1.
- the evaluated external events (seismic, internal fire, internal flood, external flood, and high winds) do not pose a significant risk to the plant.

The CDF and LRF risk metrics illustrate conformance with the quantitative health objectives defined in Reference 19.1-36. Conformance with the prompt fatality quantitative health objective (QHO) is illustrated by an LRF that is well below the surrogate risk metric of less than 1×10^{-6} per reactor year. Similarly, risk results show that NuScale demonstrates conformance with the latent cancer QHO as illustrated by a CDF that is well below the surrogate metric of less than 1×10^{-4} per reactor year.

COL Item 19.1-8: A COL applicant that references the NuScale Power Plant design certification will confirm the validity of the "key assumptions" and data used in the design certification application probabilistic risk assessment (PRA) and modify, as necessary, for applicability to the as-built, as-operated PRA.

19.1.9.2 Perspective of the NuScale Small Core with Respect to Safety Goals

The safety goals are independent of design, thus the size of the potential radionuclide source term is not considered in the core damage or large release frequency safety goals. These goals are surrogates for potential public health consequences. With regard to potential consequences, an additional insight into the significance of a core damage event can be gained by considering the small NuScale radionuclide source term.

As a small reactor, the potential radionuclide source term associated with a severe accident is much smaller than that associated with typical currently operating and large advanced plant designs, e.g., the source term is five percent of that associated with a 1000 MWe design. Even the postulate of severe accidents occurring in all modules would produce a source term that is only a fraction of that associated with a larger design. Thus, while the risk to public health and safety is small as evidenced by the very low calculated CDF, LRF and CCFP risk metrics, the risk of operating a NuScale plant is further reduced because of the small potential radionuclide source term.

19.1.9.3 "Focused" Probabilistic Risk Assessment

An additional perspective on the CDF is gained by reporting results of a "focused PRA" which credits only safety-related SSC. In the focused PRA, SSC that are not safety-related are assumed to be failed. The focused PRA was performed as a sensitivity study to the full-power, internal events PRA with results provided in Table 19.1-22 and Table 19.1-31. The results illustrate that safety goals for CDF and LRF are met without reliance on nonsafety-related SSC. A focused PRA was also performed as a sensitivity to the LPSD probabilistic risk assessment; results show that safety goals are met without reliance on nonsafety-related SSC.

19.1.9.4 Unique System Capability

The NuScale design provides the unique capability to employ power-independent, fail-safe safety systems that rely on passive heat transfer to the UHS to achieve stable long-term core cooling for an extended time period with no operator action, no AC or DC power, and no inventory makeup to the RCS or UHS. This capability is illustrated by the following accident sequence from Figure 19.1-9, Sequence 4:

- a LOOP occurs as indicated by initiating event EHVS--LOOP-----
- onsite AC power sources are initially unavailable and not recovered
- automatic reactor shutdown occurs
- DHRS valves open
- 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 American Society of Mechanical Engineers/American Nuclear Society, "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), New York, NY.

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

19.1-3 DC/COL-ISG-028, "Assessing the Technical Adequacy of the Advanced Light-Water Reactor Probabilistic Risk Assessment for the Design Certification Application and Combined License Application," U.S. Nuclear Regulatory Commission, November 2016.

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

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

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

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

19.1-8 NuScale Power, LLC, "Risk Significance Determination," TR-0515-13952-A, Rev 0.

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

19.1-10 U.S. Nuclear Regulatory Commission "Code Manual for MACCS2: Volume 1, User's Guide," NUREG/CR-6613 (SAND97-0594), May 1998.

19.1-11 U.S. Nuclear Regulatory Commission, "Rates of Initiating Events at US Nuclear Power Plants: 1987-1995," NUREG/CR-5750, February 1999 with subsequent updates including:

- 2013 Summary Update
- 2013 Data Tables

19.1-12 Electric Power Research Institute, "Program on Technology Innovation: Comprehensive Risk Assessment Requirements for Passive Safety Systems," EPRI #1016747, Palo Alto, CA, 2008.

19.1-13 International Atomic Energy Institute, "Progress in Methodologies for the Assessment of Passive Safety System Reliability in Advanced Reactors," IAEA-TECHDOC-1752, Vienna, Austria, 2014.

19.1-14 Not Used.

19.1-15 Not Used.

19.1-16 U.S. Nuclear Regulatory Commission, "Reevaluation of Station Blackout Risk at Nuclear Power Plants, Analysis of Loss of Offsite Power Events: 1986-2004," with subsequent updates including, "Analysis of Loss of Offsite Power Events 2013 Update," NUREG/CR-6890, 2005.

19.1-17 Electric Power Research Institute, "ATWS: A Reappraisal. Part 3. Frequency of Anticipated Transients," EPRI NP-2230, Palo Alto, CA, 1982.

19.1-18 U.S. Nuclear Regulatory Commission, "Seismic Safety Margins Research Program: Equipment Fragility Data Base," NUREG/CR-2680, January 1983.

19.1-19 U.S. Nuclear Regulatory Commission, "Seismic Safety Margins Research Program: Handbook of Nuclear Power Plant Seismic Fragilities," NUREG/CR-3558, June 1985.

19.1-20 U.S. Nuclear Regulatory Commission, "Seismic Fragility of Nuclear Power Plant Components," NUREG/CR-4659, August 1991.

19.1-21 Electric Power Research Institute, "A Methodology for Assessment of Nuclear Power Plant Seismic Margin (Revision 1)," EPRI NP-6041-SL, Palo Alto, CA, 1991.

19.1-22 U.S. Nuclear Regulatory Commission, "The SPAR-H Human Reliability Analysis Method," NUREG/CR-6883 (INL/EXT-05-00509), August 2005.

19.1-23 U.S. Nuclear Regulatory Commission, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," NUREG/CR-6928, Initial Issue 2007 and 2010 Update, September 2012.

19.1-24 Idaho National Laboratory, "Analysis of Loss-of-Offsite-Power Events 1997-2014," INL/EXT-16-37873, February 2016.

19.1-25 U.S. Nuclear Regulatory Commission, "Evaluation of JNES Equipment Fragility Tests for Use in Seismic Probabilistic Risk Assessments for U.S. Nuclear Power Plants," NUREG/CR-7040, April 2011.

19.1-26 Not Used.

19.1-27 U.S. Nuclear Regulatory Commission, "System Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE)," NUREG/CR-7039, Version 8, Volumes 1-7, June 2011.

19.1-28 Sandia National Laboratories, "MELCOR Computer Code Manuals," (Version 2.1), Vol. 1 through Vol. 3, Albuquerque, NM, August 2015.

19.1-29 U.S. Nuclear Regulatory Commission, "MELCOR Best Practices as Applied in the State of the Art Reactor Consequence Analyses (SOARCA) Project," NUREG/CR-7008, August 2014.

19.1-30 U.S. Nuclear Regulatory Commission, "State-of-the-Art Reactor Consequence Analyses Project Uncertainty - Analysis of the Unmitigated Short-Term Station Blackout of the Surry Power Station," (Draft Report), Agencywide Documents Access and Management System (ADAMS) Accession No. ML15224A001.

19.1-31 U.S. Nuclear Regulatory Commission, "Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process," NUREG-1829, April 2008.

19.1-32 Electric Power Research Institute, "Advanced Light Water Reactor Passive Plant Utility Requirements Document," Rev. 13, EPRI #3002000507, Palo Alto, CA, 2014.

19.1-33 U.S. Nuclear Regulatory Commission, "Policy and Technical Issues Associated With The Regulatory Treatment of Non-Safety Systems (RTNSS) In Passive Plant Designs," Commission Paper SECY-94-084, March 28, 1994.

19.1-34 U.S. Nuclear Regulatory Commission, "Policy and Technical Issues Associated With The Regulatory Treatment of Non-Safety Systems (RTNSS) In Passive Plant Designs (SECY-94-084)," Commission Paper SECY-95-132, May 22, 1995.

19.1-35 Not Used.

19.1-36 U.S. Nuclear Regulatory Commission, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement; Correction and Republication," Federal Register, Vol. 51, No. 162, August 21, 1986, pp. 30028-30033.

- U.S. Nuclear Regulatory Commission, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement," Federal Register, Vol. 51, No. 149, August 4, 1986, pp. 28044-28049. (Note: this was original publication, but 51 FR 30028 was published to correct errors)

19.1-37 U.S. Nuclear Regulatory Commission, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs," Commission Paper SECY-93-087, April 2, 1993, and the related SRM dated July 21, 1993.

19.1-38 U.S. Nuclear Regulatory Commission, "PRA Procedures Guide," NUREG/CR-2300, Vol. 1, Chapter 7, January 1983.

19.1-39 U.S. Nuclear Regulatory Commission, "An Approach for Estimating the Frequencies of Various Containment Failure Modes and Bypass Events," NUREG/CR-6595 Rev. 1, October 2004.

19.1-40 U.S. Environmental Protection Agency, “PAG Manual: Protective Action Guides and Planning Guidance for Radiological Incidents,” (Draft for Interim Use and Public Comment), March 2013.

19.1-41 U.S. Nuclear Regulatory Commission, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, February 1987.

19.1-42 U.S. Nuclear Regulatory Commission, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities," NUREG/CR-6850 (EPRI #1011989) Vol. 1 and Vol. 2 and errata, September 2005.

- U.S. Nuclear Regulatory Commission, “Fire Probabilistic Risk Assessment Methods Enhancements,” NUREG/CR-6850 (EPRI #1019259) Supplement 1, September 2010.

19.1-43 Nuclear Energy Institute, "Guidance for Post Fire Safe Shutdown Circuit Analysis," NEI 00-01, Rev. 2, Washington, DC, May 2009.

19.1-44 Nuclear Energy Institute, "Guidance for Post Fire Safe Shutdown Circuit Analysis," NEI 00-01, Rev. 3, Washington, DC, October 2011.

19.1-45 U.S. Nuclear Regulatory Commission, "Nuclear Power Plant Fire Ignition Frequency and Non-Suppression Probability Estimation Using the Updated Fire Events Database: United States Fire Event Experience Through 2009," NUREG-2169 (EPRI #3002002936), January 2015.

19.1-46 U.S. Nuclear Regulatory Commission, "Joint Assessment of Cable Damage and Quantification of Effects from Fire (JACQUE-FIRE)," NUREG/CR-7150 (EPRI #1026424, #3002001989), Vol. 1, October 2012, Vol 2, May 2014.

19.1-47 Nuclear Energy Institute, "External Flooding Integrated Assessment Guidelines," NEI 16-05, Revision 0, Washington, DC, April 2016.

19.1-48 U.S. Nuclear Regulatory Commission, "Tornado Climatology of the Contiguous United States," NUREG/CR-4461, Rev. 2, February 2007.

19.1-49 American Society of Civil Engineers, "Minimum Design Loads in Buildings and other Structures," ASCE 7-10ASCE, 2010, New York, NY.

19.1-50 American Nuclear Society/American Society of Mechanical Engineers, "Requirements for Low Power and Shutdown Probabilistic Risk Assessment," ANS/ASME 58.22-2014, New York, NY.

19.1-51 U.S. Nuclear Regulatory Commission, “Control of Heavy Loads at Nuclear Power Plants,” NUREG-0612, July 1980.

19.1-52 U.S. Nuclear Regulatory Commission, "Single-Failure-Proof Cranes for Nuclear Power Plants," NUREG-0554, May 1979.

19.1-53 Institute of Electrical and Electronics Engineers, "IEEE Guide To The Collection And Presentation Of Electrical, Electronic, Sensing Components, and Mechanical Equipment Reliability for Nuclear-Power Generating Stations," IEEE Standard 500-1984, New York, NY.

19.1-54 Quanterion Solutions Incorporated, "Quanterion Automated Databook: Electronic Parts Reliability Data 2014 (EPRD-2014), Nonelectric Parts Reliability Data 2011 (NPRD-2011), Failure Mode/Mechanism Distribution 2013 (FMD-2013)," Utica, NY.

19.1-55 Electric Power Research Institute, "An Analysis of Loss of Decay Heat Removal and Loss of Inventory Event Trends (1990-2009)," EPRI #1021167, Palo Alto, CA, 2010.

19.1-56 DC/COL-ISG-020, "Implementation of a Seismic Margin Analysis for New Reactors Based on Probabilistic Risk Assessment," U.S. Nuclear Regulatory Commission, March 2010.

19.1-57 Electric Power Research Institute, "Methodology for Developing Seismic Fragilities," EPRI #103959, Palo Alto, CA, 1994.

19.1-58 Electric Power Research Institute, "Seismic Fragility Applications Guide Update," EPRI #1019200, Palo Alto, CA, 2009.

19.1-59 Electric Power Research Institute, "Advanced Light Water Reactor Passive Plant Utility Requirements Document," Rev. 13, EPRI #3002000507, Palo Alto, CA, 2014.

19.1-60 U.S. Nuclear Regulatory Commission, "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment," NUREG/CR-5485, June 1998.

19.1-61 NUREG/CR-5497 - 2012 Update, "Common Cause Failure Parameter Estimations," U.S. Nuclear Regulatory Commission, January 2012.

19.1-62 Microsemi, "Reliability Report," Rev. 11, No. 51000001-11/05.13, Aliso Viejo, CA, May 2013.

19.1-63 Sandia National Laboratories, "Accident Source Terms for Light Water Nuclear Power Plants Using High-Burnup or MOX Fuel," SAND2011-0128, January 2011.

19.1-64 Not Used.

19.1-65 U.S. Nuclear Regulatory Commission, "Amendments to 10 CFR 50 Related to Anticipated Transients without Scram," Commission Paper SECY-89-293, July 19, 1983.

19.1-66 U.S. Nuclear Regulatory Commission, “State-of-the-Art Reactor Consequence Analyses Project, Volume 1: Peach Bottom Integrated Analysis,” NUREG/CR-7110, Rev. 1, May 2013.

Table 19.1-1: Uses of Probabilistic Risk Assessment at the Design Phase

Use	Applicable Section
Identify dominant risk contributors	Section 19.1.4.1.2, Section 19.1.4.2.2, Section 19.1.5.1.2, Section 19.1.5.2.2, Section 19.1.5.3.2, Section 19.1.5.4.2, Section 19.1.5.5.2, Section 19.1.6.2, Section 19.1.6.3, Section 19.1.7.2
With regard to capability in comparison to currently operating plants: • Address significant risk contributors of currently operating plants • Demonstrate that the design addresses known issues related to the reliability of core and containment heat removal systems at some operating plants (i.e., the additional Three Mile Island-related requirements in 10 CFR 50.34(f)) • Evaluate whether plant design, including potential effect of site-specific characteristics, represents a reduction in risk compared to currently operating plants	 • Section 19.1.3 • Section 19.2.6 • Section 19.1.3
Evaluate design robustness and tolerance of severe accidents	Section 19.2
Evaluate risk significance of human error including a characterization of the significant human errors that may be used as an input to operator training programs and procedure refinement	Section 19.1.4.1.2, Section 19.1.4.2.2, Section 19.1.5.1.2, Section 19.1.5.2.2, Section 19.1.5.3.2, Section 19.1.5.4.2
Evaluate conformance with NRC safety goals	Section 19.1.4.1.2, Section 19.1.4.2.2, Section 19.1.9.1
Assess the balance of preventive and mitigative features and consistency with SECY-93-087 (Reference 19.1-37) and associated SRM	Section 19.2.2
Support Design Reliability Assurance Program including RTNSS classification of SSC	Section 17.4, Section 19.3
Severe Accident Management Design Alternatives	Section 19.2.6
Support Regulatory Oversight Processes, for example, • Mitigating Systems Performance Index • Significance Determination Process	Section 19.1.8.3
Technical Specifications support • Design-specific surveillance frequencies • Criterion 4 of 10CFR50.36(c)(2)(ii)(D)	Section 19.1.8.6
Maintenance Rule (SSC classification)	Section 17.6
Human performance insights	Chapters 18, 19

Table 19.1-2: Design Features/Operational Strategies to Reduce Risk

Design Feature	Description	Effect on Risk
Primary cooling by natural circulation	NuScale design incorporates natural circulation cooling during almost all modes of operation (during startup circulation of the primary cooling is enhanced by using CVCS pumps).	• Absence of reactor coolant pumps means no threat of reactor coolant pump seal failures. • No dependence of electric power or seal cooling water for primary coolant circulation and hence less likelihood of a reactor trip due to forced flow transients. • Contributes to robust plant response during potential ATWS condition. Flow and hence heat transfer and reactivity control, is effectively self-regulated by the natural forces controlling flow through core.
Integrated primary cooling system design	All components of the primary cooling system are contained inside the RPV. This includes the pressurizer, steam generators, and the entire primary system cooling loop.	• No external reactor cooling system pipe results in less likelihood of a LOCA. • Steam generator tubes that are in compression (i.e., feedwater is on the inside and coolant circulates on the outside).
Internal (to RPV) helical-coil steam generator (SG)	Helical coil steam generator (SG) tubes wrap-around central riser inside the RPV. Primary coolant flows on outside of the tubes, with secondary, feedwater on inside.	• With primary, high-pressure coolant on outside of the SG tubes and the lower-pressure feedwater flow on the inside, the tubes are maintained in a constant state of compression. This is in contrast to the typical tensile stresses on the SG tubes in conventional plants. Maintaining the tubes in compression is expected to prevent crack propagation and reduce the likelihood of SG tube failure.
Passive, fail-safe ECCS	ECCS consists of 5 valves that fail-safe on a loss of power. Heat is transferred directly to the UHS by passive natural processes (i.e., condensation, natural circulation, convection and conduction)	• No dependence on support systems (i.e., AC or DC power, or service water) or operator action for heat transfer to the UHS. • ECCS is effective in maintaining core cooling for possible LOCA sizes. • No reliance on external sources of inventory addition to the RPV.
Passive fail-safe DHRS	Passive, natural circulation, closed-loop isolation condenser removes heat from the secondary side of the SGs.	• No electric power needed to remove heat from the secondary side of the SGs. • Closed-loop system does not need additional inventory. • Passive, electric-power independent plant response to unplanned reactor trip.
Small reactor core	Reactor core in each module is about five percent the size of a typical large PWR core.	• Small reactor core is easier to keep cool under both normal and abnormal conditions. (Cycling of just one of the two passive reactor safety valves is sufficient to maintain core cooling without DHRS or ECCS operation.) • Each core, in a plant of up to 12-modules, is contained in a separate RPV, which in turn is contained in a separate CNV. The distribution of the total plant core material, combined with the small size of each core, enhances the ability to cool the core passively. • Small reactor core results in relatively low heat load on RPV lower head in the unlikely event a severe accident results in core relocation to the lower head; in this configuration, analysis indicates that RPV failure does not occur.
No RPV penetrations below top of core	The RPV does not have penetrations below the refueling flange.	• No penetrations in the lower portion of the RPV means there is not a credible mechanism for draining the RPV and uncovering the core.

Table 19.1-2: Design Features/Operational Strategies to Reduce Risk (Continued)

Design Feature	Description	Effect on Risk
Vessel (RPV) within a vessel (CNV) design	The RPV is contained within the high-pressure/low-volume CNV. The CNV, which is partially immersed in the UHS, is designed to preserve primary system inventory in the event of a LOCA or an ECCS actuation.	• The CNV is partially immersed in the UHS; thus, it provides an efficient steam condensation surface that condenses inventory lost from the RPV and preserves it for recirculation back into the RPV. • CNV atmosphere is maintained at a near vacuum, which limits the available oxygen. Also, the near vacuum acts to insulate the RPV thereby obviating the need for insulating materials on the RPV, which eliminates the potential for lose material to interfere with coolant recirculation. • This vessel within a vessel design combined with ECCS results in a rapid equalizing of pressures between the RPV and the CNV, thereby precluding high pressure RPV failure associated with potential severe accidents. • The lack of concrete precludes the generation of non-condensable gases (i.e., concrete ablation) and long-term containment pressurization concerns.
Interfacing systems designed for full RCS pressure	The only system that directly interfaces with the RCS is the CVCS, which comprises four lines: RCS injection, RCS discharge, pressurizer spray, and RPV high point degas. All of these are designed for full RCS pressure and temperature.	• Limited number of interfacing systems and the design for full RCS operating system pressure and temperature significantly decreases the likelihood of an interfacing system LOCA (ISLOCA).
Fully engineered seismic class-1 UHS	The UHS is a subsurface water pool containing a large volume of borated water. The pool is stainless steel lined with a leak detection system imbedded in the floor.	• The NuScale UHS is not susceptible to becoming unavailable as a result of biofouling, weather-related conditions (e.g., freezing) or catastrophic external event. • Inventory in the UHS is sufficient to maintain cooling for 12 modules indefinitely.
Robust, aircraft impact resistant, seismic class 1 reactor building	Each of the 12 NPMs includes its own CNV. All 12 NPMs and the UHS are housed in the RXB, which is designed as a seismic class 1 structure and to withstand aircraft impact.	• The robust RXB provides an additional protective barrier between the reactor core and the environment.
Extensive use of fiber-optic controls	Both safety-related and nonsafety-related control systems use fiber optic cables as signal transmission media.	• Signal integrity ensured through triplication. • No potential for hot shorts to cause spurious operation.
Underwater refueling	Module disassembly and refueling take place under water in the UHS.	• CNV is flooded as a prerequisite to refueling; the RPV is not drained and hence there are no "mid-loop" operations or conditions that result in reduced coolant inventory. After the CNV is flooded, decay heat is passively transferred to the UHS by conduction and convection.

Table 19.1-3: Use of Probabilistic Risk Assessment in Selection of Design Alternatives

Design Issue	Purpose
Decay heat removal system design options	Optimize DHRS configuration among four options that are passive, single-active-failure-proof, and provide at least 72 hours of cooling.
Feedwater design options	Provide system reliability (unreliability) values for the various options that are being considered in the feedwater/auxiliary feedwater design decision.
Pressure locking options for ECCS valves	Evaluate design configurations involving “pressure locking” the ECCS valves to prevent them from opening at high pressure. Evaluate effect of diverse designs to eliminate CCF.
Decay heat removal system CIVs	Evaluate potential decay heat removal system containment isolation valve configurations.
Arrangement of reactor trip breakers (RTBs)	Sensitivity study for of the number and arrangement of reactor trip breakers on the reliability of the MPS.
Spurious opening of ECCS valves	Evaluate likelihood of a spurious partial opening event in an ECCS vent or recirculation valve.
Main steam isolation valve options	Evaluate feedwater and main steam isolation valve options.
Conditional core damage probability for station blackout	Examine the effect of a station blackout event on the safe shutdown capability.
Failure probability for RBC	Evaluate failure probability for RBC used for module movements.
ECCS valve reliability	Estimates the frequency of spurious ECCS valve open and probability that a single ECCS valve might fail to open upon on demand.
MPS common-cause failure and availability	Evaluate CCF failure; evaluate effect of online maintenance.

Table 19.1-4: Systems Modeled in the Probabilistic Risk Assessment

System*	Abbreviation	Summary Description
Chemical and volume control system	CVCS	As modeled in the PRA, the CVCS consists of a single loop with the DWS as the suction source for two parallel makeup pumps. The system provides the primary coolant makeup capability to remove core heat in the event of a LOCA.
Containment flooding and drain system	CFDS	As modeled in the PRA, the CFDS consists of two parallel pumps and associated valves, used to provide inventory, taken from the reactor pool, piped to the CNV, to remove core heat during a beyond design basis event.
Control rod drive system	CRDS	As modeled in the PRA, the CRDS includes the control rod assemblies which insert negative reactivity into the core; the CRDS is actuated by the RTS, which is part of the MPS.
Decay heat removal system	DHRS	As modeled in the PRA, the DHRS consists of two redundant trains, one feeding each SG. Each train of the DHRS is equipped with a passive isolation condenser type heat exchanger located in the reactor pool and two actuation valves. The system functions to remove core heat from the RCS.
Demineralized water system	DWS	As modeled in the PRA, the DWS consists of three parallel pumps, drawing suction from the common demineralized water storage tank, which discharges into a common header that feeds the CVCS.
Electrical power systems	EHVS EMVS ELVS EDSS BPSS	As modeled in the PRA, the electrical power systems includes parts of five plant systems: 13.8 kV and switchyard, medium voltage AC electrical distribution system, low voltage AC electrical distribution system, the module-specific portion of the EDSS, and the backup power supply system (BPSS) which includes the alternate AC power supply. The electrical systems provide power to the required loads during a plant transient.
Emergency core cooling system	ECCS	As modeled in the PRA, the ECCS consists of three independent RVVs and two independent RRVs, which open to allow recirculation of reactor coolant water between the reactor vessel and the CNV to remove core heat during a plant transient.
Module protection system	MPS	As modeled in the PRA, the MPS consists of four groups of instrumentation that supply signals to two divisions of the RTS and the ESFAS. It also provides signals to the MCR display for use by the operator, as well as data for control and indication.
Reactor coolant system	RCS	As modeled in the PRA, the RCS consists of two redundant reactor safety valves that respond to sequences which include increases in primary system pressure to the point of an RSV demand.
Ultimate heat sink	UHS	As modeled in the PRA, the UHS supports DHRS and ECCS as the UHS. The UHS also provides suction to the CFDS.
Containment system	CNTS	As modeled in the PRA, the CNTS consists of the CIVs that isolate the CNV and contain fission products in the event of a severe accident.

*The main steam and condensate and feedwater systems are not considered as mitigating systems in the PRA because all initiators are expected to generate a safety actuation signal to actuate DHRS (through the ESFAS and RTS) with isolation of the FWIVs and MSIVs.

Table 19.1-5: System Dependency Matrix

		Frontline PRA System							
		BPSS[A]	CFDS	CNTS[B]	CVCS	DHRS	ECCS	RCS[C]	RTS[D]
Support Systems	BAS[1]				X				
	CNTS[2]		X		X	X			
	DWS[1]				X				
	EDSS[3]		X		X				
	EHVS[4]	X							
	ELVS	X	X		X				
	MPS		X	X[5]	X	X[5]	X[5]		X[5]
	UHS		X			X	X		

Notes on support system dependencies (shaded boxes):

1. Although the PRA models the DWS to support CVCS injection, the BAS provides an immediate source of inventory and allows time for operators to locally align the DWS supply isolation valves following a reactor trip. The DWS pumps and isolation valves are powered from the ELVS.
2. As a support system, CNTS is modeled in the Level 1 PRA to open the CIVs (i.e., the CFDS and the CVCS) and close the CIVs and the backup isolation valves (i.e., the FWS and the MSS).
3. The EDSS is powered from the ELVS with backup power from batteries.
4. In the PRA, EHVS is powered from offsite power.
5. The NuScale design is fail-safe; in response to a loss of all power (AC and DC), the MPS actuates the RTS and the ESFAS (i.e., the CNTS, the DHRS, and the ECCS).

Notes on PRA frontline systems:

A. Includes the BDGs and a CTG as the AAPS.
B. As a frontline system, the CNTS is modeled to close the CIVs and backup FWS and MSS isolation valves.
C. In the PRA, the RCS modeled as the RSVs, provides RPV pressure relief.
D. In the PRA, the RTS includes the reactor trip breakers and the CRDS, including control rod assembly insertion.

Table 19.1-6: System Success Criteria per Event Tree Sequence

Event Tree	Seq. No.	RTS	CNV Isolation	DHRS	RSV	ECCS	CVCS	CFDS	End State	Thermal-hydraulic Simulation
CVCS--ALOCA-COC	1	S	S	S	--	--	--	--	OK	LCI-01T-1D0E0C0F0S-00-S
(Figure 19.1-2)	2	S	S	F	S	--	--	--	OK	LCI-02T-0D0E0C0F1S-00-S
	3	S	S	F	FO	S	--	--	OK	LCI-03T-0D1E0C0FSS-00-S
	6	S	F	--	--	S	--	S	OK	LCU-05T-0D1E0C1F0S-00-S
	9	F	S	--	S	--	--	--	OK	LCI-11A-0D0E0C0F1S-00-S
	10	F	S	--	FO	S	--	--	OK	LCI-06A-0D1E0C0FSS-00-S
CVCS--ALOCA-LOC	1	S	S	S	--	--	--	--	OK	LCI-01T-1D0E0C0F0S-00-S
(Figure 19.1-3)	2	S	S	F	S	--	--	--	OK	LCI-02T-0D0E0C0F1S-00-S
	3	S	S	F	FO	S	--	--	OK	LCI-03T-0D1E0C0FSS-00-S
	4	S	S	F	FO	F20	S	--	OK	LLI-02T-0D0E1C0FSS-00-S
	7	S	F	--	--	S	S	--	OK	LLU-01T-0D0E1C0F0S-00-S
	8	S	F	--	--	S	F	S	OK	LCU-05T-0D1E0C1F0S-00-S
	10	S	F	--	--	F20	S	--	OK	LLU-01T-0D0E1C0F0S-00-S
	12	F	S	--	S	--	--	--	OK	LCI-11A-0D0E0C0F1S-00-S
	13	F	S	--	FO	S	--	--	OK	LCI-06A-0D1E0C0FSS-00-S
	14	F	S	--	FO	F	S	--	OK	LEC-10A-0D0E1C0F0S-00-S
	17	F	F	--	--	S	S	--	OK	LLU-04A-0D0E1C0F0S-00-S
CVCS--ALOCA-CIC	1	S	S	--	--	S	--	--	OK	LCC-07T-0D1E0C0F0S-00-S
(Figure 19.1-4)	2	S	--	S	--	F	S	--	OK	LCC-01T-0D0E1C0F0S-00-S
	5	F	S	--	--	S	--	--	OK	LEC-13A-0D1E0C0F0S-00-S
	6	F	--	S	--	F20	S	--	OK	LCC-02A-0D0E1C0F0S-00-S
RCS---ALOCA-IC	1	S	S	--	--	S	--	--	OK	LEC-07T-0D1E0C0F0S-00-S
(Figure 19.1-5)	2	S	--	--	--	F20	S	--	OK	LEC-09T-0D0E1C0F0S-00-S
	4	F	S	--	--	S	--	--	OK	LEC-13A-0D1E0C0F0S-00-S
	5	F	--	--	--	F20	S	--	OK	LEC-10A-0D0E1C0F0S-00-S
ECCS--ALOCA-RV1	1	S	S	--	--	S	--	--	OK	LEC-07T-0D1E0C0F0S-00-S
(Figure 19.1-6)	2	S	--	--	--	F20	S	--	OK	LEC-09T-0D0E1C0F0S-00-S
	4	F	S	--	--	S	--	--	OK	LEC-13A-0D1E0C0F0S-00-S
	5	F	--	--	--	F20	S	--	OK	LEC-10A-0D0E1C0F0S-00-S

Table 19.1-6: System Success Criteria per Event Tree Sequence (Continued)

Event Tree	Seq. No.	RTS	CNV Isolation	DHRS	RSV	ECCS	CVCS	CFDS	End State	Thermal-hydraulic Simulation
MSS---ALOCA-SG (Figure 19.1-7)	1	S	S	S	--	--	--	--	OK	LSI-03T-1D0E0C0F0S-00-S
	2	S	S	F	S	--	--	--	OK	LSI-04T-0D0E0C0F1S-00-S
	3	S	S	F	FO	S	--	--	OK	LCI-03T-0D1E0C0FSS-00-S
	4	S	S	F	FO	F20	S	--	OK	LLI-02T-0D0E1C0FSS-00-S
	7	S	F	--	--	S	S	--	OK	LSU-07T-0D0E1C0F0S-00-S
	8	S	F	--	--	S	F	S	OK	LCU-05T-0D1E0C1F0S-00-S
	10	S	F	--	--	F20	S	--	OK	LSU-07T-0D0E1C0F0S-00-S
	12	F	S	--	S	--	--	--	OK	LSI-02A-0D0E0C0F1S-00-S
	13	F	S	--	FO	S	--	--	OK	LCI-06A-0D1E0C0FSS-00-S
	14	F	S	--	FO	F20	S	--	OK	LEC-10A-0D0E1C0F0S-00-S
	17	F	F	--	--	S	S	--	OK	LLU-04A-0D0E1C0F0S-00-S
TGS---FMSLB-UD (Figure 19.1-8)	1	S	S	S	--	--	--	--	OK	LMI-01T-1D0E0C0F0S-00-S
	2	S	S	S	S	--	--	--	OK	LMI-01T-1D0E0C0F0S-00-S
	3	S	S	S	FO	S	--	--	OK	LCI-03T-0D1E0C0FSS-00-S
	4	S	S	S	FO	F20	S	--	OK	LMU-02T-0D0E1C0FSS-00-S
	6	S	--	F	S	--	--	--	OK	LMU-01T-0D0E0C0F1S-00-S
	7	S	S	F	FO	S	--	--	OK	LCI-03T-0D1E0C0FSS-00-S
	8	S	--	F	FO	F20	S	--	OK	LMU-02T-0D0E1C0FSS-00-S
	11	F	--	--	S	--	--	--	OK	LMU-03A-0D0E0C0F1S-00-S
	12	F	S	--	FO	S	--	--	OK	LCI-06A-0D1E0C0FSS-00-S
	13	F	--	--	FO	F20	S	--	OK	LEC-10A-0D0E1C0F0S-00-S
EHVS-LOOP (Figure 19.1-9)	3	S	S	S	--	--	--	--	OK	TRN-18T-1D0E0C0F0S-00-S
	4	S	S	S	--	S	--	--	OK	LEC-07T-0D1E0C0F0S-00-S
	6	S	S	S	S	--	--	--	OK	TRN-18T-1D0E0C0F0S-00-S
	7	S	S	S	S	S	--	--	OK	LEC-07T-0D1E0C0F0S-00-S
	9	S	S	S	FO	S	--	--	OK	LCI-03T-0D1E0C0FSS-00-S
	11	S	--	F	S	--	--	--	OK	TRN-01T-0D0E0C0F1S-00-S
	12	S	S	F	S	S	--	--	OK	LEC-07T-0D1E0C0F0S-00-S
	14	S	S	F	FO	S	--	--	OK	LEC-07T-0D1E0C0F0S-00-S
	17	F	--	--	S	--	--	--	OK	TRN-14A-0D0E0C0F1S-00-S
	18	F	S	--	S	S	--	--	OK	TRN-20A-2D2E0C0F1S-00-S
	20	F	S	--	FO	S	--	--	OK	LCI-06A-0D1E0C0FSS-00-S

Table 19.1-6: System Success Criteria per Event Tree Sequence (Continued)

Event Tree	Seq. No.	RTS	CNV Isolation	DHRS	RSV	ECCS	CVCS	CFDS	End State	Thermal-hydraulic Simulation
EDSS-LODC (Figure 19.1-10)	1	S	S	S	--	S	--	--	OK	LEC-07T-0D1E0C0F0S-00-S
	2	S	S	S	--	F20	S	--	OK	LCC-01T-0D0E1C0F0S-00-S
	4	S	S	F	S	S	--	--	OK	LEC-07T-0D1E0C0F0S-00-S
	5	S	--	F	S	F20	S	--	OK	LCC-01T-0D0E1C0F0S-00-S
	8	F	S	--	S	S	--	--	OK	TRN-20A-1D2E0C0F1S-01-S
TGS---TRAN-NPC (Figure 19.1-11)	1	S	S	S	--	--	--	--	OK	TRN-18T-1D0E0C0F0S-00-S
	2	S	S	S	S	--	--	--	OK	TRN-01T-0D0E0C0F1S-00-S
	3	S	S	S	FO	S	--	--	OK	LCI-03T-0D1E0C0FSS-00-S
	4	S	S	S	FO	F20	S	--	OK	LLI-02T-0D0E1C0FSS-00-S
	6	S	--	F	S	--	--	--	OK	TRN-01T-0D0E0C0F1S-00-S
	7	S	S	F	FO	S	--	--	OK	LCI-03T-0D1E0C0FSS-00-S
	8	S	S	F	FO	F20	S	--	OK	LLI-02T-0D0E1C0FSS-00-S
	10	S	--	F	FC	--	--	S	OK	TRN-19T-0D0E0C1F0S-00-S
	12	F	S	S	S	--	--	--	OK	TRN-14A-0D0E0C0F1S-00-S
	13	F	S	S	FO	S	--	--	OK	LCI-06A-0D1E0C0FSS-00-S
	14	F	S	S	FO	F20	S	--	OK	LEC-10A-0D0E1C0F0S-00-S
	16	F	S	S	FC	--	S	--	OK	TRN-06A-1D0E1C0F0S-00-D
	18	F	--	F	S	--	--	--	OK	TRN-14A-0D0E0C0F1S-00-S
	19	F	S	F	FO	S	--	--	OK	LCI-06A-0D1E0C0FSS-00-S
	20	F	--	F	FO	F20	S	--	OK	LEC-10A-0D0E1C0F0S-00-S
TGS---TRAN-NSS (Figure 19.1-12)	1	S	S	S	--	--	--	--	OK	TRN-18T-1D0E0C0F0S-00-S
	2	S	S	S	S	--	--	--	OK	TRN-01T-0D0E0C0F1S-00-S
	3	S	S	S	FO	S	--	--	OK	LCI-03T-0D1E0C0FSS-00-S
	5	S	--	F	S	--	--	--	OK	TRN-01T-0D0E0C0F1S-00-S
	6	S	S	F	FO	S	--	--	OK	LCI-03T-0D1E0C0FSS-00-S
	9	F	--	--	S	--	--	--	OK	TRN-14A-0D0E0C0F1S-00-S
	10	F	S	--	FO	S	--	--	OK	LCI-06A-0D1E0C0FSS-00-S

Table 19.1-6: System Success Criteria per Event Tree Sequence (Continued)

Event Tree	Seq. No.	RTS	CNV Isolation	DHRS	RSV	ECCS	CVCS	CFDS	End State	Thermal-hydraulic Simulation

Key for Success Criteria

S: Minimum system performance requirements for success

- RSV, one RSV cycles open and closed, or cycling
- DHRS, one train of DHRS operational
- ECCS, one RRV and one RVV open
- CVCS, one CVCS makeup pump operational
- CFDS, one CFDS pump operational

F: System Failure

FO: one RSV fails open

F20: Two RRVs open and three RVVs fail to open

Key for Thermal Hydraulic Simulation

1st letter: Initiating Event Classification

- T=Transient
- L=LOCA

2nd letter: Initiating Event Type

- C = Charging (injection) line
- L = Letdown (discharge) line
- E = ECCS valve spurious opening
- M = Main steam line break
- S = SGTF
- R = Transient

3rd letter: Isolation Status

- I = Isolated
- U = Unisolated
- C = Inside containment
- N = Transient

4th and 5th letters: Serial number of run

- E.g., 01 is first run

6th letter: Reactor Trip Status

- T = Trip
- A = ATWS

Table 19.1-7: Success Criteria per Top Event

Mitigating System[1]	Top Event	Redundancy	Description
Containment flooding and drain system (CFDS)	CFDS-T01	One of two pumps needed for success. System is shared by six modules.	In sequences with a loss of RCS inventory (e.g., un-isolated LOCA) and success of the RTS, CFDS, in conjunction with ECCS, can provide control of RCS inventory. In transients where DHRS and both RSVs fail and RTS is successful, CFDS can provide fuel assembly heat removal by establishing a convection/conduction heat transfer pathway from the RPV through the CNV to the reactor pool. Operator action to use CFDS to add water to the CNV can prevent core damage in sequences involving: • Pipe breaks outside containment not isolated • SGTF not isolated • General reactor trip Actuation requires an operator action which includes un-isolating containment, aligning a flow path and activating a CFDS pump. It may also require valve realignment because CFDS is a shared system. The CFDS is not credited to mitigate an unisolated break or SGTF if the reactor fails to trip; i.e., given the additional power due to the ATWS, CFDS does not guarantee success.
Chemical and volume control system (CVCS) for RCS injection	CVCS-T01	One of two pumps needed for success. Each module supported by a dedicated system.	The CVCS can provide control of RCS inventory. As a modeling simplification, DWS provides CVCS makeup inventory. Operator action to inject CVCS can prevent core damage in sequences involving: • Failure of ECCS • Pipe breaks outside containment not isolated • SGTF not isolated • Failure of the control rods to insert and both RSVs to open following a general reactor trip (to alleviate RPV pressure through the normal operation of pressurizer spray and CVCS discharge) Operator action requires un-isolating containment, aligning a flow path from the DWS, and activating a makeup pump.

Table 19.1-7: Success Criteria per Top Event (Continued)

Mitigating System[1]	Top Event	Redundancy	Description
Chemical and volume control system (CVCS) for RCS spray injection	CVCS-T04	One of two pumps needed for systems. Each module is supported by a dedicated system.	For injection line LOCAs inside containment, CVCS makeup is available only through the pressurizer spray lines because the CVCS injection pathway is the location of the break. Operator action requires un-isolating containment, aligning a flow path from the DWS, and activating a makeup pump. Given that information may not be available in the MCR to determine the location of the LOCA, operators are expected to inject through the CVCS injection line but switch to the pressurizer spray lines when RPV level does not respond but CNV level increases.
Chemical and volume control system (CVCS) for RCS injection	CVCS-T05	One of two pumps needed for success. Each module supported by a dedicated system.	For loss of DC initiator (with a success of the RTS), a failure of ECCS can be compensated with CVCS makeup water to the RPV. This requires at least at least one EDSS bus. If the initiator is a loss of all four EDSS buses, CVCS is not available because there is no MCR panel indication. If the initiator is a loss of two or three EDSS buses, operators locally open the CVCS injection isolation valves. Local action to unisolate the CIVs is required because DC power from both divisions is not available. The system can be initiated from the control room. The loss of DC power does not prevent operators from starting CVCS makeup pumps because control power for the makeup pumps is supplied from the pump's MCC which is fed from ELVS.
Decay heat removal system (DHRS)	DHRS-T01	One of two trains needed for success. Each module is supported by a dedicated system.	The DHRS is a passive cooling system that removes fuel assembly heat by circulating coolant through the SGs and DHRS condensers which transfers heat to the reactor pool. If DHRS success does not prevent an RSV demand (e.g., due to an ATWS), it is not asked in the event tree. DHRS success requires opening an actuation valve, and closing an FWIV and an MSIV. There are no operator actions associated with DHRS operation.
Decay heat removal system (DHRS)	DHRS-T02	An SGTF is assumed to render one of the two trains unavailable. Therefore one of one trains needed for success. Each module is supported by a dedicated system.	For a steam generator tube failure, DHRS flow in the faulted SG stagnates due to the filling of the steam lines with water and the lack of steaming. Therefore, only one DHRS train is considered (i.e., the train not affected by the SGTF). Similarly, for a secondary line break, only one steam generator is available for heat removal.

Table 19.1-7: Success Criteria per Top Event (Continued)

Mitigating System[1]	Top Event	Redundancy	Description
Emergency core cooling system (ECCS)	ECCS-T01	One of three RVVs and one of two RRVs needed for success. Each module is supported by a dedicated system.	The ECCS provides fuel assembly heat removal and control of RCS inventory. The system passively circulates coolant inventory by removing heat from the reactor core to the CNV which transfers heat to the reactor pool. Success requires one RVV and one RRV to open; failure of both RRVs or all three RVVs to open is an incomplete ECCS actuation. The ECCS is actuated on high CNV water level. The system is also demanded upon a loss of two or more EDSS buses, and 24 hours after a loss of AC power. As discussed in Section 6.3.2.2, the system includes an inadvertent actuation block (IAB) that prohibits the valves from opening until the differential pressure between the RPV and CNV is low; this precludes a valve from opening at power. In some postulated scenarios, it is possible to actuate the IAB when the differential pressure between the RPV and CNV is high. However, as differential pressure lowers, the main spring, assisted by reactor coolant pressure, will open the valve. Therefore, failure of the IAB does not affect successful opening of the ECCS valves. An operator action to actuate ECCS is considered in cases where automatic initiation fails; the action can be completed from the MCR. For initiators that involve a continued loss of coolant from the RPV to outside of containment, this top event is credited only if makeup coolant is successful. For initiators that involve a loss of coolant inside of containment, with success of RTS, ECCS provides passive fuel cooling without the need for inventory makeup or containment isolation.
Reactor coolant system RSV opens	RCS-T01	One of two RSVs needed for success. Each module is supported by a dedicated system.	The RSVs provide RPV pressure relief and RCS integrity. The RSVs are self-actuating pressure relief valves and not operator controlled. Cycling of an RSV transfers RCS to containment and removes fuel assembly heat by convection and conduction to the reactor pool; pressure eventually stabilizes below the RSV setpoint. If both trains of DHRS fail and both RSVs fail to open, the ECCS IAB prohibits the ECCS valves from opening and RPV pressure continues to increase.

Table 19.1-7: Success Criteria per Top Event (Continued)

Mitigating System[1]	Top Event	Redundancy	Description
Reactor coolant system RSV cycling	RCS-T02	One of two RSVs needed for success. Each module is supported by a dedicated system.	The RSVs can serve as a backup to the DHRS and ECCS by providing fuel assembly heat removal. Repeated cycling of an RSV adds inventory to containment and removes fuel assembly heat by convection and conduction from the RPV through the CNV and to the reactor pool. When pressure eventually stabilizes below the RSV setpoint, RSV closure reestablishes RCS integrity. If an RSV fails to re-close, the open path transfers water from the RPV to the CNV. The increase in CNV water level eventually signals an ECCS actuation. The open RSV decreases the pressure differential between the RPV and the CNV enough to nullify the ECCS IAB. Note that if AC power is not restored following a LOOP, ECCS is demanded whether or not an RSV fails to re-close.
	RCS-T03	Not used	
Steam generator tube failure isolation	RCS-T04	Each of the two steam generators in each module can by isolated by either a safety related MSIV and FWIV or by a nonsafety-related isolation valve provided as backup to the MSIV and FWIV. Each module is supported by dedicated main steam and feedwater systems.	Containment isolation on low low pressurizer level closes the MSIVs and the FWIVs, thereby isolating the SGTF.
Reactor coolant system (RCS) RSV demanded	RCS-T05	One of two RSVs needed for success. Each module is supported by a dedicated system.	This event accounts for the possibility that primary pressure increases to the point of reaching the RSV setpoint; this possibility is reflected by assigning a probability to the failure branch that the RSV opens. Only one train of DHRS functioning (in response to a high RPV pressure) may not remove heat quickly enough to prevent an RSV demand.

Table 19.1-7: Success Criteria per Top Event (Continued)

Mitigating System[1]	Top Event	Redundancy	Description
Reactor coolant system RSV cycled	RCS-T06	One of two RSVs needed for success. Each module is supported by a dedicated system.	If the primary pressure increases to the point of reaching the RSV setpoint, this event models closure of the RSV to maintain RCS integrity.
Reactor trip system (RTS)	RTS-T01	RTS has designed-in redundancy. Each module is supported by a dedicated system.	The RTS provides reactivity control. The RTS is part of the MPS. The MPS automatically initiates a reactor trip when a setpoint has been exceeded. Expected automatic trip signals include: • Low pressurizer level or low pressurizer pressure for pipe break outside containment. • Low pressurizer level or low pressurizer pressure for an SGTF. • High containment pressure for LOCA or secondary line break inside containment. • Low steam pressure for secondary line break outside containment. • Loss of AC power. • Loss of two or more EDSS buses. • Low AC voltage. • High steam pressure (closure of Main Steam secondary isolation valves).

Table 19.1-8: Level 1 Internal Probabilistic Risk Assessment Initiating Events

Category	Initiator	Label	Description	Mean Frequency (mcyr^{-1})	Error Factor
Loss-of Coolant Accident and Decrease in Reactor Coolant Inventory Events	CVCS Pipe Break Outside Containment - Charging Line	IE-CVCS--ALOCA-COC	Breaks in the injection flowpath (RCS injection line and pressurizer spray supply line break outside of containment) to the RPV. The distinguishing characteristic of this initiator is that makeup cannot be credited because the break would act as a flow diversion for CVCS makeup.	2.8E-04	10
	CVCS Pipe Break Outside Containment - Letdown Line	IE-CVCS--ALOCA-LOC	Breaks in the RCS discharge line outside of containment; such breaks would not divert flow from CVCS makeup to the RPV.	1.4E-04	10
	CVCS LOCA Inside Containment - Charging Line	IE-CVCS--ALOCA-CIC	Breaks in the RCS injection line inside containment; such breaks cannot be isolated because backflow from the RPV through the break into containment would persist regardless of containment isolation valve closure.	1.4E-04	10
	RCS LOCA Inside Containment	IE-RCS---ALOCA-IC	Breaks in the RCS discharge line, pressurizer spray supply line, and the RPV high point degasification line between their respective RPV penetrations and their CIVs. Breaks in these locations cannot be isolated. Spurious operation of the RSVs and induced LOCAs from pressurizer heaters failing to shut off after a transient are also included in this IE.	2.0E-03	10
	Spurious Opening of an ECCS Valve	IE-ECCS--ALOCA-RV1	Unintended actuation of an ECCS valve (RVV or RRV).	1.1E-05	10
Steam Generator Tube Failure	SGTF	IE-MSS---ALOCA-SG-	Failure of a single steam generator tube.	4.5E-05	10
Secondary Side Line Break	Secondary Side Line Break	IE-TGS---FMSLB-UD-	Breaks in the main steam, feedwater, and decay heat removal piping, as well as spurious operation of the main steam safety valves inside and outside containment.	4.4E-05	10
Loss of Electric Power	Loss of Offsite Power (Loss of Normal AC Power)	IE-EHVS--LOOP---	Loss of AC power to plant transformers. These include plan-centered, switchyard-centered, grid-centered, and weather-related events.	3.1E-02	10
	Loss of DC Power	IE-EDSS--LODC-----	De-energization of at least two highly reliable DC buses.	4.7E-05	10

Table 19.1-8: Level 1 Internal Probabilistic Risk Assessment Initiating Events (Continued)

Category	Initiator	Label	Description	Mean Frequency ($mcyr^{-1}$)	Error Factor
Transients	General reactor trip	IE-TGS---TRAN--NPC	Transients that demand a reactor trip and characterized by availability of modeled support systems (i.e. instrument air and AC power). The initiator includes events such as a loss of component cooling water, loss of feedwater, loss of service water, and loss of condenser heat sink.	1.3	10
	Loss of support systems	IE-TGS---TRAN--NSS	The loss of instrument air or partial loss of AC power support systems resulting in unavailability of the CVCS and the CFDS to provide inventory.	1.6E-02	10

Table 19.1-9: Basic Events with Modified Generic Data

Description	Generic Basis	Generic Mean Value	NuScale Mean Value	Uncertainty	Use
Given actuation, at least 3 of 16 control rods fail to insert	NUREG/CR-6928	1.32E-5 per rod per demand	6.55E-06	Beta distribution	Three rods is the minimum number of stuck rods that results in a failed RTS.
Loss of two or three DC buses	LERs; NUREG-1022	7.88E-4/yr per bus	3.71E-5/mcyr	-	Credit for operator response to use CVCS following a loss of DC power event is dependent on whether the event is a complete loss of DC (all four DC buses) or if the event is a loss of two or three buses. Initiator is CCF of 2 or 3 of 4 EDSS DC buses.
Loss of all four DC buses	LERs; NUREG-1022	7.88E-4/yr per bus	1.02E-5/mcyr	-	Initiator is CCF of 4 of 4 EDSS DC buses
DC bus failure to operate	NUREG/CR-6928	N/A	7.84E-08/hour	R=0.5; gamma distribution	DC bus failure to operate
Restoration of Offsite Power	NUREG/CR-5750	N/A	3.9E-02	Error factor = 3	Offsite power not restored before an ECCS demand (24 hours).
MPS Module Failures: • Equipment interface module (EIM) • Scheduling and bypass module • FM • Scheduling and voting module (SVM)	Microsemi Reliability Report (Reference 19.1-62)	N/A	3.62E-04	Error factor=10; Poisson distribution	Each event failure probability in the MPS is developed based on a reliability estimate for one of the field programmable gate arrays that make up the MPS. Value is the assumed mission time of a latent failure in a standby component over a two-year refueling outage interval.
Hydraulic-operated ECCS main valve fails to open/close	LERs; NUREG/CR-6928	N/A	5.88E-05	*b* = 8.51E+03 Beta distibution	Failure probabilities of the ECCS valves are based on design-specific information and calculated using a fault tree model. The ECCS main valve is approximated as the main part of a boiling water reactor (BWR) safety relief valve.
Solenoid-operated ECCS trip valve fails to open/close	LERs; NUREG/CR-6928	N/A	3.80E-04	*b* = 3.02E+04 Beta distibution	The ECCS trip valve is approximated by a solenoid operated valve.

Table 19.1-10: Basic Events Requiring Design-Specific Analysis

Description	Mean	Uncertainty	Use
CVCS LOCA does not initiate excess flow check valve	1E-01	EF = 10; lognormal	For sequences when there is a potential that the flow rate of a LOCA, resulting from a leak or small break, does not engage the CVCS excess flow check valve to isolate, this failure probability of the valve to close is assumed based on engineering judgment.
ECCS reactor vent valve passive opening at low differential pressure	1E-01	EF = 10; lognormal	When the dp across the valve gets low for a sufficient amount of time, the spring force becomes the dominant term in the force balance and pulls the main valve open. This characteristic of passive opening is considered when a valve fails to open on demand; the failure probability to open passively is assumed based on engineering judgment.
ECCS reactor recirculation valve passive opening at low differential pressure	1E-01	EF = 10; lognormal	When the dp across the valve gets low for a sufficient amount of time, the spring force becomes the dominant term in the force balance and pulls the main valve open. This characteristic of passive opening is considered when a valve fails to open on demand; the failure probability to open passively is assumed based on engineering judgment.
Probability that the RSV is demanded to open	5E-01	N/A	In sequences when there is a small pressure margin for an RSV demand, the probability that an RSV is demanded to open is considered; this probability is based on engineering judgment.
DHRS train passive heat transfer to reactor pool	4E-06	EF = 2; lognormal	Following successful actuation of a DHRS train, this event represents a failure of passive heat transfer (i.e., natural circulation) to the UHS over the mission time.
ECCS passive heat transfer to reactor pool	1E-07	EF = 3; lognormal	Following successful actuation of ECCS, this event represents a failure of passive heat transfer (i.e., natural circulation) to the UHS over the mission time.
MPS test or maintenance unavailability for: • Scheduling and bypass module • SFM • Scheduling and voting module SVM)	 2.7E-03 2.7E-03 2.1E-03	 EF = 10; lognormal EF = 10; lognormal EF = 10; lognormal	Twelve hours of maintenance between refueling outages (i.e., 2 years) is assumed to result in unavailability of each MPS channel. When an MPS channel is in maintenance, it is placed into trip or bypass.
Temperature induced SGTF	2.5E-02	EF = 2; lognormal	The conditional probability that a helical coil steam generator tube (in compression) fails following core damage.

Table 19.1-11: Phenomena Affecting Emergency Core Cooling System Passive Performance

Parameter	Significance*
Decay power	Decay heat level defines the required capacity of the ECCS. Higher energy production after shutdown increases the long-term ECCS heat removal requirements.
CNV convective heat transfer	Increased wall-fluid heat transfer decreases pressure in the CNV, reducing the RPV level.
RPV initial level	A lower initial RPV level reduces the available hydrostatic head for recirculation.
Non-condensable gas	A lower non-condensable gas inventory increases the condensation rate of steam and decreases pressure in the CNV, which has the net effect of reducing the RPV level.
ECCS valve flow	An increased pressure drop across the ECCS valves (decreased flow capacity) maintains the RPV at higher pressure, reducing the RPV level.
Pool temperature	A lower pool pool temperature increases heat transfer through the CNV and decreases pressure in the CNV, reducing the RPV level.

*Note: Parameter significance is provided with respect to the passive reliability of the ECCS to facilitate liquid coolant recirculation to the RPV.

Table 19.1-12: Phenomena Affecting Decay Heat Removal System Passive Performance

Parameter	Significance*
Decay power	Decay heat level defines the required capacity of the DHRS. Higher energy production after shutdown increases the long-term DHRS heat removal requirements.
DHRS fluid inventory	A higher inventory level decreases the efficiency of the DHRS by reducing the condensation surface area and can further exacerbate the effect of non-condensables.
DHRS condenser convective heat transfer	Decreased wall-fluid heat transfer decreases heat removal in the DHRS, increasing RPV pressure.
Steam generator convective heat transfer	Decreased wall-fluid heat transfer decreases heat transfer to the steam generator, increasing RPV pressure.
Steam generator plugging	Increased plugging decreases the heat transfer capacity of the steam generator, increasing RPV pressure.
Non-condensable gas in DHRS	A higher non-condensable gas inventory in the DHRS condenser tubes decreases the condensation rate of steam, thereby decreasing heat transfer to the UHS and increasing RPV pressure.

*Note: Parameter significance is provided with respect to the passive reliability of the DHRS to remove sufficient decay heat to prevent RPV overpressurization.

Table 19.1-13: Modeled Human Actions (Pre-Initiator)

Name	Description	HEP	Error Factor
CFDS--HFE-0001A-UTM-N	Operator misaligns MDP 0004A CFDS Train A manual valves during test and maintenance	9.7E-04	5
CFDS--HFE-0002A-UTM-N	Operator misaligns MDP 0004B CFDS Train B manual valves during test and maintenance	9.7E-04	5
CVCS--HFE-0001A-UTM-N	Operator misaligns MDP 0098A CVCS Train A manual valves during test and maintenance	9.7E-04	5
CVCS--HFE-0002A-UTM-N	Operator misaligns MDP 0098B CVCS Train B manual valves during test and maintenance	9.7E-04	5
EHVS--HFE-0001A-UTM-N	Operator misaligns CTG 0003X EHVS CTG during test and maintenance	8.0E-04	10
ELVS--HFE-0001A-UTM-N	Operator misaligns DGN 0001X ELVS standby diesel generator during test and maintenance	8.0E-04	10
ELVS--HFE-0002A-UTM-N	Operator misaligns DGN 0002X ELVS standby diesel generator during test and maintenance	8.0E-04	10
MPS---HFE-0001A-UTM-S	Operator miscalibrates safety function modules during test and maintenance	1.7E-03	4

Table 19.1-14: Modeled Human Actions (Post-Initiator)

Name	Description	Applicable Initiating Event	HEP [1, 2, 3, 4] (Diagnosis + Action)
CFDS--HFE-0001C-FOP-N[5]	Operator fails to unisolate and initiate CFDS injection. This action is completed in the control room.	Used for CVCS line breaks outside containment, SGTFs, and general transients • IE-CVCS--ALOCA-COC • IE-CVCS--ALOCA-LOC • IE-MSS---ALOCA-SG- • IE-TGS---TRAN--NPC	4.0E-03
CNTS--HFE-0001C-FTC-N	Operator fails to manually actuate CIVs following the failure of the MPS to automatically isolate. This action is completed in the control room.	Backup action to MPS autofunction failure. Applicable to core damage sequences with an intact containment. This is a Level 2 operator action.	2.2E-04
CVCS--HFE-0001C-FOP-N [5, 6]	Operator fails to unisolate and initiate CVCS injection through either the injection line or the pressurizer spray line. This action is completed in the control room.	Used for CVCS injection line LOCA inside containment, CVCS discharge line break outside containment, inadvertent ECCS valve opening, SGTF, RCS line LOCA, secondary side line break, and general transients: • IE-CVCS--ALOCA-CIC • IE-CVCS--ALOCA-LOC • IE-ECCS--ALOCA-RV1 • IE-MSS---ALOCA-SG- • IE-RCS---ALOCA-IC- • IE-TGS---FMSLB-UD- • IE-TGS---TRAN-NPC	4.0E-03
CVCS--HFE-0002C-FOP-N [6]	Operator fails to locally unisolate and initiate CVCS injection through either the injection line or the pressurizer spray line. This action is completed locally.	Local action due to lack of control due to a partial loss of DC power: • IE-EDSS--LODC-----	1.4E-03
ECCS--HFE-0001C-FTO-N	Operator fails to manually open the ECCS valves following the failure of the MPS to automatically actuate. This action is completed in the control room.	Backup action to MPS autofunction failure: Applicable to all initiating events.	2.2E-04
EHVS--HFE-0001C-FTS-N	Operator fails to start and load the CTG following the deenergization of the eight 13.8 kV and switchyard system (EHVS) buses. This action is completed in the control room or locally at the CTG and the local breakers.	Backup local action to control room initiation failure during LOOP: • IE-EHVS--LOOP-----	1.4E-03

Table 19.1-14: Modeled Human Actions (Post-Initiator) (Continued)

Name	Description	Applicable Initiating Event	HEP [1, 2, 3, 4] (Diagnosis + Action)
ELVS--HFE-0001C-FTS-N	Operator fails to start and load the BDGs following the deenergization of the eight 13.8 kV EHVS buses. This action can be completed in the control room or locally at the BDGs and local breakers.	Backup local action to control room initiation failure during LOOP: • IE-EHVS--LOOP-----	1.4E-03

1.) HEP = 4.0E-03
For diagnosis, operators have at least 30 minutes (based on thermal hydraulic analyses), and the time available to perform the action is nominal (i.e., greater than the time required to perform the action).

2.) HEP = 2.2E-04
For diagnosis, operators have at least 30 minutes (based on thermal hydraulic analyses), and the time available is significantly greater than the time required to perform the action.

3.) HEP = 1.4E-03
For diagnosis, operators have an hour or more (based on thermal hydraulic analyses), and the time available is significantly greater than the time required to perform the action, however complexity is greater as the action is local.

4.) Even though individual calculations were performed for each post-initiator operator action, as a modeling convenience, a generic HFE basic event quantification approach has been incorporated in the PRA model by setting the first HFE in a sequence to the bounding calculated post-initiator HEP.

5.) The containment system isolation override allows operators to take manual control to support injection.

6.) The PRA models the DWS to support CVCS injection; the BAS provides an immediate source of inventory and allows time (i.e., hours) for operators to locally align the DWS supply isolation valves, if additional inventory is needed.

Table 19.1-15: Generic Sources of Level 1 Model Uncertainty

Uncertainty Source	Description (Reference 19.1-7)	Level 1 Assumption	Effect on Model
		Initiating Event Analysis	
Grid stability	The LOOP frequency is a function of several factors including switchyard design, the number and independence of offsite power feeds, the local power production and consumption environment and the degree of plant control of the local grid and grid maintenance. Three different aspects relate to this issue: • LOOP initiating event frequency values and recovery probabilities • Conditional LOOP probability • Availability of DC power to perform restoration actions	The generic data is applicable to NuScale. The estimation of LOOP frequency accounts for plant-centered, switchyard-centered, gird-related and weather-related LOOP events.	Although this is not expected to be a source of model uncertainty because it is based on generic industry data for LOOP events, Sensitivity Study 3a (provided in Table 19.1-22 and Table 19.1-31) was performed to account for the design-specific diverse Non-1E power system.
Support system initiating events	Increasing use of plant-specific models for support system initiators (e.g., loss of plant air, loss of AC or DC buses) have led to inconsistencies in approaches across the industry. A number of challenges exist in modeling of support system initiating events: • Treatment of CCFs • Potential for recovery	Support system initiating event frequencies are based on generic data, without credit for recovery.	Because support system initiating events are modeled, based on a review of all plant systems, this is judged not to be a significant source of model uncertainty.
LOCA initiating event frequencies	It is difficult to establish values for events that have not occurred or have rarely occurred with a high level of confidence. The choice of available data sets or use of specific methodologies in the determination of LOCA frequencies could impact base model results and some applications.	LOCA frequencies are calculated for applicable systems based on pipe length. The potential LOCA piping is also similar in size to generic data. The typical LOCA size distinction (i.e. large, medium, and small) is not required because makeup capability is sufficient for all break sizes.	Because the LOCA initiating event frequencies are based on design-specific piping design and consideration of likely potential degradation mechanisms, this is judged not to be a source of significant model uncertainty.
		Accident Sequence Analysis	
Operation of equipment after battery depletion	Station Blackout events are important contributors to baseline CDF at nearly every U.S. nuclear plant. In many cases, battery depletion may be assumed to lead to loss of all system capability. Some PRAs have credited manual operation of systems that normally require DC for successful operation (e.g., turbine-driven systems such as the reactor core isolation cooling system and auxiliary feedwater).	Safety-related system valves go to their fail-safe position on a loss of DC power. A loss of all DC power also results in a loss of indication and control. Following a loss of AC power, the DC batteries are assumed to deplete in 24 hours.	Event trees explicitly consider module response following a loss of AC and DC power, thus, this is judged not to be a source of significant model uncertainty.
Reactor coolant pump seal LOCA treatment	The assumed timing and magnitude of a reactor coolant pump seal LOCAs given a loss of seal cooling can have a substantial influence on the risk profile.	The design does not include reactor coolant pumps.	Not applicable

Table 19.1-15: Generic Sources of Level 1 Model Uncertainty (Continued)

Uncertainty Source	Description (Reference 19.1-7)	Level 1 Assumption	Effect on Model
Recirculation pump seal leakage treatment - Isolation Condensers	Recirculation pump seal leakage can lead to loss of the Isolation Condenser. While recirculation pump seal leakage is generally modeled, there is no consensus approach on the likelihood of such leaks.	The design does not include recirculation pumps with seals.	Not applicable
Success Criteria			
Impact of containment venting on core cooling system net-positive suction head	Many BWR core cooling systems utilize the suppression pool as a water source. Venting of containment as a decay heat removal mechanism can substantially reduce net-positive suction head, even lead to flashing of the pool. The treatment of such scenarios varies across BWR PRAs.	There is not a credible CNV overpressure scenario that would benefit from containment venting. Based on the design, in which the CNV is immersed in the reactor pool, and RPV in-vessel retention is ensured in cases with containment isolation, CNV pressure suppression is ensured.	Because the ECCS is a passive safety system that does not rely on pumps, and failures of containment isolation do not impact ECCS, this is judged not to be a source of significant model uncertainty.
Core cooling success following containment failure or venting through non hard pipe vent paths	Loss of containment heat removal leading to long-term containment over-pressurization and failure can be a significant contributor in some PRAs. Consideration of the containment failure mode might result in additional mechanical failures of credited systems. Containment venting through "soft" ducts or containment failure can result in loss of core cooling due to environmental impacts on equipment in the reactor/auxiliary building, loss of net positive suction head on ECCS pumps, steam binding of ECCS pumps, or damage to injection piping or valves. There is no definitive reference on the proper treatment of these issues.	The CNV is immersed in the reactor pool, which contains sufficient water inventory to cool the modules for an extended period under adverse conditions	Because the CNV is not susceptible to long-term containment over-pressurization and failure, this is judged not to be a source of significant model uncertainty.
Room heatup calculations	Loss of heating ventilation and air conditioning (HVAC) can result in room temperatures exceeding equipment qualification limits. Treatment of HVAC requirements varies across the industry and often varies within a PRA. There are two aspects to this issue. One involves whether the SSC affected by loss of HVAC are assumed to fail (i.e., there is uncertainty in the fragility of the components). The other involves how the rate of room heatup is calculated and the assumed timing of the failure.	The RXB ventilation system is not needed or credited to maintain a controlled environment for safety-related equipment. Once safety-systems are actuated, they do not need to change state.	System models do not include ventilation support dependencies. However, nonsafety-related mitigating systems do require operator action, such that opening doors or other measures could be performed, if needed, to prevent operating equipment temperatures beyond qualification limits. Sensitivity Study 1 addresses HEP uncertainty. Sensitivity Study 7 (provided in Table 19.1-22 and Table 19.1-31) addresses the effect of not crediting nonsafety-related systems.

Table 19.1-15: Generic Sources of Level 1 Model Uncertainty (Continued)

Uncertainty Source	Description (Reference 19.1-7)	Level 1 Assumption	Effect on Model
Battery life calculations	Station Blackout events are important contributors to baseline CDF at nearly every US NPP. Battery life is an important factor in assessing a plant's ability to cope with a station blackout. Many plants only have design basis calculations for battery life. Other plants have very plant/condition specific calculations of battery life. Failing to fully credit battery capability can overstate risks, and mask other potential contributors and insights. Realistically assessing battery life can be complex.	Although the design includes redundant batteries, it is uncertain how long DC power would be available if more than one battery is utilized for a bus. For this reason, the limiting assumption of a 24-hour battery life is used.	This is judged not to be a source of significant model uncertainty because the LOOP event tree considers DC battery depletion and subsequent system response (i.e., ECCS actuation).
Number of PORVs required for bleed and feed-PWRs	PWR EOPs direct opening of all PORVs to reduce RCS pressure for initiation of bleed and feed cooling. Some plants have performed plant-specific analysis that demonstrate that less than all PORVs may be sufficient, depending on ECCS characteristics and initiation timing.	The design does not include PORVs or feed and bleed cooling.	Not applicable
Containment sump/strainer performance	All PWRs are improving ECCS sump management practices, including installation of new sump strainers at most plants.	The design does not contain insulation or other typical sources of debris, strainers are not needed.	This is judged not to be a source of significant model uncertainty because there is limited potential for debris in the CNV, and the process of CNV draining after refueling provides assurance that there is no debris in the CNV.
Impact of failure of pressure relief	Certain scenarios can lead to RCS/RPV pressure transients requiring pressure relief. Usually, there is sufficient capacity to accommodate the pressure transient. However, in some scenarios, failure of adequate pressure relief can be a consideration. Various assumptions can be taken on the impact of inadequate pressure relief.	In sequences where the thermal-hydraulic simulations predict the ultimate failure pressure is reached, RPV failure and core damage are assumed.	This is judged not to be a source of significant model uncertainty because the PRA models RPV failure and core damage in sequences with inadequate pressure relief.
Systems Analysis			
Operability of equipment in beyond design basis environments	Due to the scope of PRAs, scenarios may arise where equipment is exposed to beyond design basis environments (without room cooling, without component cooling, deadheading, in the presence of an unisolated LOCA, etc.).	Safety-related equipment is designed to operate without electric power and ventilation. Once safety-systems are actuated, they do not need to change state.	Although ventilation is not modeled for nonsafety SSC, the RTNSS Sensitivity Study 7 (provided in Table 19.1-22 and Table 19.1-31) captures this source of model uncertainty.

Table 19.1-15: Generic Sources of Level 1 Model Uncertainty (Continued)

Uncertainty Source	Description (Reference 19.1-7)	Level 1 Assumption	Effect on Model
Human Reliability Analysis			
Credit for Emergency Response Organization	Most PRAs do not give much, if any credit, for initiation of Emergency Response Organization, including actions included in plant specific severe accident mitigation guidelines and the new B5b mitigation strategies. The additional resources and capabilities brought to bear by the Emergency Response Organization can be substantial, especially for long term events.	No credit is given for the Emergency Response Organization, including severe accident mitigation guidelines, or FLEX equipment and mitigation strategies.	Not crediting the Emergency Response Organization, severe accident mitigation guidelines, or FLEX in the PRA is not expected to be a source of model uncertainty.

Table 19.1-16: Design-Specific Sources of Level 1 Model Uncertainty

Uncertainty Source	Description	Level 1 Assumption	Effect on Model
General			
Design state	Design changes are likely as the design evolves beyond design certification.	The PRA model reflects the current state of design for the design certification.	The PRA model is updated to remain consistent with the maturing design. As such, this is judged not to be a significant source of model uncertainty.
Initiating Event Analysis			
List of initiating events	Comprehensive list of internal initiating events, including potential initiators from other modules.	The PRA model captures potential initiating events; based on a thorough review of potential initiating events. There is not a size of LOCA that exceeds the capability of the ECCS (e.g., reactor vessel rupture). Address other module initiators.	The PRA model includes a wide range of initiating events to capture potential accident progression scenarios; the initiators cover LOCAs, SGTFs, secondary line breaks, loss of electric power, and transients. As such, this is judged not to be a significant source of model uncertainty.
Operating experience and data	Frequencies for initiating events with no plant experience.	Generic data and plant-specific analyses are representative of the initiating event frequencies.	It is judged that initiating event frequencies are not higher than generic data; the design reflects opportunities to improve SSC based on operating experience. Although generic data is used, a lognormal distribution with an error factor of 10 is used to bound the uncertainty. Sensitivity Studies 3a, 3b, 3c and 3d (provided in Table 19.1-22 and Table 19.1-31) were performed to address Initiating event frequency uncertainty.
Availability and capacity factor	Initiating event frequency adjustment for capacity factor.	Plant availability is assumed to be 100 percent.	The initiating event frequencies are conservative; i.e., they are not weighted by the fraction of time the plant is at power.
SGTF	Frequency for an SGTF in a helical steam generator with no plant experience.	A study was performed to estimate the frequency of an SGTF based on a probabilistic physics of failure approach.	Sensitivity Study 3b (provided in Table 19.1-22 and Table 19.1-31) illustrates that an increase in the frequency of an SGTF has a very small impact on the results. As such, this is judged not to be a significant source of model uncertainty.
Secondary line breaks	Frequency for a secondary line break with no plant experience.	A study was performed to analyze system design to estimate the frequency of a secondary line break.	Sensitivity Study 3c (provided in Table 19.1-22 and Table 19.1-31) illustrates that an increase in the frequency of a secondary line break has a very small impact on the results. As such, this is judged not to be a significant source of model uncertainty

Table 19.1-16: Design-Specific Sources of Level 1 Model Uncertainty (Continued)

Uncertainty Source	Description	Level 1 Assumption	Effect on Model
Accident Sequence Analysis and Success Criteria			
ECCS Inadvertent Actuation Block (IAB)	Thermal-hydraulic modeling of the ECCS IAB setpoints.	The thermal-hydraulic simulations are best estimate; if ECCS actuation is demanded while the RPV/CNV differential pressure is high, the IAB prevents primary system blowdown (i.e., ECCS actuation) until the lower differential pressure setpoint is reached. Actuation is permitted if first demanded when the RPV/CNV differential pressure is below the high differential pressure setpoint.	This is only a consideration in sequences where there is an unisolated pipe break outside containment; the differential pressure is low following a LOCA inside containment and following DHRS actuation or an RSV demand after a transient, loss of power, or isolated pipe breaks or an SGTF. In sequences where there is an unisolated loss of coolant (including an SGTF), the event tree includes makeup following success of ECCS, which requires operator action. As such, the uncertainty of a potential delay in actuating ECCS is effectively captured in the HEP sensitivity studies (Sensitivity Studies 1a, 1b). Similarly, Sensitivity Study 2 for CCF and Sensitivity Study 5 (provided in Table 19.1-22 and Table 19.1-31) address uncertainty in ECCS actuation.
Passive decay heat removal	Reliability and effectiveness of passive decay heat removal systems with no plant experience.	Experimental testing data and design-specific analysis reflect system success criteria and reliability, including availability of the UHS.	Sensitivity Study 4 (provided in Table 19.1-22 and Table 19.1-31) illustrates that there is little effect on CDF with order of magnitude increase in passive heat removal failure probability.
ECCS low differential pressure opening mode	Reliability of the ECCS low differential pressure operating mode with no plant experience.	The probability of the ECCS low differential pressure opening mode is assumed to be 0.1.	Sensitivity Study 5 (provided in Table 19.1-22 and Table 19.1-31) evaluated the effect of increasing the failure probability as small. In addition, Sensitivity Study 2 addressed uncertainty in ECCS actuation due to CCF.
ATWS and definition of core damage	Power oscillations during ATWS sequences.	Only sequences that exceed peak clad temperature are assumed to result in core damage.	Successful end states in the PRA do not require the core to remain subcritical. Because this is not a safety issue as heat removal is effective, it is not expected to be a source of model uncertainty.
Data Analysis			
Mission time	Use of a 72 hour mission time for a passive design. Standard industry PRA practice uses a 24 hour mission time.	Time-dependent component failures generally modeled using a 72 hour mission time.	Use of a 72-hour mission time is consistent with the guidance for passive reactor designs. This may result in conservative equipment reliability estimates.
Testing scheme	Plant testing scheme.	Standby failure rates assume non-staggered testing.	This is conservative assumption; results are slightly conservative in comparison to a staggered testing assumption.
Test and Maintenance Unavailability	Identification and modeling of test and maintenance unavailability events with no plant experience.	Test and maintenance unavailabilities were identified from draft technical specifications, discussions with operations and design engineers, and other PRA models. Unavailabilities are based on generic data.	The PRA model includes several system test and maintenance unavailabilities; although generic data is used, a lognormal distribution with an error factor of 10 is used to bound the uncertainty.

Table 19.1-16: Design-Specific Sources of Level 1 Model Uncertainty (Continued)

Uncertainty Source	Description	Level 1 Assumption	Effect on Model
Component failure data	Reliability data with no plant experience.	Generic data is assumed to better represent reliability of components.	Potential for over or under estimating component reliability; this is captured in the parametric uncertainty results and not expected to be a measurable source of model uncertainty. Because some of the sensors being used to monitor plant parameters may utilize new technologies (e.g., digital components), Sensitivity Study 6 (provided in Table 19.1-22 and Table 19.1-31) was performed to address this uncertainty.
Common Cause Events	Only intra-system CCF events considered.	Common cause events are considered for intra-system components, based on common coupling mechanisms. Generic NRC data are used for common cause alpha factor parameters.	The only potential for inter-system CCFs (i.e., between different systems that perform a similar function) is between CVCS and CFDS (e.g., pumps). Because operation of these systems requires operator action, the uncertainty of any potential inter-system CCF is effectively captured in Sensitivity Study 1 (provided in Table 19.1-22 and Table 19.1-31) which addresses HEP.
Human Reliability Analysis			
Operator actions	The identification of credible operator actions (including availability, procedures, and time to perform actions), as well as the dependencies between actions and control room habitability.	The actions modeled in the PRA is reflected in procedures; they are based on discussions with operations personnel and system engineers. There is sufficient staff, time, direction, and conditions to perform the actions.	The uncertainty in the operator actions modeled in the PRA is captured in Sensitivity Study 1 (provided in Table 19.1-22 and Table 19.1-31) which addresses HEP.
Latent actions	The potential for over counting latent human actions.	Latent HFEs are not assumed to be captured in generic component reliability data, and are explicitly modeled in the PRA.	Results are slightly conservative if latent human actions are also counted in generic reliability data.
Commission errors	The potential for commission errors based on a new design with no design-basis operator actions.	A review of potential commission errors was performed, but no impactful errors of commission were identified.	Consideration was given to the potential of defeating ECCS by unisolating the CNV, however, the vapor loss associated with opening the CES would not impact ECCS, and opening the CFDS would require a subsequent break downstream of several isolation valves to have an impact on ECCS. Therefore, this is judged not to be a significant source of model uncertainty.
Systems Analysis			
PCS unavailability	Availability of PCS following an initiating event with no plant experience.	In the current design, PCS is not expected to be available following an initiating; the PRA does not model PCS as a mitigating system.	This is best estimate; there may be a slight conservatism in the results by not crediting PCS.

Table 19.1-16: Design-Specific Sources of Level 1 Model Uncertainty (Continued)

Uncertainty Source	Description	Level 1 Assumption	Effect on Model
Island mode	The potential for supplying plant loads AC power from another module instead of from offsite power.	Island mode is not credited in the PRA.	Sensitivity Study 3a (provided in Table 19.1-22 and Table 19.1-31) evaluates the effect of LOOP frequency.
Digital instrumentation and controls (I&C) Misbehavior	Defensive measures that are a part of digital I&C systems ensure the dependability of these systems but potentially can have negative effects if they misbehave. (e.g., contribute to the prevention of mitigating system operation or cause inadvertent operation when not needed)	I&C is modeled down to the digital module level which is the level at which generic data are available and consistent with the PRA Standard. I&C related behaviors at the module, system or functional level that could have an adverse impact on mitigating system operation or have negative effects on plant response have been identified and are modeled explicitly in the PRA.	The context of the digital I&C within the systems that it actuates and controls, and the role that they play in the overall integrated plant design dictates the level of detail to which the I&C should be modeled. This level of detail is achieved by modeling at the digital module level and is more than adequate to address both the prevention of mitigating system functions as well as unneeded spurious operation. This modeling detail is reflected in selection of IEs, development of accident sequence structure and fault tree logic.

Table 19.1-17: Significant Core Damage Sequences (Full Power, Internal Events, Single Module)

Event Tree Initiator	Sequence	Contribution (% CDF)	Sequence Description
RCS LOCA inside containment (RCS---ALOCA-IC)	Figure 19.1-5 Sequence 3	22.3	An RCS LOCA inside containment initiating event followed by failure of ECCS and failure to make up RCS inventory from the CVCS.
Loss of DC power (EDSS-LODC)	Figure 19.1-10 Sequence 3	15.7	A loss of DC power initiating event followed by an incomplete ECCS actuation and failure to make up RCS inventory from the CVCS.
Loss of offsite power (EHVS-LOOP)	Figure 19.1-9 Sequence 5	10.4	A LOOP initiating event followed by a failure of the CTG and BDGs, failure to restore power before the timers time out, and an incomplete ECCS actuation.
Loss of offsite power (EHVS-LOOP)	Figure 19.1-9 Sequence 8	10.4	A LOOP initiating event with an RSV demand, followed by a failure of the CTG and BDGs, failure to restore power before the timers time out, and an incomplete ECCS actuation.
Loss of support system (TGS---TRAN---NSS)	Figure 19.1-12 Sequence 4	8.8	Loss of support system initiating event followed by an RSV demand but failure to reclose, and failure of ECCS.
CVCS charging line pipe break outside containment (CVCS--ALOCA-COC)	Figure 19.1-2 Sequence 7	6.0	A CVCS injection line pipe break outside containment initiating event followed by a failure to isolate the break and a failure to make up inventory from the CFDS.
General reactor trip (TGS-TRAN-NPC)	Figure 19.1-11 Sequence 5	5.3	Transient initiating event followed by an RSV demand but failure to reclose, a failure of ECCS, and failure to make up RCS inventory from the CVCS.
Loss of support system (TGS---TRAN---NSS)	Figure 19.1-12 Sequence 8	4.9	Loss of support system initiating event followed by a failure to remove heat through the DHRS or the RSVs.
Loss of support system (TGS---TRAN---NSS)	Figure 19.1-12 Sequence 12	4.3	Loss of support system initiating event followed by a failure of the reactor to trip (ATWS) and failure of the DHRS and both RSVs to provide fuel assembly heat removal and pressure relief.
General reactor trip (TGS-TRAN-NPC)	Figure 19.1-11 Sequence 11	3.9	Transient initiating event followed by failures of the DHRS, RSVs, and CFDS.
Other sequences	All	8.0	

Table 19.1-18: Significant Core Damage Cutsets (Full Power, Internal Events, Single Module)

Cutset	Prob/Freq	Contribution	Basic Event	Description
1	2.56E-11	9.4%		
	4.70E-5		IE-EDSS--LODC-----	Loss of DC Power
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	2.16E-1		EDSS--EBD-1CC44-FOP-N	INITIATOR IS CCF OF 4 OF 4 EDSS DC BUSSES TO OPERATE
2	2.02E-11	7.4%		
	2.00E-3		IE-RCS---ALOCA-IC-	LOCA Inside Containment
	1.00E+0		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
3	1.48E-11	5.4%		
	1.60E-2		IE-TGS---TRAN--NSS	Loss of Support System
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	7.32E-4		RCS---RSV-0003A-FTC-S	RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
4	1.26E-11	4.6%		
	4.70E-5		IE-EDSS--LODC-----	Loss of DC Power
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	2.16E-1		EDSS--EBD-1CC44-FOP-N	INITIATOR IS CCF OF 4 OF 4 EDSS DC BUSSES TO OPERATE
5	1.03E-11	3.8%		
	1.60E-2		IE-TGS---TRAN--NSS	Loss of Support System
	1.38E-5		DHRS--HOV-1CC44-FTO-S	CCF OF 4 OF 4 DHRS ACTUATION VALVES FAIL TO OPEN
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
6	9.94E-12	3.7%		
	2.00E-3		IE-RCS---ALOCA-IC-	LOCA Inside Containment
	1.00E+0		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
7	7.28E-12	2.7%		
	1.60E-2		IE-TGS---TRAN--NSS	Loss of Support System
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	7.32E-4		RCS---RSV-0003A-FTC-S	RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
8	5.76E-12	2.1%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	1.00E+0		CFDS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CFDS INJECTION

Table 19.1-18: Significant Core Damage Cutsets (Full Power, Internal Events, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
9	4.90E-12	1.8%		
	1.60E-2		IE-TGS---TRAN--NSS	Loss of Support System
	6.55E-6		CRDS--ROD-1CC316FOP-S	GIVEN ACTUATION, AT LEAST 3 OF 16 RODS FAIL TO INSERT
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
10	4.83E-12	1.8%		
	1.31E+0		IE-TGS---TRAN--NPC	General Reactor Trip
	1.00E+0		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	7.32E-4		RCS---RSV-0003A-FTC-S	RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
11	4.79E-12	1.8%		
	2.00E-3		IE-RCS---ALOCA-IC-	LOCA Inside Containment
	9.51E-4		CVCS--AOV-0091X-FTO-N	AOV 0091X CVCS MAKEUP COMBINING VALVE FAILS TO OPEN
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
12	4.79E-12	1.8%		
	2.00E-3		IE-RCS---ALOCA-IC-	LOCA Inside Containment
	9.51E-4		DWS-00AOV-0033X-FTO-N	AOV 0033X DWS NORTH REACTOR BUILDING CVCS PUMP ISOLATION VALVE FAILS TO OPEN
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
13	3.38E-12	1.2%		
	1.31E+0		IE-TGS---TRAN--NPC	General Reactor Trip
	1.00E+0		CFDS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CFDS INJECTION
	1.38E-5		DHRS--HOV-1CC44-FTO-S	CCF OF 4 OF 4 DHRS ACTUATION VALVES FAIL TO OPEN
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN

Table 19.1-19: Criteria for Risk Significance

Parameter	Criteria for Risk Significance
Component	Conditional CDF $\geq$ 3 x 10^{-6}/yr
System	Conditional CDF $\geq$ 1 x 10^{-5}/yr
Component	Conditional LRF $\geq$ 3 x 10^{-7}/yr
System	Conditional LRF $\geq$ 1 x 10^{-6}/yr
Component	Total FV $\geq$ 0.20

Table 19.1-20: Listing of Candidate Risk Significant Structures, Systems, and Components (Full Power, Single Module) Level 1 Probabilistic Risk Assessment

System	Description	CCDF	FVCDF
ECCS	Emergency core cooling system	Met	
MPS	Module protection system	Met	
UHS	Ultimate heat sink	Met	
Component	**Basic Event Description**	**CCDF**	**FVCDF**
ECCS-HOV-0001A	HOV 0001A ECCS reactor vent valve	Not Met	Met[1]
ECCS-HOV-0001B	HOV 0001B ECCS reactor vent valve	Not Met	Met[1]
ECCS-HOV-0001C	HOV 0001C ECCS reactor vent valve	Not Met	Met[1]
ECCS-HOV-0002A	HOV 0002A ECCS reactor recirculation valve	Not Met	Met[1]
ECCS-HOV-0002B	HOV 0002B ECCS reactor recirculation valve	Not Met	Met[1]
EHVS-CTG-0003X	CTG 0003X combustion turbine generator	Not Met	Met
RCS-RSV-0003A	RCS reactor safety valve 0003A	Not Met	Met[1]
Initiator	**Description**	**CCDF**	**FVCDF**
IE-RCS---ALOCA-IC-	LOCA inside containment		Met
IE-EHVS--LOOP-----	Loss of offsite power		Met

Notes**:**

- Spaces that are grayed out' indicate categories in which the criteria do not apply, as described in TR-0515-13952-A.
- As stated in the DCA text, no human actions are risk significant.

[1] The criterion is Met with CCFs conservatively included in the calculation of the single component FV.

Table 19.1-21: Key Assumptions for the Level 1 Full Power Internal Events Probabilistic Risk Assessment

Assumption	Basis
Initiating Events	
Initiating event frequencies, based on generic data, are applicable to the NuScale design. The probability of recovering offsite power, based on generic data, is also applicable to the NuScale design.	Common engineering practice
Initiating event frequencies, based on design-specific analyses, are representative and appropriate. Examples include SGTF and spurious opening of an ECCS valve.	Common engineering practice and engineering judgment
Initiating event frequencies, based on data from NUREG/CR-5750, are lognormal with an error factor of 10.	Common engineering practice
Initiating event frequencies are based on full power operation for a year (i.e., availability is 100 percent).	Bounding assumption
Pipe break and LOCA initiating event frequencies are based on pipe lengths from design documents.	Common engineering practice
A turbine trip is included in a general reactor trip despite the ability of the NuScale design to support 100 percent bypass flow.	Bounding simplification
A SGTF initiating event is assumed to be failure of a single tube. Because the steam generator tubes are in compression, multiple tube failures are assumed not to be a credible initiating event.	Engineering judgment
Systems Analysis	
Equipment is generally assumed to be operable without heating, ventilation, and air conditioning systems to support the PRA function. Outdoor equipment (e.g., DWS) is maintained ready to operate.	Engineering judgment
Air or operator action ensures that valves are open to provide flowpaths for mitigating systems (e.g., CVCS demineralized water isolation valves).	Common engineering practice and engineering judgment
Inventory from the DWST and UHS is sufficient to provide inventory to the CVCS and CFDS, respectively, for the PRA mission.	Common engineering practice and engineering judgment
Component failure modes (e.g., spurious failures) are generally not modeled if they met the ASME/ANS PRA Standard screening criterion (i.e., Supporting Requirement SY-A15).	Common engineering practice
Although shared systems are considered in the PRA (e.g., CFDS, DWS), they are available to be realigned to support accident mitigation.	Common engineering practice and engineering judgment
System models include assumptions on operating alignments (e.g., primary and backup pumps, electrical bus supplies).	Common engineering practice
The electric power system fault trees include modeling simplifications (e.g., automatic cross-ties are not modeled, power supplies to shared systems are modeled as though they are provided exclusively from module 1).	Bounding simplification
The MPS fault tree includes assumptions and simplifications (e.g., maintenance unavailability for the SVMs is accounted for on channel X but includes unavailability on channels Y and Z).	Bounding simplification
Only a subset of transmitters is credited in actuating the MPS; multiple sensor groups are typically capable of detecting the need for a protective action.	Bounding simplification
The auxiliary AC power supply is a CTG.	Engineering judgment
Testing and maintenance on the DHRS and ECCS is performed during refueling outages.	Common engineering practice and engineering judgment

Table 19.1-21: Key Assumptions for the Level 1 Full Power Internal Events Probabilistic Risk Assessment (Continued)

Assumption	Basis
One RSV is sufficient to reduce pressure and the uncertainty in the heat transfer mechanism (single-phase conduction/convention) that allows the RSVs to passively remove heat from the RPV is negligible.	Common engineering practice and engineering judgment
The probability that an RSV fails to reclose assumes that liquid water is passed (versus steam) when demanded.	Bounding simplification
The CFWS and MSS are not considered as mitigating systems; because almost any unplanned transient results in actuation of DHRS, it also includes isolation of the feedwater and main steam lines.	Bounding simplification
Accident Sequence	
Based on the RPV ultimate pressure capacity analysis, a flange gap is expected to form at the outer O-ring of the pressurizer heater access ports in an RPV overpressure sequence. This leak area relieves RCS and RPV pressure, without further pressurization. Based on thermal-hydraulic simulation results, this sequence of failures is modeled as core damage without a consequential containment failure.	Engineering analysis and judgment
Restoration of offsite power is only considered within 24 hours on the basis of precluding an ECCS demand; further recovery or mitigation is not considered.	Bounding simplification
Success Criteria	
Success criteria and accident sequence progression are based on plant-specific thermal-hydraulic analyses which are based on best estimates of the design for the design certification and include bounding simplifications (e.g., CVCS breaks are simulated as double-ended guillotine breaks, an end-of-cycle core is used because it is most challenging with respect to decay heat).	Common engineering practice and engineering judgment, bounding simplification
An accident sequence is assigned an “OK” end state in the Level 1 if it is simulated directly by thermal-hydraulic analysis and the results meet the success criteria (i.e., PCT does not reach 2,200 degrees Fahrenheit), or if a similar but more challenging simulated sequence demonstrates success.	Common engineering practice and engineering judgment
The PRA mission time of 72 hours is sufficient to demonstrate that at a minimum, a stable or improving condition has been achieved and the overall success criterion is met.	Common engineering practice
Operators 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 containment isolation valves to inject makeup following incomplete ECCS actuation).	Common engineering practice and engineering judgment
Human Reliability Analysis	
A simplified approach to HRA is used to model pre-initiator and post-initiator operator actions (i.e., NUREG/CR-4772 and NUREG/CR-6883, respectively).	Common engineering practice
Deliberate or malicious acts such as sabotage are outside the scope of the HRA.	Common engineering practice
Control room staffing is based on the minimum staffing as described in Technical Specification 5.2.2 “Facility Staff.”	Common engineering practice
Pre-initiator and post-initiator human actions were identified through interviews with system engineers and operators.	Common engineering practice
Timing for post-initiator human actions is based on the timing from the limiting thermal-hydraulic analysis.	Common engineering practice and engineering judgment
Control room indication is available to operators unless there is a loss of all 4 EDSS busses.	Common engineering practice and engineering judgment

Table 19.1-21: Key Assumptions for the Level 1 Full Power Internal Events Probabilistic Risk Assessment (Continued)

Assumption	Basis
Operators are expected to readily identify cases where the initiator is a break in the CVCS injection line outside of containment (or discharge line), and actuate CFDS (or CVCS through the pressurizer spray line, respectively) if makeup is needed.	Common engineering practice and engineering judgment
The HEPs are assumed to have a lognormal distribution.	Common engineering practice and engineering judgment
Data Analysis	
Component failure rates and unavailabilities, based on generic data, are applicable to the NuScale design.	Common engineering practice
Component failure rates, based on design-specific analyses, are representative and appropriate. Examples include ECCS hydraulic-operated valve fails to operate and equipment interface module fails to operate.	Common engineering practice and engineering judgment
Component failure rates, based on engineering judgment, are representative and appropriate. Examples include ECCS reactor vent valve passive actuation to open fails and CVCS LOCA does not initiate excess flow check valve.	Common engineering practice and engineering judgment
Passive safety system reliability, based on plant-specific analysis, is representative; the analysis focuses on failures of the DHRS and ECCS natural circulation heat transfer mechanisms that provide core cooling and maintain the coolant pressure boundary.	Engineering analysis and judgment
Common cause failures follow the alpha factor model and are based on generic data; both are applicable to the NuScale design.	Common engineering practice
Standby failure rates are based on a non-staggered testing scheme.	Bounding simplification.
The refueling outage schedule is every 2 years.	Design condition
Quantification	
A simplified approach was used to address HEP dependencies; a second HEP in a cutset is set to moderate dependence, a third HEP in a cutset is set to high dependence, and additional HEPs in a cutset are set to complete dependence.	Bounding simplification
Maintenance is not performed concurrently on multiple trains of a system, multiple low voltage load centers, or both backup diesel generators.	Common engineering practice
Recovery of failed equipment or recovery of equipment that is in maintenance is not considered in the model.	Bounding simplification

Table 19.1-22: Sensitivity Studies for Level 1 Full Power, Internal Events Evaluation

Item	Modeling Assumption or Uncertainty	Sensitivity Study	Basis	Result
1.	Human Error Probability	Effect of HEP	Generic uncertainty identified in EPRI TR-1016737	Safety goals met irrespective of selected HEP.
1a.	5th percentile value	All HEPs (pre-initiator, post initiator and dependent probabilities) set to success.	Bounding representation of 5^{th} percentile value	CDF decreased slightly.
1b.	95th percentile value	All HEPs (pre-initiator, post initiator and dependent probabilities) set to failure.	Bounding representation of 95^{th} percentile value	CDF increased by two orders of magnitude in comparison to base case.
2.	Common cause failure	All CCFs set to 0.002, the mean value of the highest CCF demand event	Generic uncertainty identified in EPRI TR-1016737. Modeling simplification judged representative of 95th percentile value.	CDF increases to 4E-06/mcyr
3.	Initiating Event Frequency	Effect of uncertainty in initiating event frequencies.	Initiating event frequency for some initiating events is based on generic data	Safety goals met irrespective of initiating event frequency
3a.	IE-EHVS-LOOP	LOOP frequency increased to 1.0 per year (from 3.1E-02). LOOP frequency decreased by an order of magnitude (to 3.1E-3).	Address uncertainty of grid stability at various sites	CDF increase by a factor of 8. CDF decreased slightly.
3b.	IE-MSS---ALOCA-SG-	SGTF frequency increased from 4.0E-05 to 1.4E-03 per year.	Address uncertainty in unique design feature; value based on 2010 industry average data.	Negligible CDF change.
3c.	IE-TGS---FMSLB-UD	Secondary line break initiating event frequency increased from 4.4E-05 to 7.7E-03	Address uncertainty in nonsafety related initiator frequency; value based on 2010 industry average data.	CDF increased slightly.
3d.	IE-CVCS---ALOCA-CIC	Increase CVCS injection line LOCA inside containment initiating event frequency by an order of magnitude	Address design-specific uncertainty of very small LOCA inside containment resulting in containment isolation.	CDF increased slightly.
4.	Passive heat removal reliability	Increase the failure probability of passive heat removal (ECCS, DHRS) by an order of magnitude	Address the design-specific uncertainty of passive decay heat removal, including UHS reliability.	CDF increased slightly.
5.	ECCS opening on low differential pressure	Increase the failure probability of ECCS opening on low differential pressure from 0.1 to 0.5.	Address the design-specific uncertainty of ECCS success criteria	CDF increase by a factor of 2.
6.	Failure probability of sensors	Increase the failure probability of sensors an order of magnitude	Address the design-specific uncertainty of potentially utilizing new technologies (e.g., digital components) to monitor plant parameters.	Negligible CDF change.

Table 19.1-22: Sensitivity Studies for Level 1 Full Power, Internal Events Evaluation (Continued)

Item	Modeling Assumption or Uncertainty	Sensitivity Study	Basis	Result
7.	Credit for nonsafety systems	Focused PRA which credits only safety-related systems performed to evaluate RTNSS Criterion C.	Evaluate effect of crediting only safety-related systems with regard to safety goal conformance.	Safety goals met without credit for nonsafety-related systems: CDF is 3E-06/mcyr
8.	Core damage system importance and the use of generic data	Evaluate system importance for core damage; PRA systems are identified in Table 19.1-4	Evaluate PRA system importance to address the uncertainty of using generic LWR component failure data due to the absence of design-specific operating experience; evaluate system importance against the core damage risk significance threshold of CCDF $\geq 1 \times 10^{-5}$ /year, as identified in Table 19.1-19.	Three systems meet the core damage threshold for risk significance: the ECCS, the MPS, and the UHS. These systems are safety-related. In addition, the MPS comprises both the RTS and ESFAS subsystems.

Table 19.1-23: Key Insights from Level 1 Full Power, Internal Events Evaluation

Insight	Comment
Failure to scram events (ATWS) do not lead directly to core damage.	Core characteristics result in ATWS power levels that are comparable to decay heat levels. Heat transfer from CNV to reactor pool is adequate to prevent core damage and results in most ATWS sequences requiring approximately the same system success criteria as non-ATWS events.
Passive heat removal capability is sufficient to prevent core damage if RSVs cycle.	RSV cycling transfers adequate RCS water to CNV to allow heat transfer through RPV to CNV and ultimately reactor pool to remove decay heat.
Post-accident heat removal through steam generators or DHRS is unnecessary if RSVs cycle.	The SGs and DHRS provide effective heat removal paths to prevent core damage, but are unnecessary if RSV cycling allows heat transfer to reactor pool.
ECCS functions to preserve RCS inventory, which is sufficient to allow core cooling without RCS makeup from external source.	ECCS function provides natural circulation path through core and CNV, thus providing heat transfer to the reactor pool.
Containment isolation preserves RCS inventory for core cooling without external makeup.	Containment isolation eliminates the potential for breaks outside of containment to result in loss of RCS inventory. For breaks inside of containment, containment isolation is not necessary to support passive core cooling and heat removal.
Support systems are not needed for safety-related (ECCS, DHRS, RSVs) system function.	Safety-related mitigating systems are fail-safe on loss of power and do not require supporting systems such as lube oil, air or HVAC to function.
There are no risk significant, post-initiator human actions associated with the full-power PRA.	No operator actions, including backup and recovery actions, are risk significant to the CDF because of passive system reliability and fail-safe system design.
Risk significant SSC for external events are largely the same as those found risk significant for internal events.	The module response to external events is comparable to the response to internal event due to the passive features of the design and independence from support systems such as power. Additional systems and components have been identified as risk significant for external events due to a conservative evaluation.
Active systems providing backup inventory addition to the RPV are not risk significant.	Inventory addition is possible by the active systems CVCS and CFDS. Due to the reliability of the passive safety systems, the active systems providing this backup function were found not to be risk significant, as indicated in Table 19.1-20 and Table 19.1-64.

Table 19.1-24: Containment Penetrations

Penetration number[6]	Function	Isolation Method	Normal operating position[1]	PRA
CNV 1	FWS 1	Two valves	open	modeled[2]
CNV 2	FWS 2	Two valves	open	modeled[2]
CNV 3	MSS 1	Two valves	open	modeled[2]
CNV 4	MSS 2	Two valves	open	modeled[2]
CNV 5	RCCWS return	Two valves	open	screened[3]
CNV 6	RCS injection (CVCS)	Two valves	open	modeled
CNV 7	RCS Pressurizer spray (CVCS)	Two valves	open	modeled
CNV 8-9	I&C division 1 and 2	Sealed penetration	sealed	screened
CNV 10	CES	Two valves	open	modeled
CNV 11	CFDS	Two valves	closed	screened
CNV 12	RCCWS supply	Two valves	open	screened[3]
CNV 13	RCS discharge (CVCS)	Two valves	open	modeled
CNV 14	RPV high point degas (CVCS)	Two valves	closed	screened
CNV 15-16	Electrical 1 & 2 (pressurizer heater)	Sealed penetration	sealed	screened
CNV 17-20	I&C channels A-D	Sealed penetration	sealed	screened
CNV 21	n/a	n/a	n/a	n/a
CNV 22	DHRS 1	Closed loop	closed	screened[4]
CNV 23	DHRS 2	Closed loop	closed	screened[4]
CNV 24	CNV head manway	Bolted closure	closed	screened
CNV 25	Control rod drive mechanism access hatch	Bolted closure	closed	screened
CNV 26	CNV access manway	Bolted closure	closed	screened
CNV 27-30	SG plenum inspection ports 1-4	Bolted closure	closed	screened
CNV 31-32	Pressurizer heater access port 1 and 2	Sealed penetration	sealed	screened
CNV 33	RVV trip/reset 1	Sealed penetration	sealed	screened[5]
CNV 34	RVV trip/reset 2	Sealed penetration	sealed	screened[5]
CNV 35	RRV trip/reset 1	Sealed penetration	sealed	screened[5]
CNV 36	RRV trip/reset 2	Sealed penetration	sealed	screened[5]
CNV 37	Electrical control rod drive mechanism power	Sealed penetration	sealed	screened
CNV 38-39	I&C rod position indication group 1 and 2	Sealed penetration	sealed	screened
CNV 40	RVV trip/reset 3	Sealed penetration	sealed	screened[5]
CNV 41	RVV trip 3	Sealed penetration	sealed	screened[5]

Notes:

1. Normally closed and sealed penetrations are screened.
2. Because these lines are not connected directly to the RCS, an SGTF is also required for a release outside containment.
3. Because the RCCWS is a closed loop inside containment, and not connected directly to the RCS, it is screened.
4. Because the DHRS lines are not connected directly to the RCS, and the FWS and MSS isolation valves (CNV penetrations 1-4) act as the CIVs for the DHRS lines, the DHRS penetrations are screened.
5. The ECCS valve trip/reset pilot assembly safe-end penetrations are welded to the external side of the penetration nozzle; each has a double seal with monitor capability.
6. Although not identified by a penetration number, the CNV is designed in two parts that are connected at the CNV main flange; it is normally closed and therefore screened.

Table 19.1-25: Significant Large Release Sequences (Full Power, Internal Events, Single Module)

Event Tree Initiator	Sequence	Contribution (% LRF)	Sequence Description
CVCS charging line break outside CNV (IE-CVCS--ALOCA-COC)	Figure 19.1-2 Sequence 7	93	A CVCS injection line LOCA outside containment initiating event followed by a failure to isolate the break, and a failure to make up inventory from the CFDS.
CVCS letdown line break outside CNV (IE-CVCS--ALOCA-LOC)	Figure 19.1-3 Sequence 9	6	A CVCS discharge line LOCA outside containment initiating event followed by a failure to isolate the break, and a failure to make up inventory from the CFDS.
SGTF (IE-MSS---ALOCA-SG)	Figure 19.1-7 Sequence 9	1	An SGTF initiating event with a failure to isolate the feedwater or steam line on the secondary side, and failure to provide make up inventory from the CVCS or CDFS.

Table 19.1-26: Significant Large Release Cutsets (Full Power, Internal Events, Single Module)

Cutset	Prob/Freq	Contribution	Basic Event	Description
1	5.76E-12	33.1%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	1.00E+0		CFDS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CFDS INJECTION
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
2	1.73E-12	9.9%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	1.20E-3		CFDS--HOV-0021X-FTO-N	HOV 0021X CNTS CFDS CONTAINMENT ISOLATION VALVE FAILS TO OPEN
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
3	1.73E-12	9.9%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	1.20E-3		CFDS--HOV-0022X-FTO-N	HOV 0022X CNTS CFDS CONTAINMENT ISOLATION VALVE FAILS TO OPEN
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
4	1.37E-12	7.9%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	9.51E-4		CFDS0AAOV-0010X-FTO-N	AOV 0010X CFDS MODULE 1 ISOLATION VALVE FAILS TO OPEN
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
5	5.21E-13	3.0%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE

Table 19.1-26: Significant Large Release Cutsets (Full Power, Internal Events, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	3.62E-4		MPS---EIM-1010X-FOP-S	EIM 1010X DIVISION I ESFAS EIM 10 FAILS TO OPERATE
6	5.21E-13	3.0%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	3.62E-4		MPS---EIM-1009X-FOP-S	EIM 1009X DIVISION I ESFAS EIM 09 FAILS TO OPERATE
7	5.21E-13	3.0%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	3.62E-4		MPS---EIM-2010X-FOP-S	EIM 2010X DIVISION II ESFAS EIM 10 FAILS TO OPERATE
8	5.21E-13	3.0%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	3.62E-4		MPS---EIM-2009X-FOP-S	EIM 2009X DIVISION II ESFAS EIM 09 FAILS TO OPERATE
9	4.32E-13	2.5%		
	1.40E-4		IE-CVCS--ALOCA-LOC	CVCS LOCA Letdown Line Outside Containment
	1.00E+0		CFDS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CFDS INJECTION
	1.00E+0		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.50E-1		HEP02	HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE

Table 19.1-26: Significant Large Release Cutsets (Full Power, Internal Events, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
10	3.65E-13	2.1%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	1.00E+0		CFDS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CFDS INJECTION
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	3.26E-6		MPS---APL-5CC22-FOP-S	CCF OF 2 OF 2 APL MODULES IN CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES
11	1.82E-13	1.1%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	1.26E-4		MPS---MSW-2001X-FTC-S	MSW 2001X MANUAL DIVISION II ESFAS NS ENABLE SWITCH FAILS TO CLOSE
12	1.82E-13	1.1%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	1.26E-4		MPS---MSW-1004X-FTC-S	MSW 1004X MANUAL DIVISION I CIS OVERRIDE SWITCH FAILS TO CLOSE
13	1.82E-13	1.1%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	1.26E-4		MPS---MSW-1001X-FTC-S	MSW 1001X MANUAL DIVISION I ESFAS NS ENABLE SWITCH FAILS TO CLOSE
14	1.82E-13	1.1%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE

Table 19.1-26: Significant Large Release Cutsets (Full Power, Internal Events, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	1.26E-4		MPS---MSW-2004X-FTC-S	MSW 2004X MANUAL DIVISION II CIS OVERRIDE SWITCH FAILS TO CLOSE
15	1.61E-13	0.9%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	1.00E+0		CFDS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CFDS INJECTION
	1.20E-3		CVCS--HOV-0334X-FTC-S	HOV 0334X CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVE FAILS TO CLOSE
	1.20E-3		CVCS--HOV-0335X-FTC-S	HOV 0335X CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVE FAILS TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
16	1.09E-13	0.6%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	1.20E-3		CFDS--HOV-0022X-FTO-N	HOV 0022X CNTS CFDS CONTAINMENT ISOLATION VALVE FAILS TO OPEN
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	3.26E-6		MPS---APL-5CC22-FOP-S	CCF OF 2 OF 2 APL MODULES IN CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES
17	1.09E-13	0.6%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	1.20E-3		CFDS--HOV-0021X-FTO-N	HOV 0021X CNTS CFDS CONTAINMENT ISOLATION VALVE FAILS TO OPEN
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	3.26E-6		MPS---APL-5CC22-FOP-S	CCF OF 2 OF 2 APL MODULES IN CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES
18	1.09E-13	0.6%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	7.60E-5		MPS---APL-2009X2FOP-S	APL 2009X2 (or 2010X2) DIVISION II ESFAS EIM 09 ACTUATION PRIORITY LOGIC MODULE 2 FAILS TO OPERATE

Table 19.1-26: Significant Large Release Cutsets (Full Power, Internal Events, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
19	1.09E-13	0.6%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	7.60E-5		MPS---APL-1009X2FOP-S	APL 1009X2 (or 1010X2) DIVISION I ESFAS EIM 09 ACTUATION PRIORITY LOGIC MODULE 2 FAILS TO OPERATE
20	1.09E-13	0.6%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	7.60E-5		MPS---HWM-2002X-FOP-S	HWM 2002X MPS DIVISION II HARD-WIRED MODULE FOR ESFAS FAILS TO OPERATE
21	1.09E-13	0.6%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	7.60E-5		MPS---HWM-1002X-FOP-S	HWM 1002X MPS DIVISION I HARD-WIRED MODULE FOR ESFAS FAILS TO OPERATE
22	9.09E-14	0.5%		
	1.40E-4		IE-CVCS--ALOCA-LOC	CVCS LOCA Letdown Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	1.26E-4		MPS---MSW-2001X-FTC-S	MSW 2001X MANUAL DIVISION II ESFAS NS ENABLE SWITCH FAILS TO CLOSE
23	9.09E-14	0.5%		
	1.40E-4		IE-CVCS--ALOCA-LOC	CVCS LOCA Letdown Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE

Table 19.1-26: Significant Large Release Cutsets (Full Power, Internal Events, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	1.26E-4		MPS---MSW-1004X-FTC-S	MSW 1004X MANUAL DIVISION I CIS OVERRIDE SWITCH FAILS TO CLOSE
24	9.09E-14	0.5%		
	1.40E-4		IE-CVCS--ALOCA-LOC	CVCS LOCA Letdown Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	1.26E-4		MPS---MSW-1001X-FTC-S	MSW 1001X MANUAL DIVISION I ESFAS NS ENABLE SWITCH FAILS TO CLOSE
25	9.09E-14	0.5%		
	1.40E-4		IE-CVCS--ALOCA-LOC	CVCS LOCA Letdown Line Outside Containment
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	1.26E-4		MPS---MSW-2004X-FTC-S	MSW 2004X MANUAL DIVISION II CIS OVERRIDE SWITCH FAILS TO CLOSE
26	8.67E-14	0.5%		
	2.80E-4		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	9.51E-4		CFDS0AAOV-0010X-FTO-N	AOV 0010X CFDS MODULE 1 ISOLATION VALVE FAILS TO OPEN
	1.00E-1		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	3.26E-6		MPS---APL-5CC22-FOP-S	CCF OF 2 OF 2 APL MODULES IN CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES

Table 19.1-27: Listing of Candidate Risk Significant Structures, Systems, and Components (Full Power, Single Module) Level 2 Probabilistic Risk Assessment

System	Description	CLRF	FVLRF
CNTS	Containment system	Met	
MPS	Module protection system	Met	
Component	**Basic Event Description**	**CLRF**	**FVLRF**
CVCS-HOV-0334X	HOV 0334X CNTS CVCS discharge line containment isolation valve	Not Met	Met[1]
CVCS-HOV-0335X	HOV 0335X CNTS CVCS discharge line containment isolation valve	Not Met	Met[1]
Human Action	**Description**	**CLRF**	**FVLRF**
CFDS-HFE-0001C	Operator fails to initiate CFDS injection	Not Met	Met
Initiator	**Description**	**CLRF**	**FVLRF**
IE-CVCS--ALOCA-COC	CVCS LOCA charging line outside containment		Met

Notes:

- Spaces that are grayed out indicate categories in which the criteria do not apply, as described in TR-0515-13952-A.

[1] The criterion is 'Met' with CCFs conservatively included in the calculation of the single component FV.

Table 19.1-28: Key Assumptions for the Level 2 Full Power Internal Events Probabilistic Risk Assessment

Assumption	Basis
Containment penetrations are screened if they are sealed, normally closed, or formed a closed loop inside containment; screened penetrations are assumed to be negligible contributors to the potential for a containment release. The CNV is maintained at a vacuum during normal operation.	Common engineering practice and engineering judgment.
Only the first two CIVs are modeled; many lines include additional isolation valves that are not considered.	Bounding simplification
A single sensor group is modeled to initiate containment isolation. The design includes multiple sensor groups that may initiate containment isolation.	Bounding assumption
The probability of a thermally induced SGTF is based on a creep rupture model that uses historical data for conventional SG tube flaws and time-history temperature and pressure conditions representative of NuScale severe accident progression. In the NuScale design, the steam generator tubes are in compression (i.e., feedwater is on the inside and primary reactor coolant circulates on the outside) which is opposite the typical tensile stresses in conventional plants. A thermally induced SGTF is assumed to result in a double-ended rupture of a single tube.	Engineering analysis and judgment
Core damage sequences are binned into a single plant damage state (i.e., core damage). Source term release categories are binned into two release categories (i.e., core damage with containment isolation, and core damage with failure of containment isolation or bypass). Additional plant damage states and release categories are not needed to support evaluation of a large release.	Common engineering practice and bounding assumption
Core damage sequences that include containment bypass or failure of containment isolation are typically assumed to result in a large release; a large release is defined as a release that results in an acute whole body 200 rem dose to a hypothetical individual located at the reactor site boundary over the course of 96 hours.	Bounding assumption
Mitigating factors such as fission product deposition, retention or scrubbing of fission products (e.g., spray or filtration), or deflection or absorption (i.e., biological shield) are not credited in the Level 2 PRA.	Bounding assumption
The Level 2 PRA does not credit recovery of the containment envelope (e.g., through implementation of severe accident management guidelines), if lost.	Bounding assumption

Table 19.1-29: Generic Sources of Level 2 Model Uncertainty

Uncertainty Source	Description (Reference 19.1-7)	Level 2 Assumption	Effect on Model
	Level 2 Analysis		
Core melt arrest in-vessel	Typically, the treatment of core melt arrest in-vessel has been limited. However, recent NRC work has indicated that there may be more potential than previously credited.	Conservative analysis has been performed that shows core melt arrest in-vessel in the RPV in all severe accident scenarios with containment isolation (or injection from the CFDS); heat transfer occurs through the water in the CNV and reactor pool.	Heat transfer occurs through the water in the CNV and reactor pool; water in the CNV ensures in-vessel retention in the RPV. As such, this is judged not to be a source of significant model uncertainty.
Thermally induced failure of hot leg/SG tubes - PWRs	NRC analytical models and research findings continue to show that a thermally induced steam generator tube rupture (TI-SGTR) is more probable than predicted by the industry. There is a need to come to agreement with NRC on the thermal hydraulics modeling of TI SGTR.	Based on design-specific analysis, a thermally-induced SGTF is included in the model following core damage.	Because thermally induced SGTFs are considered and Sensitivity Study 3b (provided in Table 19.1-22 and Table 19.1-31) is included on the failure probability, this is not judged to be a source of significant model uncertainty.
Vessel failure mode	The progression of core melt to the point of vessel failure remains uncertain. Some codes (MELCOR) predict that even vessels with lower head penetrations remain intact until the water has evaporated from above the relocated core debris. Other codes (MAAP) predict that lower head penetrations might fail early. The failure mode of the vessel and associate timing can impact LERF binning, and may influence HPME characteristics (especially for some BWRs and PWR ice condenser plants).	There are no penetrations in the RPV lower head. In sequences where thermal-hydraulic simulations predict the ultimate failure pressure is reached (i.e., penetration in upper head), RPV failure and core damage are assumed.	Because the PRA models RPV failure and core damage in sequences with inadequate pressure relief, this uncertainty has been addressed conservatively.
Ex-vessel cooling of lower head	The lower vessel head of some plants may be submerged in water prior to the relocation of core debris to the lower head. This presents the potential for the core debris to be retained in-vessel by ex-vessel cooling. This is a complex analysis impacted by insulation, vessel design and degree of submergence.	Conservative analysis has been performed that shows in-vessel retention in the RPV for core damage accidents with containment isolation (or injection from the CFDS); heat transfer occurs through the water in the CNV and reactor pool.	Based on conservative analysis, ex-vessel cooling of the lower head is ensured in sequences with containment isolation (or injection from the CFDS). As such, this is judged not to be a source of significant model uncertainty.

Table 19.1-29: Generic Sources of Level 2 Model Uncertainty (Continued)

Uncertainty Source	Description (Reference 19.1-7)	Level 2 Assumption	Effect on Model
Core debris contact with containment	In some plants, core debris can come in contact with the containment shell (e.g., some BWR Mark I, some PWRs including free-standing steel containments). Molten-core debris can challenge the integrity of the containment boundary. Some analyses have demonstrated that core debris can be cooled by overlying water pools.	Conservative analysis demonstrates in-vessel retention for the RPV following containment isolation (or injection from the CFDS).	Based on the RPV in-vessel retention analysis, with the CNV immersed in the reactor pool, this is judged not to be a source of significant model uncertainty.
ISLOCA initiating event frequency determination	ISLOCA is often a significant contributor to LERF. One key input to the ISLOCA analysis are the assumptions related to CCF of isolation valves between the RCS/RPV and low pressure piping. There is no consensus approach to the data or treatment of this issue. Additionally, given an overpressure condition in low pressure piping, there is uncertainty surrounding the failure mode of the piping.	There is no low pressure piping connected to the RCS susceptible to this failure model. Redundant CIVs are included on all RPV and CNV penetrations.	Because the PRA assesses the potential for pipe breaks outside containment (i.e., CVCS injection and discharge line break outside containment initiating events), this is judged not to be a source of significant model uncertainty.
Treatment of hydrogen combustion in BWR Mark III and PWR ice condenser plants	The amount of hydrogen burned, the rate at which it is generated and burned, the pressure reduction credited by the suppression pool, ice condenser, structures, etc. can have a significant impact on the accident sequence progression.	The CNV is not threatened because of the combination of limited oxygen, the equivalence ratio, and the steam concentration.	This is judged not to be a source of significant model uncertainty based on conservative, plant-specific analysis of the potential for hydrogen deflagration and detonation.

Table 19.1-30: Design-Specific Sources of Level 2 Model Uncertainty

Uncertainty Source	Description	Level 2 Assumption	Effect on Model
Level 2 Analysis			
Large release definition	Definition and modeling of a large release.	The failure of containment isolation is assumed to result in a large release and there is no credit for mitigation (e.g., deposition).	This is a bounding assumption; sequences with a failure of containment isolation are included in the frequency of a large release.
Level 2 physical phenomena	Susceptibility of the design to the typical severe accident phenomena that challenge containment, including hydrogen combustion, steam explosion, high pressure melt ejection, containment pressurization from a LOCA blowdown, overpressure, etc.	Based on design-specific analysis, the design is not susceptible to the typical severe accident phenomena. Severe accidents do not generate enough steam or hydrogen to pose a threat, the design pressure of the CNV is high, and immersion in the reactor pool is an effective heat removal mechanism.	The containment event tree is limited to failures of containment isolation and induced SGTFs. This is judged not to be a significant source of model uncertainty because of CNV immersion in the reactor pool, which contains sufficient water inventory to cool modules for an extended period under adverse conditions.

Table 19.1-31: Sensitivity Studies for Level 2 Evaluation

Item	Modeling Assumption or Uncertainty	Sensitivity Study	Basis	Result
1.	Human Error Probability	Effect of HEP	Generic uncertainty identified in Reference 19.1-7 (EPRI TR-1016737)	Safety goals met irrespective of selected HEP
1a.	5th percentile value	All HEPs (pre-initiator, post initiator and dependent probabilities) set to success.	Bounding representation of 5th percentile value	LRF decreased slightly.
1b.	95th percentile value	All HEPs (pre-initiator, post initiator and dependent probabilities) set to failure.	Bounding representation of 95th percentile value	LRF increased by over 2 orders of magnitude in comparison to base case.
2.	Common cause failure	All CCFs set to 0.002, the mean value of the highest CCF demand event.	Generic uncertainty identified in EPRI TR-1016737. Modeling simplification judged representative of 95th percentile value.	LRF increases to 4E-08/mcyr.
3.	Initiating Event Frequency	Effect of uncertainty in initiating event frequencies.	Initiating event frequency for some initiating events is based on generic data	Safety goals met irrespective of initiating event frequency.
3a.	IE-EHVS-LOOP	LOOP frequency increased to 1.0 per year (from 3.1E-02). LOOP frequency also decreased one order of magnitude.	Address uncertainty of grid stability at various sites	Negligible LRF change
3b.	IE-MSS---ALOCA-SG-	SGTF frequency increased from 4.0E-05 to 1.4E-03 per year.	Address uncertainty in unique design feature; value based on 2010 industry average data.	Negligible LRF change
3c.	IE-TGS---FMSLB-UD	Secondary line break initiating event frequency increased from 4.4E-05 to 7.7E-03.	Address uncertainty in nonsafety related initiator frequency; value based on 2010 industry average data.	Negligible LRF change
3d.	IE-CVCS—ALOCA-CIC	Increase CVCS injection line LOCA inside containment initiating event frequency by an order of magnitude	Address design-specific uncertainty of very small LOCA inside containment resulting in containment isolation.	Negligible LRF change
4.	Passive heat removal reliability	Increase the failure probability of passive heat removal (ECCS, DHRS) by an order of magnitude	Address the design-specific uncertainty of passive decay heat removal, including UHS reliability.	Negligible LRF change
5.	ECCS opening on low differential pressure	Increase the failure probability of ECCS opening on low differential pressure from 0.1 to 0.5.	Address the design-specific uncertainty of ECCS success criteria.	Negligible LRF change
6.	Failure probability of sensors	Increase the failure probability of sensors an order of magnitude.	Address the design-specific uncertainty of potentially utilizing new technologies (e.g., digital components) to monitor plant parameters.	Negligible LRF change
7.	Credit for nonsafety systems	Focused PRA which credits only safety-related systems performed to evaluate RTNSS Criterion C.	Evaluate effect of crediting only safety-related systems with regard to safety goal conformance.	Safety goals met without credit for nonsafety-related systems: LRF is 2E-07/mcyr

Table 19.1-31: Sensitivity Studies for Level 2 Evaluation (Continued)

Item	Modeling Assumption or Uncertainty	Sensitivity Study	Basis	Result
8.	Large release system importance and the use of generic data	Evaluate system importance for large release; PRA systems are identified in Table 19.1-4.	Evaluate PRA system importance to address the uncertainty of using generic LWR component failure data due to the absence of design-specific operating experience; evaluate system importance against the large release risk significance threshold of CLRF ≥ 1 x 10^{-6} /year, as identified in Table 19.1-19.	Two systems meet the large release threshold for risk significance: the CNTS and the MPS. These systems are safety-related.
9.	Probability of induced SGTF	Increase the probability of an induced SGTF using the 95th percentile value of the creep rupture model.	Address the uncertainty in creep rupture failure on SG tubes.	Negligible LRF change

Table 19.1-32: Key Insights from Level 2 Evaluation

Insight		Comment
Containment Isolation	The primary purpose of CNTS is to retain primary coolant inventory within the CNV. With primary coolant inventory maintained in the RPV or CNV, cooling of core debris is ensured.	If coolant remains primarily within the RPV, then the core is covered. If the core is not covered in the RPV then sufficient primary coolant is in the CNV to submerge the outside of the lower RPV and establish conductive heat removal from the core debris to the coolant in the CNV through the RPV wall.
	CNTS terminates releases through penetrations leading outside containment.	Containment penetrations through which releases are assumed to occur that dominate risk include those that bypass containment such as CVCS (injection and discharge) and paths through the steam generator tubes (main steam and feedwater piping). Isolation of normally open valves in these penetrations prevents releases from bypassing containment.
Passive Heat Removal	The RPV has no insulating material and passive heat removal capability from the RPV to the CNV is sufficient to prevent core debris from penetrating the reactor vessel.	Retaining primary coolant in the containment results in collection of sufficient RCS water in the CNV to allow heat transfer through RPV to CNV and ultimately UHS to remove heat generated in the fuel regardless of its location.
	The CNV is uninsulated and passive heat removal capability from the CNV to the UHS is sufficient to prevent the containment from pressurizing and or core debris from penetrating the containment	

Table 19.1-32: Key Insights from Level 2 Evaluation (Continued)

Insight		Comment
Severe Accident Containment Challenges	Primary coolant system overpressure failure cannot lead to overpressurization of containment (i.e., loss of decay heat removal through the steam generators plus failure of the RSVs to open).	Addition of water to the containment from external sources (CFDS) results in submergence of the reactor vessel and establishes passive heat removal through the containment wall to the reactor pool. Even if containment flooding is not successful, the RPV failure mode is such that containment ultimate capacity would not be exceeded.
	Hydrogen combustion is not likely as the containment is normally evacuated.	There is very little oxygen available (oxygen generated from radiolysis is only a long-term issue) and containment is steam inerted under severe accident conditions. In addition, conservative AICC analyses predict containment pressures that do not exceed the design pressure.
	In-vessel steam explosions are not likely due to core support design and volume of lower vessel head.	Core support failure is expected before the fuel has a chance to become molten. With the core uncovered there is little water in the bottom of the RPV with which core debris can interact.
	HPME cannot occur.	Submergence of the lower RPV establishes passive heat removal and prevents core debris from exiting the RPV. No ex-vessel challenges occur if the core remains within the vessel. With passive heat removal from the reactor to containment established, the reactor is depressurized even if core debris is postulated to exit the vessel.
	Ex-vessel steam explosion does not occur with a submerged RPV.	Submergence of the lower RPV establishes passive heat removal and prevents core debris from exiting the RPV. No ex-vessel challenges occur if the core remains within the vessel.
	Overpressure of containment due to non-condensable gas generation is not applicable to the NuScale design.	There is no concrete in the containment with which the core debris could interact and generate non-condensable gases.
	Basemat penetration is not applicable to the NuScale design.	There is no basemat making up the containment boundary. This issue is addressed as a part of considering protection against contact of core debris with the containment wall.
Support Systems	Support systems are not needed for safety-related system functions (i.e., containment isolation) important to the Level 2 PRA.	Safety-related mitigating systems are fail-safe on loss of power and do not require supporting systems such as lube oil, instrument air, or HVAC to function.
Human Action	With one exception, there are no risk significant, post-accident human actions associated with the full-power internal events Level 2 PRA. The exception is alignment of containment flooding (CFDS) during accident sequences in which isolation of a broken CVCS line outside containment fails, ECCS is successful but coolant inventory in containment needs replenishment in order to maintain natural circulation between CNV and the RPV.	Operator actions, including backup and recovery actions, are not significant to the Level 2 analysis because of passive system reliability and fail-safe system design. The operator action to align CFDS during a CVCS break outside containment meets the risk significance thresholds because of a mathematical limitation of the calculation of the Fussell-Vesely measure of importance.
External Events	Risk significant SSC for external events are largely the same as those found risk significant for internal events.	The module response to external events is comparable to the response to internal event due to the passive features of the design which are not affected by the external events and plant systems (CNTS) that are protected against external event challenges.

Table 19.1-33: External Events Screening Criteria

Number	Preliminary Screening Criterion
1	The hazard has a significantly lower mean frequency of occurrence than another hazard, taking into account the uncertainties in the estimates of both frequencies, and the hazard could not result in worse consequences than the consequences from the other hazard. The phrase significantly lower' implies that the screened hazard has a mean frequency of occurrence that is at least two orders of magnitude less than (1%) the mean frequency of occurrence of the other event.
2	The hazard does not result in a plant trip (manual or automatic) or a controlled manual shutdown and does not impact a structure, system, or component that is required for accident mitigation from at-power transients or accidents. If credit is taken for operator actions to correct the condition to avoid a plant trip or controlled shutdown, then ensure the credited operator actions and associated equipment have an exceedingly low probability of failure (i.e., collectively less than or equal to 10^{-5}) following the applicable supporting requirements.
3	The impacts of the hazard cannot occur close enough to the plant to affect it.
4	The hazard is included in the definition of another event.
Letter	**Bounding Screening Criterion**
a	The mean frequency of the initiating event is less than 1E-6 per reactor year and less than 10% of the internal events mean CDF and core damage could not occur unless at least two trains of mitigating systems are failed independent of the event.
b	The mean frequency of the initiating event is less than 1E-7 per reactor year and less than 1% of the internal events mean CDF and the initiating event does not involve or create an intersystem LOCA, containment bypass failure, or direct core damage (e.g., RPV rupture).
c	The mean frequency of the initiating event is less than 1E-8 per reactor year.
d	The external hazard affects, directly and indirectly, only components in a single system, AND it can be shown that the product of the frequency of the external hazard and the probability of SSC failure given the hazard is at least two orders of magnitude lower than the product of the non-hazard (i.e., internal events) frequency for the corresponding initiating event in the PRA, and the random (non-external hazard) failure probability of the same SSC that are assumed failed by the external hazard. If the external hazard impacts multiple systems, directly or indirectly, do not screen on this basis.

Table 19.1-34: External Events Considered for Operations at Power

1. Aircraft impacts	
Description of hazard	An aircraft impact could damage plant structures and SSC (including the switchyard and equipment important to safety), and cause a plant trip.
Screening criteria	1 - The frequency of an aircraft crash that results in a LOOP, and loss of the CTG and BDG, is expected to have a significantly lower frequency than an external flood, and does not result in worse consequences. Therefore, this event is not considered in the PRA. When a site is selected, screening this hazard should be confirmed.
2. Avalanche	
Description of hazard	Avalanches are large masses of snow or ice detached from a mountain slope and sliding or falling suddenly down a mountainside. An avalanche could damage plant structures and SSC (including the switchyard and equipment important to safety), cause a plant trip, and block HVAC intakes and exhausts.
Screening criteria	1 - The frequency of an avalanche that results in a LOOP, and loss of the CTG and BDGs, is expected to have a significantly lower frequency than an external flood, and does not result in worse consequences. Therefore, this event is not considered in the PRA. When a site is selected, screening this hazard should be confirmed.
Similar hazards	• landslide • snow - fall that results in accumulation • volcanic activity
3. Biological events	
Description of hazard	Biological events refer to the fouling or plugging of service water or circulating water systems resulting from biological or microbiological growth or intrusion. They include detritus, zebra mussels, and algae, and are applicable to sites that use once-through water systems drawing water from rivers, lakes, ponds, or the ocean.
Screening criteria	1 -The frequency would be significantly less than the internal event LOOP (~3E-2 per year), and does not result in worse consequences. Therefore, this hazard is not considered in the PRA. When a site is selected and circulating water system details are finalized, screening this hazard should be confirmed.
4. Coastal erosion	
Description of hazard	Coastal erosion is erosion of coastal properties caused typically by hurricanes or other severe storms. Erosion is typically slow in developing and can remove soil and rock and result in flooding.
Screening criteria	4 - Coastal erosion is subsumed in hazard 6, external flooding.
5. Drought	
Description of hazard	Drought is defined as an extended period of abnormally dry weather with below normal precipitation that causes the lowering of lake and river levels and potential lowering of groundwater levels.
Screening criteria	1 -The frequency would be significantly less than the internal event LOOP (~3E-2 per year), and does not result in worse consequences. Therefore, this hazard is not considered in the PRA. When a site is selected and circulating water system details are finalized, screening this hazard should be confirmed.
Similar hazards	• low lake or river water level • river diversion
6. External flooding	
Description of hazard	External flooding is defined in NUREG/CR-5042 as "all phenomena leading to external flooding, in which the source of water that threatens plant structures and equipment is outside the plant." The definition of "plant" is not clear. However, in order to ensure that internal and external flooding cover all flood scenarios, external flooding is defined as all flood scenarios not covered in the internal flood PRA. External flooding includes the subsumed hazards listed below, as well as river or lake flooding, and floods from dam failure and snow melt. External floods of concern are those that affect plant equipment (e.g., power transformers) and cause a plant trip or plant shutdown, and impact equipment important to safety.
Screening criteria	Evaluated in Section 19.1.5.4.

Table 19.1-34: External Events Considered for Operations at Power (Continued)

Subsumed hazards	• coastal erosion • high tide • hurricane - flooding • ice cover - that results in blockage and subsequent flooding • precipitation, intense • river diversion - flooding • snow - melt that results in flooding • storm surge • tsunami • waves
7. Extreme winds and tornadoes	
Description of hazard	High winds from tornadoes, hurricanes, or wind storms are a potential threat to plant structures and SSC (including the switchyard and equipment important to safety) due to pressure differentials, generated missiles, or direct damage due to dynamic wind loadings.
Screening criteria	Evaluated in Section 19.1.5.5.
8. Fog	
Description of hazard	Fog is a visible mass consisting of cloud water droplets or ice crystals suspended in the air at or near the Earth's surface; fog is considered a low-lying cloud. The effects of fog may increase the likelihood of a man-made accident such as a transportation accident.
Screening criteria	4 - The increase in transportation accidents associated with fog is subsumed in hazard 34, transportation accidents.
9. Forest fire	
Description of hazard	External fires are those that occur outside the site boundary, and include forest fires, grass fires, and industrial fires. . Fires could result in control room habitability concerns and inhibit site operations.
Screening criteria	1 - Operators may shut down the plant in response to a forest fire, however, the frequency would be significantly less than the internal event LOOP (~3E-2 per year), and does not result in worse consequences. Therefore, this hazard is not considered in the PRA. When a site is selected, screening this hazard should be confirmed.
10. Frost	
Description of hazard	Frost is the coating or deposit of ice that forms in humid air in cold conditions.
Screening criteria	4 - Frost is subsumed in hazard 15, ice cover, and hazard 30, snow.
11. Hail	
Description of hazard	Hail is a form of solid precipitation and consists of balls or irregular lumps of ice. The main concern is damage from impact or loading.
Screening criteria	4 - Hail impacts are subsumed in hazard 36, turbine-generated missiles. Hail roof loading is subsumed in hazard 30, snow.
12. High summer temperatures	
Description of hazard	High temperatures can potentially impact the ultimate heat sink, HVAC system efficiency, offsite power reliability, and the electrical system.
Screening criteria	2 - High temperatures would not result in a plant trip from HVAC or cooling water considerations. Therefore, this hazard is not considered in the PRA. 4 - High summer temperatures that result in a LOOP are subsumed in the internal events LOOP.
13. High tide	
Description of hazard	Tides are the rise and fall of sea levels caused by the combined effects of gravitational forces exerted by the moon, sun, and rotation of the Earth. High tide is an external flooding concern.
Screening criteria	4 - High tide is subsumed in hazard 6, external flooding.
14. Hurricane	
Description of hazard	Hurricanes are extreme tropical storms that originate offshore and are characterized by high winds, intense precipitation, and storm surges. Hurricanes can result in high winds and flooding concerns.
Screening criteria	4 - Hurricane flooding is subsumed in hazard 6, external flooding. Hurricane winds are evaluated in Section 19.1.5.5.

Table 19.1-34: External Events Considered for Operations at Power (Continued)

15. Ice cover	
Description of hazard	The ice cover hazards can block rivers causing floods, and also impact cooling water intakes and reduce makeup inventory to systems that draw water from rivers, lakes or ponds. Frazil ice is a collection of loose, randomly oriented needle-shaped ice crystals in water that forms in open, turbulent, supercooled water.
Screening criteria	2 - Ice cover would not result in a plant trip because it does not impact cooling water intakes. Therefore, it is not considered in the PRA. 4 - Ice cover that would result in blockage and external flooding is covered in hazard 6, external flooding.
16. Industrial or military facility accident	
Description of hazard	Industrial and military facility accidents could impact the plant through a release of hazardous materials, explosions, or fires. The release of hazardous materials is a potential concern for control room habitability and operations personnel health. Explosions or missiles could damage site structures and equipment. Fires could result in control room habitability concerns and inhibit site operations.
Screening criteria	1 - An industrial or military facility accident could result in a LOOP, however, the frequency would be significantly less than the internal event LOOP (~3E-2 per year), and does not result in worse consequences. Therefore, this hazard is not considered in the PRA. When a site is selected, screening this hazard should be confirmed.
Similar hazards	• pipeline accidents • transportation accidents
17. Internal flooding	
Description of hazard	Internal flooding is defined as all events involving the effects of floods (including submergence, spray, jet impingement, etc.) originating inside the plant buildings/structures.
Screening criteria	Evaluated in Section 19.1.5.3.
18. Landslide	
Description of hazard	Landslides are large masses of dirt or rock swiftly moving down a slope. Similar to an avalanche, a landslide could damage plant structures and SSC (including the switchyard and equipment important to safety), cause a plant trip, and block HVAC intakes and exhausts.
Screening criteria	1 - The frequency of a landslide that results in a LOOP, and loss of the CTG and BDG, is expected to have a significantly lower frequency than an external flood, and does not result in worse consequences. Therefore, this event is not considered in the PRA. When a site is selected, screening this hazard should be confirmed.
Similar hazards	• avalanche • snow - fall that results in accumulation • volcanic activity
19. Lightning	
Description of hazard	Lightning is the static spark discharge resulting from the development of hundreds of millions of volts of electrical potential between clouds or between a cloud and the earth. It can be compared to the dielectric breakdown of a huge capacitor. It is the most frequent cause of overvoltage on electrical distribution systems. Lightning strikes can damage onsite electrical equipment and can impact the availability of offsite power
Screening criteria	4 - Lightning that would result in a LOOP is captured in the internal events LOOP.
20. Low lake or river level	
Description of hazard	Low lake levels or river stages can impact plants that rely on those sources for water supplies .The main concern is the potential loss of the UHS.
Screening criteria	1 -The frequency would be significantly less than the internal event LOOP (~3E-2 per year), and does not result in worse consequences. Therefore, this hazard is not considered in the PRA. When a site is selected and circulating water system details are finalized, screening this hazard should be confirmed.
Similar hazards	• drought • river diversions

Table 19.1-34: External Events Considered for Operations at Power (Continued)

21. Low winter temperature	
Description of hazard	Low winter temperatures can result in freezing of water in pipes, tanks, or reservoirs, or reduce the capability of the UHS.
Screening criteria	2 - This event does not result in a plant trip, therefore, it is not considered in the PRA.
22. Meteorite and satellite strikes	
Description of hazard	Meteorites are solar system objects that reach the ground before being vaporized. They have the potential to damage plant structures and SSC (including the switchyard and equipment important to safety), and cause a plant trip.
Screening criteria	n/a. A bounding assessment was performed.
23. Pipeline accident	
Description of hazard	Pipelines are used to transport working fluids in and among various systems and offsite transport materials across the U.S. Those of concern transport material that is combustible, explosive, or toxic. Pipeline accidents could pose a hazard to the plant due to the release of hazardous material or explosions that could damage site structures and equipment.
Screening criteria	1 - A pipeline accident could result in a LOOP, however, the frequency would be significantly less than the internal event LOOP (~3E-2 per year), and does not result in worse consequences. Therefore, this hazard is not considered in the PRA. When a site is selected, screening this hazard should be confirmed.
Similar hazards	• industrial or military facility accidents • transportation accidents
24. Precipitation, intense	
Description of hazard	Intense precipitation, including thunderstorms, may result in flooding or structural failures.
Screening criteria	4 - Intense precipitation is subsumed in hazard 6, external flooding.
25. Release of chemicals from on-site storage	
Description of hazard	The types of hazardous materials that may be released from onsite storage include diesel fuel oil, ammonia, chlorine, hydrogen, and other compressed gases (e.g., nitrogen), sodium hypochlorite, sulfuric acid, and others. Hazards include both explosive effects and toxic or asphyxiation impacts on control room habitability.
Screening criteria	1 - A shutdown in response to an on-sight explosion could be postulated, however, the frequency is expected to be significantly less than the internal event LOOP (~3E-2 per year), and does not result in worse consequences. Therefore, this hazard is not considered in the PRA. When all site chemicals are identified, including, locations, amounts, and operating control plans, screening this hazard should be confirmed.
26. River diversion	
Description of hazard	River diversion refers to the change in a river flow path or boundary resulting from natural phenomena such as flooding or seismic events. The main concern with river diversion is the potential loss of the UHS.
Screening criteria	2 - This event does not result in a plant trip, therefore, it is not considered in the PRA.
Similar hazards	• low lake or river level • river diversion
27. Sandstorm	
Description of hazard	Sand and dust storms involve strong winds entraining sand or dust into the atmosphere. Concerns are blockage of HVAC systems and effects on onsite and offsite electrical equipment.
Screening criteria	4 - Sand or dust that results in a LOOP is subsumed in the internal events LOOP.
28. Seiche	
Description of hazard	A seiche is a standing wave in an enclosed or partially enclosed body of water. The wave can be generated by meteorological effects, seismic activity, or tsunamis. The main concern with a seiche is flooding.
Screening criteria	4 - Seiche is subsumed in hazard 6, external flooding. In addition, a seismically-induced seiche in the reactor pool is not considered credible because the frequency response of the pool is much lower than the building natural frequencies and ground motions would not be significantly transmitted to the water.

Table 19.1-34: External Events Considered for Operations at Power (Continued)

29. Seismic	
Description of hazard	Seismic activity is the sudden release of energy in the Earth's crust, resulting in ground shaking and movement. Such events can damage plant structures and SSC, including the switchyard and equipment important to safety.
Screening criteria	Evaluated in Section 19.1.5.1
30.Snow	
Description of hazard	Excessive snow can result in additional loading on roofs, impacts on onsite and offsite power, and flooding during melting.
Screening criteria	1 - The frequency of a snow fall that results in a LOOP, and loss of the CTG and BDG, is expected to have a significantly lower frequency than an external flood, and does not result in worse consequences. Therefore, this event is not considered in the PRA. When a site is selected, screening this hazard should be confirmed. 4 - Snow melt resulting in flooding is subsumed in hazard 6, external flooding.
Similar hazards	• avalanche • landslide • volcanic activity
31. Soil shrink or swell	
Description of hazard	Some clays may swell (expand) when water is absorbed (i.e., wet), and shrink (contract) when the water dries up (i.e., dry). Significant expansion or contraction due to changes in moisture content can damage the foundations of the plant buildings/structures.
Screening criteria	2 - This event does not result in a plant trip, therefore, it is not considered in the PRA.
32. Storm surge	
Description of hazard	A storm surge involves coastal or estuarine flooding resulting from water level rise caused by a combination of tropical storms, extreme tides, and high local rainfall. The main concern with a storm surge is flooding.
Screening criteria	4 - Storm surge is subsumed in hazard 6, external flooding.
33. Toxic gas release	
Description of hazard	The toxic gas hazard is a potential concern for control room habitability and operations personnel health.
Screening criteria	2 - This event does not result in a plant trip, therefore, it is not considered in the PRA.
34. Transportation accidents	
Description of hazard	Transportation accidents include marine, railroad, and vehicle, both offsite and onsite. Hazards include the release of hazardous materials (i.e., toxic gas) that result in control room habitability concerns, explosions that could damage site structures and equipment, and fires.
Screening criteria	1 - A transportation accident could result in a LOOP, however, the frequency would be significantly less than the internal event LOOP (~3E-2 per year), and does not result in worse consequences. Therefore, this hazard is not considered in the PRA. When a site is selected, confirmation that this event can be screened is required.
Similar hazards	• industrial or military facility accident • pipeline accidents
35. Tsunami	
Description of hazard	A tsunami involves coastal or estuarine flooding resulting from a series of large water waves caused by displacement of a large volume of a body of water, usually an ocean. The displacement can be caused by seismic activity, volcanic eruptions, landslides, or other events. The hazard is flooding.
Screening criteria	4 - Tsunamis are subsumed in hazard 6, external flooding.
36 Turbine-generated missile	
Description of hazard	The turbine-generated missile hazard refers to main turbine generator blades failing and potentially penetrating the turbine casing and impacting PRA equipment.
Screening criteria	1 - A trip or loss of power could be postulated in response to a turbine-generated missile, however, the frequency is significantly less than the internal event LOOP (i.e., 1.2E-6 << 3E-2 per year), and does not result in worse consequences. Therefore, this hazard is not considered in the PRA.

Table 19.1-34: External Events Considered for Operations at Power (Continued)

37. Volcanic activity	
Description of hazard	Hazards associated with volcanic activity include lava flows and volcanic ashes. Either could damage plant structures and SSC (including the switchyard and equipment important to safety), cause a plant trip, and block HVAC intakes and exhausts. The ash could also result in additional roof loadings.
Screening criteria	1 - The frequency of volcanic activity that results in a LOOP, and loss of the CTG and BDG, is expected to have a significantly lower frequency than an external flood, and does not result in worse consequences. Therefore, this event is not considered in the PRA. When a site is selected, screening this hazard should be confirmed.
Similar hazards	• avalanche • landslide • snow - fall that results in accumulation
38. Waves	
Description of hazard	The hazard from waves is mainly associated with external flooding.
Screening criteria	4 - Waves are subsumed in hazard 6, external flooding.
39. Electro-magnetic interference	
Description of hazard	Electromagnetic interference, or radio-frequency interference, is a disturbance generated by an external source that may degrade electrical circuits.
Screening criteria	4 - An EMI that would result in a LOOP is captured in the internal events LOOP.
40. Radiation	
Description of hazard	Radiation is a potential concern for personnel health and control room habitability.
Screening criteria	1 - Operators may shut down the plant in response to a radiation hazard from another module, however, the frequency of a core damage and large release from another module is extremely low (< 1E-7 per year) and significantly less than the frequency of a LOOP (~3E-2 per year), and does not result in worse consequences. Therefore, this hazard is not considered in the PRA.
41. Sinkhole	
Description of hazard	A sink hole is a natural depression or hole in the earth's surface or subsurface caused by geologic processes involving soluble rocks such as limestone, dolomite, and gypsum. Sink holes could occur in an area of ground with no natural external surface drainage and all drainage occurs subsurface. Sinkholes are common where the rock below the land surface is limestone, carbonate rock, salt beds, or rocks that can naturally be dissolved by ground water circulating through them. As the rock dissolves, spaces and caverns develop underground. Sinkholes may be formed gradually or suddenly. The mechanisms of formation involve natural processes of erosion or gradual removal of slightly soluble bedrock by percolating water, the collapse of a cave roof, or a lowering of the water table. Over time, subsurface voids with the potential to impact the integrity of buildings/structures may form due to the loss of soil along with the water.
Screening criteria	1 - A sinkhole may result in a shutdown, however, the frequency would be significantly less than the internal event LOOP (~3E-2 per year), and does not result in worse consequences. Therefore, this hazard is not considered in the PRA. When a site is selected, screening this hazard should be confirmed.

Table 19.1-35: Structural Fragility Parameters and Results

Structures	A_m (g)	β_r	β_u	HCLPF (g)	Controlling Failure Mode	Assumed consequence
Reactor Building Crane	2.64	0.28	0.39	0.88	Bridge seismic restraint weldment yielding	Core damage / Large Release
Reactor Building Exterior Walls	1.92	0.12	0.33	0.92	Out-of-plane shear	Core damage / Large Release
NPM Supports	1.98	0.12	0.35	0.92	Shear failure of multiple shear lugs	Core damage/Large Release
Bio Shield - horizontal shear flexure -normal operation	11.62	0.28	0.37	3.99	Horizontal shield slab bending failure	Core damage / Large Release
Bio shield - horizontal shear flexure - double stacked for refueling of adjacent module	4.05	0.28	0.41	1.30	Bending failure of both stacked shield slabs	Core damage / Large Release when configuration present
Pool Walls	2.31	0.21	0.33	0.95	Out-of-plane shear	Core damage / Large Release
Crane Support Walls	2.61	0.12	0.34	1.23	Out-of-plane shear	Core damage / Large Release
Bay Walls	2.65	0.12	0.31	1.31	In-plane flexure	Core damage / Large Release
Roof	2.22	0.12	0.26	1.20	In-plane shear	Core damage / Large Release
Basemat	3.57	0.27	0.31	1.38	Out-of-plane shear	Core damage / Large Release

A_m = median seismic capacity; βu = uncertainty in the median seismic capacity; βr = randomness of the fragility evaluation; HCLPF = High-Confidence (95%) of a Low Probability (5%) of Failure (EPRI 103959)

Table 19.1-36: Seismic Margin Analysis Location Information

Location ID	Location Description
NPM	NUSCALE POWER MODULE
RXB	REACTOR BUILDING
CHILL	CHILLER BUILDING
HVSWG	HIGH VOLTAGE SWITCHGEAR
SITE	NUSCALE PLANT SITE GROUNDS
LVPDC	LOW VOLTAGE POWER DISTRIBUTION CENTER
MVSWG	MEDIUM VOLTAGE SWITCHGEAR
CRB	CONTROL BUILDING

Table 19.1-37: Seismic Margin Analysis Component Types

Component ID	Component Description
ACV	AIR OPERATED CONTROL VALVE
AOV	AIR OPERATED VALVE
BAT	BATTERY
BCH	BATTERY CHARGER
BIOBN	BIO SHIELD BAY WALL ANCHOR BOLT (NORMAL OPERATION)
BIOBR	BIO SHIELD BAY WALL ANCHOR BOLT REFUELING OPERATIONS)
BION	HORIZONTAL BIO SHIELD SLAB (NORMAL OPERATION)
BIOPN	BIO SHIELD POOL WALL ANCHOR BOLT (NORMAL OPERATION)
BIOPR	BIO SHIELD POOL WALL ANCHOR BOLT (REFUELING)
BIOR	HORIZONTAL BIO SHIELD SLAB (REFUELING)
BYW	REACTOR POOL BAY WALL
CBH	HIGH VOLTAGE CIRCUIT BREAKER
CBL	LOW VOLTAGE CIRCUIT BREAKER
CBM	MEDIUM VOLTAGE CIRCUIT BREAKER
CKV	CHECK VALVE
CRDGT	CONTROL ROD GUIDE TUBE
CRN	REACTOR BUILDING CRANE
CTG	COMBUSTION TURBINE GENERATOR
DGN	DIESEL GENERATOR
EBA	AC BUS
EBD	DC BUS
HOV	HYDRAULICALLY OPERATED VALVE
HTX	HEAT EXCHANGER
MCC	MOTOR CONTROL CENTER
MDP	MOTOR DRIVEN PUMP
MOV	MOTOR OPERATED VALVE
MSW	MANUAL SWITCH
RBW	REACTOR BUILDING WALL
RRV2	ALL ECCS REACTOR RECIRCULATION VALVES
RSV	REACTOR SAFETY VALVE
RTB	REACTOR TRIP SYSTEM CIRCUIT BREAKER
RVV3	ALL ECCS REACTOR VENT VALVES
SGT	STEAM GENERATOR TUBE
SOV	SOLENOID OPERATED VALVE
SUPP	MODULE SUPPORT
TFM	TRANSFORMER

Table 19.1-38: Seismic Correlation Class Information

Seismic Correlation Class	Component ID	Elevation (ft)	Location	NuScale Component	Failure Mode Description	A_m (g)	β_r (g)	β_u (g)	HCLPF (g)[1]	Contributes to seismic margin?[2]	Fragility Method[3]
Seismically Induced Initiating Events											
SUPP-75-RXB-SHR-SEIS	SUPP	75	RXB	NPM Supports	Shear Failure of Multiple Shear Lugs	1.98	0.12	0.35	0.92	Yes	DS
HTX---50--RXB---HXF-SEIS[4]	HTX	50	RXB	CVCS Heat Exchanger	Heat Exchanger Failure	6.81	0.32	0.51	1.74	No	Generic
RRV2--50--RXM---FTC-SEIS	RRV2	50	RXM	All ECCS Reactor Recirculation Valves	Fails to Close	3.32	0.24	0.32	1.32	No	DS
					Fails to Remain Closed						
					Spuriously Open						
RSV---75--RXM---FTC-SEIS[4]	RSV	75	RXM	All Reactor Safety Valves	Fails to Close	3.37	0.24	0.32	1.34	No	DS
					Fails to Remain Closed						
					Fails to Reclose						
					Spuriously Open						
RVV3--75--RXM---FTC-SEIS	RVV3	75	RXM	All ECCS Reactor Vent Valves	Fails to Close	2.38	0.28	0.5	0.66	No	DS
					Fails to Remain Closed						
					Spuriously Open						
SGT---50--RXM---BRK-SEIS[4]	SGT	50	RXM	Steam Generators	Tube/Support Failure	2.53	0.28	0.36	0.88	No	DS
TFM---100-SITE--CIF-SEIS	TFM	100	SITE	Offsite Power Transformer	Ceramic Insulator Failure	0.3	0.29	0.47	0.09	No	Generic
Structural Failure Events											
BIOBN-125-RXB---BSF-SEIS	BIOBN	125	RXB	Bioshield Bay Wall Anchor Bolts	Bolt Shear Failure - Normal Operation	4.89	0.28	0.35	1.73	Yes	DS
BIOBR-125-RXB---BSF-SEIS	BIOBR	125	RXB	Bioshield Bay Wall Anchor Bolts	Bolt Shear Failure - Refueling Adjacent Module	2.73	0.28	0.35	0.97	Yes	DS
BION--125-RXB---OPB-SEIS	BION	125	RXB	Horizontal Bioshield	Out of Plane Bending - Normal Operation	11.62	0.28	0.37	3.99	Yes	DS
BIOR--125-RXB---OPB-SEIS	BIOR	125	RXB	Horizontal Bioshield	Out of Plane Bending - Refueling Adjacent Module	4.05	0.28	0.41	1.3	Yes	DS
BYW-------RXB---FLX-SEIS	BYW	NA	RXB	Reactor Bay Wall	In-Plane Flexure Failure	2.65	0.12	0.31	1.31	Yes	DS
CRN---145-RXB---RWF-SEIS	CRN	145	RXB	Reactor Building Crane	Seismic Restraint Weldment Failure	2.64	0.28	0.39	0.88	Yes	DS
RBW-------RXB---OPS-SEIS	RBW	NA	RXB	Exterior Reactor Building Wall	Out of Plane Shear Failure	1.92	0.12	0.33	0.92	Yes	DS
Component Failure Events											
ACV---100-CHILL-FCR-SEIS	ACV	100	CHILL	DWS Recirc Control Valve	Fails to Control	9	0.32	0.52	2.26	No	Generic

Table 19.1-38: Seismic Correlation Class Information (Continued)

Seismic Correlation Class	Component ID	Elevation (ft)	Location	NuScale Component	Failure Mode Description	A_m (g)	β_r (g)	β_u (g)	HCLPF (g)[1]	Contributes to seismic margin?[2]	Fragility Method[3]
ACV---100-RXB---FTO-SEIS	ACV	100	RXB	CFDS Flow Control Valve	Fails to Open	4.41	0.32	0.52	1.11	No	Generic
ACV---100-RXM---FTC-SEIS	ACV	100	RXM	FWS Regulating Valve	Fails to Close	22.13	0.27	0.37	7.72	No	DS
ACV---100-RXM---FTO-SEIS	ACV	100	RXM	CVCS Control Valve	Fails to Open	0.57	0.32	0.52	0.14	No	Generic
AOV---100-CHILL-FTO-SEIS	AOV	100	CHILL	DWS Pump Isolation Valve	Fails to Open	9	0.32	0.52	2.26	No	Generic
AOV---100-RXB---FTC-SEIS	AOV	100	RXB	CFDS Drain Valve	Fails to Close	4.41	0.32	0.52	1.11	No	Generic
AOV---100-RXB---FTO-SEIS	AOV	100	RXB	CVCS Module Heatup Isolation Valve, CFDS Flooding Valve	Fails to Open	0.57	0.32	0.52	0.14	No	Generic
AOV---100-RXM---FTC-SEIS	AOV	100	RXM	MSS Secondary Isolation Valve	Fails to Close	22.13	0.27	0.37	7.72	No	DS
AOV---100-RXM---FTO-SEIS	AOV	100	RXM	CFDS Isolation Valve	Fails to Open	0.57	0.32	0.52	0.14	No	Generic
AOV---50--RXB---FTO-SEIS	AOV	50	RXB	CVCS DWS Supply Isolation Valve	Fails to Open	7.74	0.32	0.52	1.94	No	Generic
BAT---75--RXB---FOP-SEIS	BAT	75	RXB	RXM Batteries	Fails to Operate	4.37	0.24	0.39	1.55	No	Generic
BCH---86--RXB---FOP-SEIS	BCH	86	RXB	RXM Battery Chargers	Fails to Operate	2.11	0.24	0.39	0.75	No	Generic
CBH---100-HVSWG-FTC-SEIS	CBH	100	HVSWG	High Voltage Supply Circuit Breakers	Fails to Close	2.8	0.24	0.39	0.99	No	Generic
CBL---100-LVPDC-FTC-SEIS	CBL	100	LVPDC	Low Voltage Circuit Breakers	Fails to Close	5.9	0.24	0.39	2.09	No	Generic
CBM---100-MVSWG-FTC-SEIS	CBM	100	MVSWG	4KV Circuit Breakers	Fails to Close	2.8	0.24	0.39	0.99	No	Generic
CKV---100-CHILL-FTO-SEIS	CKV	100	CHILL	DWS Check Valve	Fails to Open	9	0.32	0.52	2.26	No	Generic
CKV---100-RXB---FTO-SEIS	CKV	100	RXB	CFDS Check Valve	Fails to Open	4.41	0.32	0.52	1.11	No	Generic
CKV---100-RXM---FTC-SEIS	CKV	100	RXM	CVCS Check Valve	Fails to Close	0.57	0.32	0.52	0.14	No	Generic
CKV---100-RXM---FTO-SEIS	CKV	100	RXM	CVCS Check Valve	Fails to Open	0.57	0.32	0.52	0.14	No	Generic
CKV---50--RXB---FTO-SEIS	CKV	50	RXB	DWS Check Valve	Fails to Open	7.74	0.32	0.52	1.94	No	Generic
CRDGT-75--RXM---DEF-SEIS	CRDGT	75	RXM	Control Rod Guide Tubes	Tube Deformation	3.63	0.28	0.4	1.19	No	DS
CTG---100-SITE--FTR-SEIS	CTG	100	SITE	Combustion Turbine Generator	Fails to Run	0.65	0.17	0.28	0.31	No	Generic
					Fails to Start						
DGN---100-SITE--FTR-SEIS	DGN	100	SITE	Backup Diesel Generators	Fails to Run	0.65	0.17	0.28	0.31	No	Generic
					Fails to Start						
EBA---100-HVSWG-FOP-SEIS	EBA	100	HVSWG	13KV AC Bus	Fails to Operate	5.9	0.24	0.39	2.09	No	Generic

Table 19.1-38: Seismic Correlation Class Information (Continued)

Seismic Correlation Class	Component ID	Elevation (ft)	Location	NuScale Component	Failure Mode Description	A_m (g)	β_r (g)	β_u (g)	HCLPF (g)[1]	Contributes to seismic margin?[2]	Fragility Method[3]
EBA---100-LVPDC-FOP-SEIS	EBA	100	LVPDC	BDG Distribution Bus	Fails to Operate	2.8	0.24	0.39	0.99	No	Generic
EBD---86--RXB---FOP-SEIS	EBD	86	RXB	DC Bus Power Channel	Fails to Operate	3.55	0.24	0.39	1.26	No	Generic
HOV---100-RXM---FTC-SEIS	HOV	100	RXM	CVCS, CES, FWS, MSS Containment Isolation Valves	Fails to Close	22.13	0.27	0.37	7.72	Yes	DS
HOV---100-RXM---FTO-SEIS	HOV	100	RXM	CVCS, CFDS Containment Isolation Valves, DHRS Actuation Valves	Fails to Open	0.57	0.32	0.52	0.14	No	Generic
HOV---50--RXM---FOP-SEIS	HOV	50	RXM	ECCS Reactor Recirculation Valves	Fails to Operate (Passive Actuation)	9.52	0.27	0.37	3.32	Yes	DS
HOV---50--RXM---FTO-SEIS	HOV	50	RXM	ECCS Reactor Recirculation Valves	Fails to Open (Valve Body Deformation)	9.52	0.27	0.37	3.32	Yes	DS
HOV---75--RXM---FOP-SEIS	HOV	75	RXM	ECCS Reactor Vent Valves	Fails to Operate (Passive Actuation)	17.45	0.27	0.37	6.09	Yes	DS
HOV---75--RXM---FTO-SEIS	HOV	75	RXM	ECCS Reactor Vent Valves	Fails to Open (Valve Body Deformation)	17.45	0.27	0.37	6.09	Yes	DS
HTX---50--RXB---HXF-SEIS[4]	HTX	50	RXB	CVCS Heat Exchanger	Heat Exchanger Failure	6.81	0.32	0.51	1.74	No	Generic
HTX---50--RXM---HXF-SEIS	HTX	50	RXM	DHRS Heat Exchangers	Heat Exchanger Failure	2.34	0.32	0.51	0.6	No	Generic
MCC---86--RXB---FOP-SEIS	MCC	86	RXB	Low Voltage Motor Control Center	Fails to Operate	3.55	0.24	0.39	1.26	No	Generic
MDP---100-CHILL-FTR-SEIS	MDP	100	CHILL	DWS Pumps	Fails to Run	4.7	0.27	0.43	1.49	No	Generic
MDP---100-RXB---FTR-SEIS	MDP	100	RXB	CFDS Makeup Pumps	Fails to Run	2.3	0.27	0.43	0.73	No	Generic
MDP---50--RXB---FTR-SEIS	MDP	50	RXB	CVCS Makeup Pumps	Fails to Run	4.05	0.27	0.43	1.28	No	Generic
MOV---100-RXM---FTC-SEIS	MOV	100	RXM	CVCS MOV Recirculation Valve	Fails to Close	0.57	0.32	0.52	0.14	No	Generic
MOV---100-RXM---FTO-SEIS	MOV	100	RXM	CVCS MOV Injection Valve	Fails to Open	0.57	0.32	0.52	0.14	No	Generic
MSW---75--CRB---FTC-SEIS	MSW	75	CRB	Manual Division Actuation Switches	Fails to Close	4.78	0.24	0.39	1.7	No	Generic
RSV---75--RXM---FTC-SEIS[4]	RSV	75	RXM	All Reactor Safety Valves	Fails to Close	3.37	0.24	0.32	1.34	No	DS
					Fails to Remain Closed						
					Fails to Reclose						
					Spuriously Open						
RSV---75--RXM---FTO-SEIS	RSV	75	RXM	All Reactor Safety Valves	Fails to Open	3.37	0.24	0.32	1.34	Yes	DS

Table 19.1-38: Seismic Correlation Class Information (Continued)

Seismic Correlation Class	Component ID	Elevation (ft)	Location	NuScale Component	Failure Mode Description	A_m (g)	β_r (g)	β_u (g)	HCLPF (g)[1]	Contributes to seismic margin?[2]	Fragility Method[3]
RTB---75--RXB---FOP-SEIS	RTB	75	RXB	Reactor Trip Circuit Breaker	Fails to Operate	3.69	0.24	0.39	1.31	No	Generic
SGT---50--RXM---BRK-SEIS[4]	SGT	50	RXM	Steam Generators	Tube/Support Failure	2.53	0.28	0.36	0.88	No	DS
SOV---50--RXM---FTO-SEIS	SOV	50	RXM	ECCS Reactor Recirculation Valve Trip Valve Solenoids	Fails to Open	3.32	0.24	0.41	1.14	No	DS
SOV---75--RXM---FTO-SEIS	SOV	75	RXM	ECCS Reactor Vent Valve Trip Valve Solenoids	Fails to Open	3.23	0.28	0.53	0.85	No	DS
TFM---100-HVSWG-FOP-SEIS	TFM	100	HVSWG	13KV High Voltage Main Power Transformer	Fails to Operate	2.1	0.24	0.39	0.75	No	Generic
TFM---100-LVPDC-FOP-SEIS	TFM	100	LVPDC	Low Voltage Transformer	Fails to Operate	2.1	0.24	0.39	0.75	No	Generic
TFM---100-MVSWG-FOP-SEIS	TFM	100	MVSWG	13KV/4KV Auxiliary Transformer	Fails to Operate	2.1	0.24	0.39	0.75	No	Generic

Notes:

[1] All HCLPF values are determined via 5% failure probability on the 95% probability of exceedance fragility curve (EPRI 103959).

[2] Contribution to the seismic margin is determined via a systematic methodology considering the MIN-MAX HCLPF determination and random CCDP product > 1% criterion described in Table 19.1-40.

[3] The methods used to evaluate component fragilities are identified as either “DS” (design-specific) or “Generic”. Design-specific fragilities include an evaluation of both the equipment capacity and demand relative to a specific structure or piece of equipment. Generic fragilities constitute fragilities determined via a library/database search of similar equipment types. Such generic fragilities are augmented with ISRS information to include ground motion amplification specific to the NPM and the NuScale reactor building. All component failure modes identified as critical have design-specific fragilities.

[4] Three seismically-induced component failure modes are also identified as seismically induced initiating events (HTX---50--RXB---HXF-SEIS, RSV---75--RXM---FTC-SEIS, and SGT---50--RXM---BRK-SEIS). In accident sequences initiated by failure of this equipment, the equipment is not available for mitigation.

Table 19.1-39: Seismic Margin Analysis In-Structure Response Spectra Locations and Demand Response Factors

#	ISRS Node #	Response #	Response Factor	Description
0	0	000	1.00	Generic for site grounds or unknown. Results in ground slab motion.
1	4	001	3.42	CNV X lug
2	7	002	14.61	CNV transition
3	8	003	16.16	CNV head top
4	11	004	3.68	RPV FW plenum access
5	14	005	6.46	RPV top head
6	32	006	4.43	Steam generator top
7	13065	007	1.16	North wall of equipment room between grid lines RX-4 and RX-5 at EL. 50′
8	17207	008	1.60	Mid-span of north slab between grid lines RX-2 and RX-3 at EL. 75′
9	18655	009	1.67	Northwest corner of equipment room between grid lines RX-2 and RX-3 at El. 81′-3″
10	23386	010	2.05	Edge of north slab along grid line RX-4 at EL. 100′
11	35787	011	1.24	MCR between grid lines CB-B and CB-C at El. 76′-6″

Table 19.1-40: Key Assumptions for the Seismic Margin Assessment

Assumption	Basis
Structures are screened out if they are not directly in contact with the NPM and do not have the potential to collapse on top of it.	Engineering judgment
Systems and components are screened if they are not included in the internal events PRA models (full power and low power and shutdown).	Common engineering practice
Seismic sequences are mapped to those in the internal events PRA but augmented with seismically induced SSC initiating events and seismically induced SSC failures.	Common engineering practice and consistent with the ASME/ANS PRA Standard.
Intra-module component groups have 100 percent correlation provided all components share the same elevation class, general component type and same failure mode. Components not meeting these shared criteria are treated as independent.	Common engineering practice, consistent with the ASME/ANS PRA Standard, and bounding assumption.
Different component failure modes (for the same component or different components of the same type) are not modelled as correlated when the specific seismic failure mode is identified, i.e. “seismic failure to open”. When the event is labeled as a functional failure, all failure modes are included and considered correlated.	Common engineering practice, consistent with the ASME/ANS PRA Standard, and bounding assumption.
Seismic component failures are not modelled for fail-safe signal logic, which includes sensors, transmitters, relays, equipment interface modules, safety function modules, actuation priority logic modules, hard-wired modules, scheduling and bypass modules, and scheduling and voting modules. As such, seismically-induced signal logic failures of the MPS are not considered credible.	Common engineering practice
Design-specific fragilities are used for failures that contribute to the seismic margin, including valves located inside the NuScale Power Module and structural events.	Common engineering practice, consistent with the ASME/ANS PRA Standard, and engineering judgment.
For SSC that do not contribute significantly to the seismic margin, design-specific response factors combined with generic capacity values are used.	Engineering judgment and common engineering practice.
Fragility parameters acquired from generic sources, including capacity, randomness, and uncertainty values, are assumed valid and relevant to the NuScale design.	Common engineering practice
Systems are assumed to fail at the ground motion in which they have an 84 percent probability of failure. For ground motions with lower failure probabilities, the success logic is treated as a probability of 1.0.	Simplifying conservative assumption to avoid duplication of success logic in SAPHIRE.
Structural events (e.g., RXB wall), are postulated to directly lead to core damage and large release. The term “structural event” is used in lieu of “structural failure”.	Bounding simplification
Control room failure is not included in the SMA because a control room collapse is bounded by the effects of a LOOP that occurs at lower ground motions with higher frequencies. A LOOP results in ECCS valve actuation; a control room collapse results in a signal loss and subsequent ECCS valve actuation.	Bounding assumption
The controlling failure mode of the RBC, which is designed with seismic restraints, is the yielding of the bridge seismic restraint weldments. The bounding consequence of crane failure during low power operations is a collapse of the crane structure on top of the module, leading to core damage and large release.	Bounding assumption
During low power and shutdown conditions, the state-specific risk to the module is during the transport phase before and after refueling, when the RBC is bearing the load of the module. Other events involving the RBC can be screened because the likelihood of the RBC being over the module (and not bearing the load of the module) is bounded by the full-power assessment.	Engineering judgment

Table 19.1-40: Key Assumptions for the Seismic Margin Assessment (Continued)

Assumption	Basis
Failure of the bridge seismic restraints, rather than the bridge girders, is expected to be the controlling failure mode of the crane bridge.	Engineering judgment
In the MIN-MAX method, cutsets containing both seismic and random failures are screened if the product of all random failure probabilities is below 1E-2 because the HCLPF is defined as a one percent failure probability on the mean fragility curve. Thus, it is reasonable to use this value as a screening criterion for the probability of non-seismic failures in the same cutset.	Common engineering practice and consistent with ISG-020.
In a cutset containing multiple seismic failures, the highest HCLPF value determines the cutset HCLPF.	Common engineering practice, application of the MIN-MAX method.
Because the dominant structural events are assumed to lead core damage and a large release, the plant-level core damage HCLPF is the same as the large release HCLPF.	Bounding assumption
Recovery, including the recovery of offsite power, is not credited in the SMA.	Bounding assumption
Extreme stress was considered for operator actions following a seismic event.	Engineering judgment
Fragilities developed via the separation of variables methodology are assumed to be representative of fragilities determined via qualification testing. The separation of variables methodology is based on the same SSC design information, specifications, and analysis as would be used to develop testing information during procurement.	Engineering judgment
Failure of the CFT does not contribute to the seismic margin because the NPM remains connected to the RBC when in the CFT. In the RFT, the RBC remains connected to the upper CNV and RPV until the upper CNV and upper RPV are removed, after which the lower RPV, which contains the reactor core, remains in the RFT, open to the UHS. Thus, failure of the RFT does not contribute to the seismic margin.	Expected operating practice
The module lifting adapter is modeled as part of the RBC structure, and design safety margins preclude it from being the controlling seismic failure.	Engineering judgment
The control rod guide tubes are assumed to be the controlling seismically induced failure associated with the reactor internals. Therefore, seismically induced damage to reactor internals is not considered in the seismic margin.	Engineering judgment
Seismic Category I structures (i.e., the RXB and the CRB) meet the seismic margin requirement of 1.67 * CSDRS for site-specific seismic hazards (e.g., sliding, overturning).	Engineering judgment

Table 19.1-41: Multiple Spurious Operation (MSO) Summary

Generic MSO ID (NUREG/ CR-6850, App G)	Challenge to Safe Shutdown	Mitigation	Consequence to FPRA
6	Failing to isolate CVCS discharge can result in the potential for RCS inventory to be lost from the RPV.	This failure can be mitigated by assuring that one division of the MPS is capable of isolating the discharge line with the CIVs.	Fire-induced failure of the discharge isolation valves is considered in the model. Spurious operation of valves in the discharge line is not modeled as creating a loss of reactor coolant inventory. In addition to multiple functional failures, including two CIVs, this would require the spurious operation of two valves in the CVCS line in addition to the spurious operation of at least one valve in the liquid radioactive waste management system (LRWMS). These combinations of failures are beyond the scope of the PRA model.
7	A combination of failures can result in a loss of RCS inventory should the CVCS makeup pumps spuriously operate in conjunction with a failure to isolate the CVCS makeup isolation valves. The failure involves overfilling the RPV and subsequently lifting the RSVs. This failure would be compounded by a subsequent failure of the CVCS makeup pumps. Additionally, should makeup continue, the makeup pumps ultimately fill the CNV at a high enough pressure that the CNV may be challenged.	This failure can be mitigated by assuring that one division of the MPS is capable of isolating the CVCS makeup and spray lines with the CIVs.	Spurious operation of the CVCS pumps is considered to the extent that it can challenge RCS integrity by forcing an RSV to open. Continued operation of the CVCS pumps following an induced opening of the RSV would mitigate the event and is accordingly not assumed to be successful. This failure can be mitigated by the successful isolation of the CVCS makeup isolation valves and is considered in the model.
24	Spuriously opening or failing to close the MSIVs and the nonsafety-related backup isolation valves on the main steam lines may result in the loss of inventory in the steam generator and DHRS heat exchangers that results in a failure of the DHRS.	This failure can be mitigated by assuring that one division of the MPS is capable of isolating the MSIVs.	Fire-induced failure to operate of the MSIVs and the nonsafety-related backup isolation valves is considered in the model.
25	Spuriously opening or failing to close the main steam isolation bypass valves and the nonsafety-related backup isolation valves on the main steam lines may result in the loss of inventory in the steam generator DHRS heat exchangers that results in a failure of the DHRS.	This failure can be mitigated by assuring that one division of the MPS is capable of isolating the main steam isolation bypass valves.	Fire-induced spurious operation of the MSIV bypass valves and the nonsafety-related backup isolation valves is considered in the model.

Table 19.1-41: Multiple Spurious Operation (MSO) Summary (Continued)

Generic MSO ID (NUREG/ CR-6850, App G)	**Challenge to Safe Shutdown**	**Mitigation**	**Consequence to FPRA**
30	NuScale does not have an auxiliary FWS; however a failure to isolate the feedwater lines, particularly when coupled with continued operation of the main feedwater pumps can result in overfilling the steam generator and the DHRS heat exchanger. This overflow can result in a failure of the DHRS.	This failure can be mitigated by assuring that one division of the MPS is capable of isolating the FWIVs.	Fire-induced failure to operate of the FWIVs and the feedwater regulating valves are considered in the model.
33a	NuScale has no auxiliary FWS; however a failure to isolate the feedwater lines, particularly when coupled with continued operation of the main feedwater pumps can result in overfilling the steam generator and the DHRS heat exchanger. This overflow can result in a failure of the DHRS.	This failure can be mitigated by assuring that one division of the MPS is capable of isolating the FWIVs.	Fire-induced failure to operate of the FWIVs and the feedwater regulating is considered in the model.
37	Operation of the pressurizer heaters when the heating elements are uncovered can result in a failure of the heating element sheaths. These sheaths constitute a portion of the reactor coolant pressure boundary and their failure can accordingly result in a loss of coolant accident (LOCA) inside containment.	This failure can be mitigated by assuring that one division of the MPS is capable of tripping the pressurizer heater breakers.	Fire-induced failure to trip of the pressurizer heater breakers is considered in the model. When it cannot be ensured that power can be removed from the pressurizer heater breakers, this is modeled as an induced LOCA inside the containment. The pressurizer heater trip breakers are physically located in the MPS equipment room associated with each division of the MPS and their control cabling is expected to be routed with their associated MPS division. Accordingly, fires affecting the pressurizer heaters also capable of inducing spurious ECCS valve operations which result in bounding LOCAs inside the containment. For simplicity, while this failure mode is considered, it is not explicitly modeled.
38	Spurious operation of the CVCS makeup pumps with the pump suction aligned to the DWS can result in the potential for a boron dilution event.	This failure can be mitigated by assuring that one division of the MPS is capable of isolating the CVCS makeup and spray lines with the CIVs.	Spurious operation of the CVCS pumps is considered to the extent that it can challenge RCS integrity by forcing an RSV to open. CVCS makeup with DWS has been demonstrated to successfully mitigate LOCAs, so dilution following the opening of an RSV is not considered separately.

Table 19.1-41: Multiple Spurious Operation (MSO) Summary (Continued)

Generic MSO ID (NUREG/ CR-6850, App G)	**Challenge to Safe Shutdown**	**Mitigation**	**Consequence to FPRA**
49	Spurious operation of the backup diesel generators or the auxiliary AC power source, depending on the specific auxiliary AC power supply utilized for a given application, may lead to non-synchronous paralleling of power supplies. This can result in a failure of the paralleled power supplies and may result in a consequential secondary fire ignition.	This failure can be mitigated by assuring that power supply output breakers and the bus supply breakers on supported buses are protected by appropriate protective devices. This failure cannot, by itself, challenge safe shutdown, but the consequences of the potential secondary fire are evaluated.	This failure mechanism is not explicitly modeled. Details regarding the protective relaying scheme have not been established, however this protection is typically provided at a location local to the switchgear. Locating these protective devices in the area of the switchgear and the generators themselves preclude a fire from being able to connect out of phase power supplies to a single bus. These protective relaying schemes can also prevent motoring of the generators.
49.2	Non-synchronous paralleling of the main turbine generator to an otherwise energized bus, similar to MSO 49 can result in the possibility of a secondary fire developing. Additionally, spurious closure to the main generator output breaker when the steam supply to the turbine has been isolated may result in motoring the main generator. This may also result in a consequential secondary fire developing.	This failure can be mitigated by assuring that power supply output breakers and the bus supply breakers on supported buses are protected by appropriate protective devices. This failure cannot, by itself, challenge safe shutdown, but the consequences of the potential secondary fire are evaluated.	This failure mechanism is not explicitly modeled. Details regarding the protective relaying scheme have not been established, however this protection is typically provided at a location local to the switchgear. Locating these protective devices in the area of the switchgear and the generators themselves preclude a fire from being able to connect out of phase power supplies to a single bus. These protective relaying schemes can also prevent motoring of the generators.
56	Spurious operation, provided the operation goes to completion, of any engineered safety feature is not a failure that can challenge safe shutdown. However, fire-induced failures of subsets of the equipment associated with DHRS or ECCS actuations can challenge safe shutdown. Such failures of the DHRS are completely addressed in MSOs 24, 25, 30, and 33a. Fire-induced failures of the ECCS valves such that only the RVVs or only the RRVs open can essentially induce a LOCA inside the containment which challenges safe shutdown.	This failure can be mitigated by assuring that at least two RVVs and one RRV remain free of fire damage.	Fire-induced failures of DHRS and ECCS are included in the model.

Table 19.1-42: Applicability of Internal Initiating Events to Fire Probabilistic Risk Assessment

Initiating Event	Applicability to Fire PRA	Basis
CVCS Charging Line LOCA Inside Containment (IE-CVCS--ALOCA-CIC)	No	A fire does not induce a pipe or vessel leak or break.
CVCS Charging Line Break Outside Containment (IE-CVCS--ALOCA-COC)	No	A fire does not induce a pipe or vessel leak or break.
CVCS Letdown Line LOCA Outside Containment (IE-CVCS--ALOCA-LOC)	No	A fire is not expected to induce a pipe or vessel leak or break.
Spurious Opening of an ECCS Valve (IE-ECCS--ALOCA-RV1)	Yes	A fire can spuriously operate an ECCS valve. This failure may occur after successfully depressurizing the RCS such that the inadvertent actuation block (IAB) is not capable of preventing actuation.
Loss of DC Power (IE-EDSS--LODC-----)	Yes	A fire can damage electrical distribution equipment.
Loss of Offsite Power (IE-EHVS--LOOP-----)	Yes	A fire can damage electrical distribution equipment.
SGTF (IE-MSS---ALOCA-SG-)	No	A fire is not expected to induce a pipe or vessel leak or break.
LOCA Inside Containment (IE-RCS---ALOCA-IC-)	Yes	Spurious operation of the chemical and volume control system (CVCS) makeup pumps may result in an RCS overpressurization event such that the reactor safety valve(s) (RSVs) are opened. This also requires a failure of the CVCS makeup isolation valves which receive signals to close.
Secondary Side Line Break (IE-TGS---FMSLB-UD-)	No	A fire does not induce a pipe or vessel leak or break.
General Reactor Trip (IE-TGS---TRAN-NPC)	Yes	A fire can result in various failures that manifest as a general reactor trip. For example, a fire may result in the spurious closure of both main steam isolation valves (MSIVs).
Loss of Support System IE-TGS---TRAN-NSS)	Yes	A fire can result in various failures that manifest as a loss of a support system. For example, a fire may result in a ground fault to the electrical supply to an AC bus.

Table 19.1-43: Ignition Source Frequencies

Bin (NUREG-2169)	Ignition Source	Total	Mean Frequency (/yr) (NUREG-2169)
Fixed Ignition Source			
1	Batteries	106	1.96E-04
4	Main control board	1	4.91E-03
8	Diesel generators (includes auxiliary AC power source as "third" DG)	3	7.81E-03
9	Air compressors	2	4.69E-03
10	Battery chargers	107	1.12E-03
14	Electric motors	34	5.43E-03
15	Electrical cabinets (non-HEAF)	947	3.00E-02
16.a	HEAF for low- voltage electrical cabinets (480-1000 V)	145	1.52E-04
16.b	HEAF for medium-voltage electrical cabinets (>1000 V)	34	2.13E-03
17	Hydrogen tanks	12	4.93E-03
19	Miscellaneous hydrogen fires	12	4.82E-03
21	Pumps	185	2.72E-02
23	Transformers	71	9.56E-03
26	Ventilation subsystems	72	1.64E-02
27	Transformer - Catastrophic	11	6.61E-03
28	Transformer - Non Catastrophic	11	6.53E-03
29	Yard transformers (others)	11	3.69E-03
32	Main feedwater pumps	36	4.38E-03
33	T/G exciter	12	8.36E-04
34	T/G hydrogen	12	4.12E-03
35	T/G oil	12	5.49E-03
Transient Ignition Source			
5	Cable fires caused by welding and cutting (Control/Aux/Reactor Building)	N/A	7.83E-04
6	Transient fires caused by welding and cutting	N/A	4.44E-03
7	Transients	N/A	3.33E-03
11	Cable fires caused by welding and cutting (Plant-Wide Components)	N/A	2.77E-04
24	Transient fires caused by welding and cutting (Plant-Wide Components)	N/A	4.79E-03
25	Transients (Plant-Wide Components)	N/A	8.54E-03
31	Cable fires caused by welding and cutting (Turbine Building)	N/A	3.47E-04
36	Transient fires caused by welding and cutting (Turbine Building)	N/A	4.67E-03
37	Transients (Turbine Building)	N/A	6.71E-03

Table 19.1-44: Fire-Induced Initiating Events

Fire Initiating Event	Description	Compartment[2]	Potential Transfers to Internal Event Trees	Mean Fire IE Frequency (per mcyr)[1]
IE-FIRE-1-LOCA	Fire Spuriously Operates CVCS Makeup Pump	010-114, 010-115, 010-116, 010-117, 010-118, 010-119, 010-120, 010-139	TGS-TRAN-NPC CVCS-ALOCA-CIC	1.2E-01
IE-FIRE-2-LOOP	Fire Causes Loss of Offsite Power	Yard and power distribution areas	TGS-TRAN-NPC EHVS--LOOP	1.3E-01
IE-FIRE-3-ECCS	Fire Induces Spurious ECCS Actuation - Division I and II Affected	010-208, 010-242, 010-275, 170-100, 170-102	TGS-TRAN-NPC ECCS-ALOCA-RV1	9.8E-02
IE-FIRE-4-ECCS	Fire Induces Spurious ECCS Actuation - Division I Affected	170-002, 170-004, 170-021, 010-211, 010-211-01	TGS-TRAN-NPC ECCS-ALOCA-RV1	1.0E-03
IE-FIRE-5-ECCS	Fire Induces Spurious ECCS Actuation - Division II Affected	170-003, 170-005, 170-017, 010-282, 010-282-02	TGS-TRAN-NPC ECCS-ALOCA-RV1	1.0E-03
IE-FIRE-6-TRANSIENT	Fire Induces Transient - No Fire Damage to FPRA Equipment	All other compartments	TGS-TRAN-NPC	8.0E-01
IE-FIRE-7-TRANSIENT	Fire Induces Transient - CFDS Failed	010-409	TGS-TRAN-NPC	1.5E-02
IE-FIRE-8-TRANSIENT	Fire Induces Transient - Steam Gallery	010-411	TGS-TRAN-NPC	1.2E-02
IE-FIRE-9-TRANSIENT	Fire Induces Transient - CRDS Gallery	010-507, 010-601	TGS-TRAN-NPC	2.2E-02
IE-FIRE-10-TRANSIENT	Fire Induces Transient - EDSS Battery Area - Power Channel A and C	010-209, 010-210	TGS-TRAN-NPC	2.0E-04
IE-FIRE-11-TRANSIENT	Fire Induces Transient - EDSS Switchgear - Power Channel C	010-280	TGS-TRAN-NPC	1.3E-04
IE-FIRE-12-TRANSIENT	Fire Induces Transient - EDSS Switchgear - Power Channel A	010-281	TGS-TRAN-NPC	1.3E-04
IE-FIRE-13-TRANSIENT	Fire Induces Transient - EDSS Battery Area - Power Channel B and D	010-212, 010-213	TGS-TRAN-NPC	2.0E-04
IE-FIRE-14-TRANSIENT	Fire Induces Transient - EDSS Switchgear - Power Channel B	010-283	TGS-TRAN-NPC	1.2E-04

Table 19.1-44: Fire-Induced Initiating Events (Continued)

Fire Initiating Event	Description	Compartment[2]	Potential Transfers to Internal Event Trees	Mean Fire IE Frequency (per mcyr)[1]
IE-FIRE-15-TRANSIENT	Fire Induces Transient - EDSS Switchgear - Power Channel D	010-284	TGS-TRAN-NPC	1.2E-04
IE-FIRE-16-LOCA	Multi-Compartment Scenario - Spread Leads to Spuriously Operated CVCS Makeup Pump	010-016 to 010-114, 010-115, 010-116, 010-117, 010-118, 010-119, 010-120, 010-139, 010-026 to 010-114, 010-115, 010-116, 010-117, 010-118, 010-119, 010-120, 010-139, 010-027 to 010-114, 010-115, 010-116, 010-117, 010-118, 010-119, 010-120, 010-139,010-028 to 010-114, 010-115, 010-116, 010-117, 010-118, 010-119, 010-120, 010-139, 010-029 to 010-114, 010-115, 010-116, 010-117, 010-118, 010-119, 010-120, 010-139, 010-030 to 010-114, 010-115, 010-116, 010-117, 010-118, 010-119, 010-120, 010-139, 010-031 to 010-114, 010-115, 010-116, 010-117, 010-118, 010-119, 010-120, 010-139, 010-107, 010-138 to 010-114, 010-115, 010-116, 010-117, 010-118, 010-119, 010-120, 010-139, 010-112 to 010-114, 010-115, 010-116, 010-117, 010-118, 010-119, 010-120, 010-139, 010-122 to 010-114, 010-115, 010-116, 010-117, 010-118, 010-119, 010-120, 010-139	TGS-TRAN-NPC CVCS-ALOCA-CIC	2.4E-05
IE-FIRE-17-ECCS	Multi-Compartment Scenario - Spread Leads Induces ECCS Actuation - CVCS Failed	010-114, 010-115, 010-116, 010-117, 010-118, 010-119, 010-120, 010-139 to 010-208, 010-242, 010-275	TGS-TRAN-NPC ECCS-ALOCA-RV1	1.2E-04

Table 19.1-44: Fire-Induced Initiating Events (Continued)

Fire Initiating Event	Description	Compartment[2]	Potential Transfers to Internal Event Trees	Mean Fire IE Frequency (per mcyr)[1]
IE-FIRE-18-ECCS	Multi-Compartment Scenario - Fire Spreads Results in Spurious ECCS Actuation - Division I and II Affected	010-206 to 010-208, 010-242, 010-275, 010-207 to 010-208, 010-242, 010-275, 010-208, 010-242, 010-275 to 010-209, 010-208, 010-242, 010-275 to 010-210, 010-208, 010-242, 010-275 to 010-212, 010-208, 010-242, 010-275 to 010-213, 010-208, 010-242, 010-275 to 010-280, 010-208, 010-242, 010-275 to 010-281, 010-208, 010-242, 010-275 to 010-284, 010-210 to 010-208, 010-242, 010-275, 010-211 to 010-208, 010-242, 010-275, 010-211 to 010-282, 010-213 to 010-208, 010-242, 010-275, 010-214 to 010-208, 010-242, 010-275, 010-216 to 010-208, 010-242, 010-275, 010-217 to 010-208, 010-242, 010-275, 010-221 to 010-208, 010-242, 010-275, 010-222 to 010-208, 010-242, 010-275, 010-224 to 010-208, 010-242, 010-275, 010-225 to 010-208, 010-242, 010-275, 010-227 to 010-208, 010-242, 010-275, 010-229 to 010-208, 010-242, 010-275, 010-230 to 010-208, 010-242, 010-275, 010-232 to 010-208, 010-242, 010-275, 010-234 to 010-208, 010-242, 010-275, 010-235 to 010-208, 010-242, 010-275, 010-237 to 010-208, 010-242, 010-275, 010-239 to 010-208, 010-242, 010-275, 010-244 to 010-208, 010-242, 010-275, 010-246 to 010-208, 010-242, 010-275, 010-248 to 010-208, 010-242, 010-275, 010-249 to 010-208, 010-242, 010-275, 010-251 to 010-208, 010-242, 010-275, 010-252 to 010-208, 010-242, 010-275, 010-255 to 010-208, 010-242, 010-275, 010-256 to 010-208, 010-242, 010-275, 010-258 to 010-208, 010-242, 010-275, 010-259 to 010-208, 010-242, 010-275, 010-261 to 010-208, 010-242, 010-275, 010-263 to 010-208, 010-242, 010-275,010-265 to 010-208, 010-242, 010-275, 010-267 to 010-208, 010-242, 010-275, 010-268 to 010-208, 010-242, 010-275, 010-271 to 010-208, 010-242, 010-275, 010-272 to 010-208, 010-242, 010-275, 010-274 to 010-208, 010-242, 010-275, 010-281 to 010-208, 010-242, 010-275, 010-282 to 010-208, 010-242, 010-275, 010-284 to 010-208, 010-242, 010-275, 010-285 to 010-208, 010-242, 010-275, 010-287 to 010-208, 010-242, 010-275, 010-289 to 010-208, 010-242, 010-275, 010-292 to 010-208, 010-242, 010-275, 010-293 to 010-208, 010-242, 010-275, 010-295 to 010-208, 010-242, 010-275, 010-298 to 010-208, 010-242, 010-275, 010-299 to 010-208, 010-242, 010-275, 010-301 to 010-208, 010-242, 010-275, 010-302 to 010-208, 010-242, 010-275, 010-304 to 010-208, 010-242, 010-275, 010-306 to 010-208, 010-242, 010-275, 010-307 to 010-208, 010-242, 010-275, 010-309 to 010-208, 010-242, 010-275, 010-311 to 010-208, 010-242, 010-275, 010-312 to 010-208, 010-242, 010-275, 010-314 to 010-208, 010-242, 010-275, 010-315 to 010-208, 010-242, 010-275, 010-318 to 010-208, 010-242, 010-275, 010-319 to 010-208, 010-242, 010-275, 010-320 to 010-208, 010-242, 010-275, 010-322 to 010-208, 010-242, 010-275, 010-324 to 010-208, 010-242, 010-275, 010-325 to 010-208,	TGS-TRAN-NPC ECCS-ALOCA-RV1	2.6E-04

Table 19.1-44: Fire-Induced Initiating Events (Continued)

Fire Initiating Event	Description	Compartment[2]	Potential Transfers to Internal Event Trees	Mean Fire IE Frequency (per mcyr)[1]
		010-242, 010-275, 010-328 to 010-208, 010-242, 010-275, 010-329 to 010-208, 010-242, 010-275, 010-331 to 010-208, 010-242, 010-275, 010-333 to 010-208, 010-242, 010-275, 010-335 to 010-208, 010-242, 010-275, 010-336 to 010-208, 010-242, 010-275, 010-339 to 010-208, 010-242, 010-275, 010-340 to 010-208, 010-242, 010-275, 010-342 to 010-208, 010-242, 010-275,170-002, 170-004 to 170-003, 170-005, 170-002, 170-004 to 170-003, 170-005, 170-003, 170-005 to 170-002, 170-004, 170-003, 170-005 to 170-002, 170-004, 170-017 to 170-100, 170-102, 170-021 to 170-100, 170-102		
IE-FIRE-19-ECCS	Multi-Compartment Scenario - Fire Spreads Results in Spurious ECCS Actuation - Division I Affected	170-001 to 170-021, 010-209 to 010-211, 010-210 to 010-211, 010-212 to 010-211, 010-213 to 010-211, 010-211 to 010-209, 010-211 to 010-210, 010-211 to 010-212, 010-211 to 010-213	TGS-TRAN-NPC ECCS-ALOCA-RV1	3.8E-06
IE-FIRE-20-ECCS	Multi-Compartment Scenario - Fire Spreads Results in Spurious ECCS Actuation - Division II Affected	010-280 to 010-282, 010-281 to 010-282, 010-283 to 010-282, 010-284 to 010-282,170-001 to 170-017, 170-007 to 170-017, 170-008 to 170-017, 170-009 to 170-017, 170-010 to 170-017, 170-011 to 170-017, 170-012 to 170-017, 170-013 to 170-017, 170-015 to 170-017, 170-016 to 170-017, 170-017 to 010-280, 170-017 to 010-281, 170-017 to 010-283, 170-017 to 010-284	TGS-TRAN-NPC ECCS-ALOCA-RV1	1.7E-05
IE-FIRE-21-ECCS	Multi-Compartment Scenario - Fire Spreads Results in Spurious ECCS Actuation - CFDS Failed	010-208, 010-242, 010-275 to 010-409	TGS-TRAN-NPC ECCS-ALOCA-RV1	3.3E-05
IE-FIRE-22-TRANSIENT	Multi-Compartment Scenario - Fire Spreads Results in Transient - CFDS Failed	010-280 to 010-409, 010-281 to 010-409, 010-282 to 010-409, 010-283 to 010-409, 010-284 to 010-409, 010-285 to 010-409, 010-286 to 010-409, 010-287 to 010-409. 010-288 to 010-409, 010-289 to 010-409, 010-290 to 010-409, 010-022, 010-023, 010-024, 010-422, 010-423 to 010-409	TGS-TRAN-NPC	1.4E-05
IE-FIRE-23-TRANSIENT	Multi-Compartment Scenario - Fire Spreads Results in Transient - CFDS and Division I ESFAS Failed	010-411 to 010-409, 010-409 to 010-411	TGS-TRAN-NPC	2.7E-05

Table 19.1-44: Fire-Induced Initiating Events (Continued)

Fire Initiating Event	Description	Compartment[2]	Potential Transfers to Internal Event Trees	Mean Fire IE Frequency (per mcyr)[1]
IE-FIRE-24-TRANSIENT	Multi-Compartment Scenario - Fire Spreads Results in Transient - Division I ESFAS Failed	010-291 to 010-411, 010-292 to 010-411, 010-293 to 010-411, 010-295 to 010-411, 010-296 to 010-411, 010-297 to 010-411, 010-298 to 010-411, 010-299 to 010-411, 010-300 to 010-411, 010-301 to 010-411, 010-302 to 010-411, 010-303 to 010-411, 010-304 to 010-411, 010-305 to 010-411, 010-306 to 010-411, 010-307 to 010-411, 010-308 to 010-411, 010-309 to 010-411, 010-310 to 010-411, 010-311 to 010-411, 010-410 to 010-411, 010-412 to 010-411, 010-414 to 010-411	TGS-TRAN-NPC	1.2E-05
IE-FIRE-25-ECCS	Multi-Compartment Scenario - Fire Spreads Results in Spurious ECCS Actuation - Division I ESFAS Failed	010-208, 010-242, 010-275 to 010-411	TGS-TRAN-NPC ECCS-ALOCA-RV1	3.3E-05
IE-FIRE-26-TRANSIENT	Multi-Compartment Scenario - Fire Spreads Results in Transient - Division II ESFAS Failed	010-506 to 010-507, 010-601, 010-508 to 010-507, 010-601	TGS-TRAN-NPC	1.1E-05
IE-FIRE-27-TRANSIENT	Multi-Compartment Scenario - Fire Spreads Results in Transient - Division I and II ESFAS Failed	010-411 to 010-507, 010-601	TGS-TRAN-NPC	1.2E-06
IE-FIRE-28-TRANSIENT	Multi-Compartment Scenario - Fire Spreads Results in Transient - CFDS and Division II ESFAS Failed	010-409 to 010-507, 010-601	TGS-TRAN-NPC	1.5E-05
IE-FIRE-29-TRANSIENT	Multi-Compartment Scenario - Fire Spreads Results in Transient - CVCS and CFDS Failed	010-014 to 010-209, 010-014 to 010-210, 010-014 to 010-212, 010-014 to 010-213, 010-209 to 010-280, 010-209 to 010-210, 010-210 to 010-281, 010-210 to 010-209, 010-212 to 010-284, 010-212 to 010-213, 010-213 to 010-283, 010-213 to 010-212, 010-280 to 010-281, 010-281 to 010-280, 010-283 to 010-284, 010-284 to 010-283	TGS-TRAN-NPC	6.1E-05

Notes:

1. Fire frequencies account for number of modules expected to be affected by a fire in a given area. as described in Section 19.1.5.2.1.
2. Room codes used to identify fire compartments are consistent with fire area definitions as presented in Appendix 9A.

Table 19.1-45: Significant Cutsets (Internal Fires, Full Power, Single Module)

Cutset	Prob/Freq	Contribution	Basic Event	Description
CDF Cutsets				
1	5.53E-11	6.7%		
	1.20E-1		IE-FIRE-1-LOCA	Fire Spuriously Operates CVCS Makeup Pump
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	7.32E-4		RCS---RSV-0003A-FTC-S	RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
2	3.80E-11	4.6%		
	9.80E-2		IE-FIRE-3-ECCS	Fire Induces Spurious ECCS Actuation - Division I and II Affected
	1.00E+0		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	7.70E-2		ECCS--SOV-0101B-SHS-N	SOV 0101B ECCS RVV TRIP VALVE FAILS DUE TO HOT SHORT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
3	3.80E-11	4.6%		
	9.80E-2		IE-FIRE-3-ECCS	Fire Induces Spurious ECCS Actuation - Division I and II Affected
	1.00E+0		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	7.70E-2		ECCS--SOV-0101A-SHS-N	SOV 0101A ECCS RVV TRIP VALVE FAILS DUE TO HOT SHORT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
4	2.81E-11	3.4%		
	1.20E-6		IE-FIRE-27-TRANSIENT	Multi-Compartment Scenario - Fire Spreads Results in Transient - Division I and II ESFAS Failed
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
5	2.73E-11	3.3%		
	1.20E-1		IE-FIRE-1-LOCA	Fire Spuriously Operates CVCS Makeup Pump
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	7.32E-4		RCS---RSV-0003A-FTC-S	RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
6	2.52E-11	3.1%		

Table 19.1-45: Significant Cutsets (Internal Fires, Full Power, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	2.60E-4		IE-FIRE-18-ECCS	Multi-Compartment Scenario - Fire Spreads Results in Spurious ECCS Actuation - Division I and II Affected
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	7.70E-2		ECCS--SOV-0101A-SHS-N	SOV 0101A ECCS RVV TRIP VALVE FAILS DUE TO HOT SHORT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
7	1.88E-11	2.3%		
	9.80E-2		IE-FIRE-3-ECCS	Fire Induces Spurious ECCS Actuation - Division I and II Affected
	1.00E+0		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	7.70E-2		ECCS--SOV-0101B-SHS-N	SOV 0101B ECCS RVV TRIP VALVE FAILS DUE TO HOT SHORT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
8	1.88E-11	2.3%		
	9.80E-2		IE-FIRE-3-ECCS	Fire Induces Spurious ECCS Actuation - Division I and II Affected
	1.00E+0		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	7.70E-2		ECCS--SOV-0101A-SHS-N	SOV 0101A ECCS RVV TRIP VALVE FAILS DUE TO HOT SHORT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	4.00E-3		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
9	1.84E-11	2.2%		
	1.20E-1		IE-FIRE-1-LOCA	Fire Spuriously Operates CVCS Makeup Pump
	6.55E-6		CRDS--ROD-1CC316FOP-S	GIVEN ACTUATION, AT LEAST 3 OF 16 RODS FAIL TO INSERT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
10	1.77E-11	2.2%		
	2.20E-2		IE-FIRE-9-TRANSIENT	Fire Induces Transient - CRDS Gallery
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	3.45E-5		MPS---SVM-1CC23-FOP-S	CCF OF 2 OF 3 DIVISION I ESFAS SCHEDULING AND VOTING MODULES
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
11	1.44E-11	1.8%		
	1.20E-2		IE-FIRE-8-TRANSIENT	Fire Induces Transient - Steam Gallery
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	5.14E-5		MSS---HOV-1CC22-FTC-S	CCF OF 2 OF 2 CNTS MSS CONTAINMENT ISOLATION VALVES FAIL TO CLOSE

Table 19.1-45: Significant Cutsets (Internal Fires, Full Power, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
12	1.44E-11	1.8%		
	1.20E-2		IE-FIRE-8-TRANSIENT	Fire Induces Transient - Steam Gallery
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	5.14E-5		FWS---HOV-1CC22-FTC-S	CCF OF 2 OF 2 CNTS FWS CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
13	1.24E-11	1.5%		
	2.60E-4		IE-FIRE-18-ECCS	Multi-Compartment Scenario - Fire Spreads Results in Spurious ECCS Actuation - Division I and II Affected
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	7.70E-2		ECCS--SOV-0101A-SHS-N	SOV 0101A ECCS RVV TRIP VALVE FAILS DUE TO HOT SHORT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
14	1.16E-11	1.4%		
	1.20E-4		IE-FIRE-17-ECCS	Multi-Compartment Scenario - Spread Leads Induces ECCS Actuation - CVCS Failed
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	7.70E-2		ECCS--SOV-0101A-SHS-N	SOV 0101A ECCS RVV TRIP VALVE FAILS DUE TO HOT SHORT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
15	1.16E-11	1.4%		
	1.20E-4		IE-FIRE-17-ECCS	Multi-Compartment Scenario - Spread Leads Induces ECCS Actuation - CVCS Failed
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	7.70E-2		ECCS--SOV-0101B-SHS-N	SOV 0101B ECCS RVV TRIP VALVE FAILS DUE TO HOT SHORT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
16	1.01E-11	1.2%		
	2.20E-2		IE-FIRE-9-TRANSIENT	Fire Induces Transient - CRDS Gallery
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	7.32E-4		RCS---RSV-0003A-FTC-S	RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
17	9.68E-12	1.2%		
	1.20E-2		IE-FIRE-8-TRANSIENT	Fire Induces Transient - Steam Gallery
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	3.45E-5		MPS---SVM-3CC23-FOP-S	CCF OF 2 OF 3 DIVISION II ESFAS SCHEDULING AND VOTING MODULES
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN

Table 19.1-45: Significant Cutsets (Internal Fires, Full Power, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
18	9.14E-12	1.1%		
	1.20E-1		IE-FIRE-1-LOCA	Fire Spuriously Operates CVCS Makeup Pump
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	3.26E-6		MPS---APL-6CC22-FOP-S	CCF OF 2 OF 2 APL MODULES IN TOP BRANCH REACTOR TRIP BREAKERS
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
19	9.14E-12	1.1%		
	1.20E-1		IE-FIRE-1-LOCA	Fire Spuriously Operates CVCS Makeup Pump
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	3.26E-6		MPS---APL-7CC22-FOP-S	CCF OF 2 OF 2 APL MODULES IN BOTTOM BRANCH REACTOR TRIP BREAKERS
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
20	9.04E-12	1.1%		
	9.80E-2		IE-FIRE-3-ECCS	Fire Induces Spurious ECCS Actuation - Division I and II Affected
	9.51E-4		CVCS--AOV-0091X-FTO-N	AOV 0091X CVCS MAKEUP COMBINING VALVE FAILS TO OPEN
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	7.70E-2		ECCS--SOV-0101B-SHS-N	SOV 0101B ECCS RVV TRIP VALVE FAILS DUE TO HOT SHORT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
21	9.04E-12	1.1%		
	9.80E-2		IE-FIRE-3-ECCS	Fire Induces Spurious ECCS Actuation - Division I and II Affected
	9.51E-4		CVCS--AOV-0091X-FTO-N	AOV 0091X CVCS MAKEUP COMBINING VALVE FAILS TO OPEN
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	7.70E-2		ECCS--SOV-0101A-SHS-N	SOV 0101A ECCS RVV TRIP VALVE FAILS DUE TO HOT SHORT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
22	9.04E-12	1.1%		
	9.80E-2		IE-FIRE-3-ECCS	Fire Induces Spurious ECCS Actuation - Division I and II Affected
	9.51E-4		DWS-00AOV-0033X-FTO-N	AOV 0033X DWS NORTH REACTOR BUILDING CVCS PUMP ISOLATION VALVE FAILS TO OPEN
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	7.70E-2		ECCS--SOV-0101B-SHS-N	SOV 0101B ECCS RVV TRIP VALVE FAILS DUE TO HOT SHORT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
23	9.04E-12	1.1%		
	9.80E-2		IE-FIRE-3-ECCS	Fire Induces Spurious ECCS Actuation - Division I and II Affected
	9.51E-4		DWS-00AOV-0033X-FTO-N	AOV 0033X DWS NORTH REACTOR BUILDING CVCS PUMP ISOLATION VALVE FAILS TO OPEN
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN

Table 19.1-45: Significant Cutsets (Internal Fires, Full Power, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	7.70E-2		ECCS--SOV-0101A-SHS-N	SOV 0101A ECCS RVV TRIP VALVE FAILS DUE TO HOT SHORT
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
LRF Cutsets				
1	2.81E-11	64.6%		
	1.20E-6		IE-FIRE-27-TRANSIENT	Multi-Compartment Scenario - Fire Spreads Results in Transient - Division I and II ESFAS Failed
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
2	7.78E-12	17.9%		
	1.20E-1		IE-FIRE-1-LOCA	Fire Spuriously Operates CVCS Makeup Pump
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
3	3.83E-12	8.8%		
	1.20E-1		IE-FIRE-1-LOCA	Fire Spuriously Operates CVCS Makeup Pump
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
4	5.03E-13	1.2%		
	1.20E-1		IE-FIRE-1-LOCA	Fire Spuriously Operates CVCS Makeup Pump
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-1		ECCS--HOV-0002A-FOP-N	HOV 0002A ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.00E-1		ECCS--HOV-0002B-FOP-N	HOV 0002B ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.63E-5		ECCS--SOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS RRV TRIP VALVES FAIL TO OPEN
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL

Table 19.1-45: Significant Cutsets (Internal Fires, Full Power, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
5	4.93E-13	1.1%		
	1.20E-1		IE-FIRE-1-LOCA	Fire Spuriously Operates CVCS Makeup Pump
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	5.00E-1		FIRE-GROWTH1-N	FIRE GROWTH - GENERAL
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	3.26E-6		MPS---APL-5CC22-FOP-S	CCF OF 2 OF 2 APL MODULES IN CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES

Table 19.1-46: Key Assumptions for the Internal Fire PRA

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. Spurious operation probabilities are influenced by assumed control circuit configurations.	Engineering judgment
Separation of redundant safe shutdown equipment and cabling is achieved.	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
Fires igniting under the bioshield and challenging plant equipment are not credible because cable is routed in conduit or is three-hour rated. (FSAR 9A.6.4.3)	Engineering judgment

Table 19.1-46: Key Assumptions for the Internal Fire PRA (Continued)

Assumption	Basis
Instrumentation required for the performance of an operator action is affected by the same fire events that affect equipment required to perform the action (e.g., pumps, valves)	Engineering judgment
The reactor building crane cannot be spuriously operated as a result of a fire.	Engineering judgment

Table 19.1-47: Buildings and Areas Included in Internal Flooding Probabilistic Risk Assessment Model

Building/Area	Contains Flood Sources	Potential for Plant Trip	Contains Mitigating Equipment
Reactor Building	Yes	Yes	Yes
Radioactive Waste Building	Yes	Yes	No
North Turbine Generator Building	Yes	Yes	No
South Turbine Generator Building	Yes	Yes	No
North Plant Cooling Towers and Pumps	Yes	Yes	No
South Plant Cooling Towers and Pumps	Yes	Yes	No
Site Cooling Water Towers and Pumps	Yes	Yes	No
Central Utilities Building	Yes	Yes	No
Utility Water Storage Tank	Yes	Yes	No
Utility Water Storage Tank Pumps	Yes	Yes	No
Lube Oil Storage Tanks (Clean & Dirty) (for TGB)	Yes	Yes	No
Chemical Storage Tanks (for TGB)	Yes	Yes	No
Condensate Storage Tanks (for TGB)	Yes	Yes	No
Reverse Osmosis Skid Equipment Area (DWS)	Yes	Yes	No
Chiller Room (Chilled Water System)	Yes	Yes	No
Compressor Room (SA, 1A Sys)	Yes	Yes	No

Table 19.1-48: Internal Flooding Sources

System	Flooding Potential	Location
Chemical and Volume Control System	Minimal. This system does not move large volumes of water. Breaks in piping result are considered in the internal events model.	RXB
Boron Addition System	Minimal. This system does not move large volumes of water.	RXB
Module Heatup System	Minimal. This system does not move large volumes of water.	RXB
Decay Heat Removal System	Minimal. This system involves a limited inventory, the bulk of which is contained within its heat exchangers and the steam generators.	RXB
Containment Evacuation System	Minimal. During operation, this system primarily contains gases from the CNV and is judged not to have a large fluid inventory.	RXB
Containment Flooding and Drain System	Moderate potential for flooding. Although not normally in operation, this system draws suction from the UHS which contains significant water volume.	RXB
Reactor Component Cooling Water System	Minimal. This system's limited inventory may result in flooding in a small area, but it is not capable of causing widespread flooding.	RXB
Process Sampling System	Minimal. Process sampling lines are small.	RXB, TGB
Liquid Radioactive Waste Management System	Minimal. Flooding may originate from storage tanks. Small, localized flooding events may originate from breaks in other system piping.	RXB, RWB
Radioactive Waste Drain System	Minimal. This system does not normally have a fluid inventory.	RXB, RWB
Spent Fuel Pool Cooling System	Significant. This system is normally in operation and draws suction from the UHS.	RXB
Pool Cleanup System	Minimal. The majority of the piping that supports this system is associated with other systems.	RXB
Reactor Pool Cooling System	Significant. This system is normally in operation and draws suction from the UHS.	RXB
Pool Surge Control System	Minimal. This system is not normally in operation.	RXB, Yard Area
Ultimate Heat Sink	Significant. This system contains a large flooding inventory.	RXB
Pool Leakage Detection Systems	Minimal. Although this system is connected to the UHS the flow into this system is limited to leakage.	RXB
Main Steam System	Moderate. Flooding from this system could primarily occur in the form of condensation.	RXB, TGB
Condensate and Feedwater System	Significant. Although breaks in this system are intended to be isolated quickly, unisolated breaks may result in substantial flooding.	RXB, TGB
Feedwater Treatment	Minimal. The majority of the piping that supports this system is associated with other systems.	TGB
Condensate Polisher Resin Regeneration System	Minimal. The majority of the piping that supports this system is associated with other systems.	TGB
Heater Vents and Drains	Minimal. The majority of the piping that supports this system is associated with other systems.	TGB
Chilled Water System	Significant. This system moves substantial volumes of water.	RXB, RWB, CRB
Auxiliary Boiler System	Minimal. The majority of the piping that supports this system is associated with other systems.	TGB
Turbine-Generator System	Minimal. The majority of the piping that supports this system is associated with other systems.	TGB
Circulating Water System	Significant. This system moves substantial volumes of water.	TGB

Table 19.1-48: Internal Flooding Sources (Continued)

System	Flooding Potential	Location
Site Cooling Water System	Significant. This system moves substantial volumes of water.	TGB
Potable Water System	Minimal. This system does not move large volumes of water.	CRB
Utility Water System	Significant. This system moves substantial volumes of water.	RXB, RWB, CRB, Annex Building
Demineralized Water System	Significant. This system moves substantial volumes of water.	RXB
Turbine Building HVAC System	Minimal. It is assumed that the only flooding mechanism applicable to this system is through the cooling coils, which is judged to be minimal.	TGB
Security Building HVAC	Minimal. It is assumed that the only flooding mechanism applicable to this system is through the cooling coils, which is judged to be minimal.	Security Building
Diesel Generator Building HVAC	Minimal. It is assumed that the only flooding mechanism applicable to this system is through the cooling coils, which is judged to be minimal.	Diesel Generator Building
Annex Building HVAC	Minimal. It is assumed that the only flooding mechanism applicable to this system is through the cooling coils, which is judged to be minimal.	Annex Building
Fire Protection System	Significant. This system moves substantial volumes of water.	RXB, RWB, CRB

Table 19.1-49: Assessment of Flood Areas Containing Equipment Modeled in the Probabilistic Risk Assessment

Area	Internal Flooding Potential
RXB - 50′ Northeast CVCS Makeup Pump Gallery (Utilities Area)	This area is subject to flooding that originates in the room. Equipment that is important to safety has been identified in this area. This is expected to include the CVCS makeup pumps and associated controls. Although flooding may originate from within this room, this area has flood protection features to that are designed to prevent floods from challenging this equipment.
RXB - Module 1 EDSS-MS Battery Room C (Battery Room)	This area contains only electrical equipment and no flooding sources have been identified in the area. This area contains equipment that has flood protection features to that are designed to prevent floods from propagating into this room and challenging this equipment.
RXB - Module 1 EDSS-MS Battery Room A (Battery Room)	This area contains only electrical equipment and no flooding sources have been identified in the area. This area contains equipment that has flood protection features to that are designed to prevent floods from propagating into this room and challenging this equipment.
RXB - Module 1 MPS Division I Equipment Room (I/O Cabinet Room)	This area contains only electrical equipment and no flooding sources have been identified in the area. This area contains equipment that has flood protection features to that are designed to prevent floods from propagating into this room and challenging this equipment.
RXB - Module 1 EDSS-MS Battery Room B (Battery Room)	This area contains only electrical equipment and no flooding sources have been identified in the area. This area contains equipment that has flood protection features to that are designed to prevent floods from propagating into this room and challenging this equipment.
RXB - Module 1 EDSS-MS Battery Room D (Battery Room)	This area contains only electrical equipment and no flooding sources have been identified in the area. This area contains equipment that has flood protection features to that are designed to prevent floods from propagating into this room and challenging this equipment.
RXB - Module 1 EDSS-MS Switchgear Room C (Charger Room)	This area contains only electrical equipment and no flooding sources have been identified in the area. This area contains equipment that has flood protection features to that are designed to prevent floods from propagating into this room and challenging this equipment.
RXB - Module 1 EDSS-MS Switchgear Room A (Charger Room)	This area contains only electrical equipment and no flooding sources have been identified in the area. This area contains equipment that has flood protection features to that are designed to prevent floods from propagating into this room and challenging this equipment.
RXB - Module 1 MPS Division II Equipment Room (I/O Cabinet Room)	This area contains only electrical equipment and no flooding sources have been identified in the area. This area contains equipment that has flood protection features to that are designed to prevent floods from propagating into this room and challenging this equipment.
RXB - Module 1 EDSS-MS Switchgear Room B (Charger Room)	This area contains only electrical equipment and no flooding sources have been identified in the area. This area contains equipment that has flood protection features to that are designed to prevent floods from propagating into this room and challenging this equipment.
RXB - Module 1 EDSS-MS Switchgear Room D (Charger Room)	This area contains only electrical equipment and no flooding sources have been identified in the area. This area contains equipment that has flood protection features to that are designed to prevent floods from propagating into this room and challenging this equipment.

Table 19.1-49: Assessment of Flood Areas Containing Equipment Modeled in the Probabilistic Risk Assessment (Continued)

Area	Internal Flooding Potential
RXB - 100’ Northwest Reactor Component Cooling Water Pump Gallery (Utilities Area)	This area is subject to flooding that originates in the room or by propagation from adjacent areas. No risk significant equipment was identified in the area, so flooding protection is expected to be minimal.
CRB - Main Control Room (Control Room)	This area contains only electrical equipment and no flooding sources have been identified in the area. This area contains equipment that is important to safety and has flood protection features to that are designed to prevent floods from propagating into this room and challenging this equipment.
Auxiliary AC Power Source	Internal flooding is not expected. Area is expected to contain only electrical equipment. This area has been screened from further consideration.
Backup Diesel Generator (North)	Internal flooding is not expected. Area is expected to contain only electrical equipment. This area has been screened from further consideration.
Backup Diesel Generator (South)	Internal flooding is not expected. Area is expected to contain only electrical equipment. This area has been screened from further consideration.
Demineralized Water System Pumps	Flooding in this area may challenge the demineralize water system pumps.
High Voltage Power Distribution Center	Internal flooding is not expected. Area is expected to contain only electrical equipment. This area has been screened from further consideration.
Low Voltage Power Distribution Center	Internal flooding is not expected. Area is expected to contain only electrical equipment. This area has been screened from further consideration.
Medium Voltage Power Distribution Center	Internal flooding is not expected. Area is expected to contain only electrical equipment. This area has been screened from further consideration.

Table 19.1-50: Applicability of Internal Initiating Events to Internal Flooding Probabilistic Risk Assessment

Initiating Event	Applicability to Internal Flooding	Comments
CVCS Charging Line LOCA Inside Containment (CVCS--ALOCA-CIC)	No	Passive components are not susceptible to flood damage; an internal flood does not result in a CVCS injection line LOCA inside the CNV.
CVCS Charging Line Break Outside Containment (CVCS--ALOCA-COC)	No	Passive components are not susceptible to flood damage; an internal flood does not result in a CVCS injection line LOCA outside the CNV. Flooding induced by this initiating event may challenge CVCS makeup pump operation. The CVCS makeup pumps are not credited for mitigating this event, so the flooding is not relevant to the accident progression.
CVCS Letdown Line LOCA Outside Containment (CVCS--ALOCA-LOC)	No	Passive components are not susceptible to flood damage; an internal flood does not result in a CVCS discharge line break outside the CNV.
Spurious Opening of an ECCS Valve (ECCS--ALOCA-RV1)	No	An internal flood does not result in the spurious opening of an ECCS valve. The main valves are not susceptible to damage from flooding and the control solenoids are normally submerged in the reactor pool so they are not susceptible to flooding. Opening resulting from the loss of control power included in the assessment of EDSS--LODC-----ET.
Loss of DC Power (EDSS--LODC-----)	No	Given flooding-induced damage to the EDSS switchgear, an internal flooding event could physically result in a loss of two or more EDSS power channels. No internal flooding sources were identified in an area containing this equipment. Accordingly, this event is not included in the internal flooding PRA.
Loss of Offsite Power (EHVS--LOOP-----)	No	Given flooding-induced damage to electrical switchgear, an internal flooding event could result in a LOOP. No internal flooding sources were identified in an area containing this equipment. Accordingly, this event is not included in the internal flooding PRA
SGTF (MSS---ALOCA-SG--)	No	Passive components are not susceptible to flood damage; an internal flood does not result in an SGTF.
LOCA Inside Containment (RCS---ALOCA-IC--)	No	Passive components are not susceptible to flood damage; an internal flood does not result in an RCS LOCA inside the CNV.
Secondary Side Line Break (TGS---FMSLB-UD--)	No	Passive components are not susceptible to flood damage; an internal flood does not result in a feedwater or steam line break.
General Reactor Trip (TGS---TRAN-NPC-)	Yes	An internal flood is assumed to result in a plant upset leading to a transient event. Flooding induced failures of pumps, control panels and other equipment may result in a reactor trip and subsequent transient.
Loss of Support System (TGS---TRAN--NSS-)	Yes	An internal flood is assumed to result in a plant upset leading to a transient event. Flooding induced failures of pumps, control panels and other equipment may result in a reactor trip and subsequent transient.

Table 19.1-51: Internal Flooding Frequencies

NUREG/CR-2300 Frequency (per reactor-year)					NuScale (per mcyr)	
Location	**Severity Level**	**5th percentile**	**95th percentile**	**Mean**	**RXB**	**TGB (and other buildings)**
Auxiliary Building	Small	2.0E-6	1.0E-2	3.1E-3	1.9E-2 (EF = 18)	N/A
	Moderate and Large	2.5E-5	1.6E-2	1.6E-2		
Turbine Building (Service Water)	Moderate to Large	2.9E-7	2.5E-2	4.9E-3	N/A	3.2E-2 (EF = 8)
Turbine Building (Circulating Water)	Moderate to Large	2.2E-3	1.3E-1	2.8E-2		

Table 19.1-52: Evaluation of Internal Flooding on Mitigating Systems

Top Event	RXB	Other Buildings	Susceptibility of Mitigating Systems to Internal Flooding
RTS-T01	None	None	An internal flood does not mechanically challenge control rod insertion capability. If the control cabinets are subjected to an internal flooding, they deenergize and signal a trip to the reactor.
DHRS-T01	None	None	The mechanical portions of this system are not susceptible to the effects of internal flooding. If an internal flood challenges the control or power for these valves, they deenergize and are signaled to open.
RCS-T06	None	None	An internal flooding event does not affect the RSVs, as they are mechanical devices not requiring control or power to function. A flood also does not affect the DHRS capability to preclude a demand on the RSVs given a loss of feedwater.
RCS-T01	None	None	An internal flooding event does not affect the RSVs, as they are mechanical devices not requiring control or power to function.
RCS-T02	None	None	An internal flooding event does not affect the RSVs, as they are mechanical devices not requiring control or power to function. This event also does not affect the number of times that these valves are cycled.
ECCS-T01	None	None	The mechanical portions of this system are not susceptible internal flooding. In the event that an internal flood challenged the control or power for these valves, they deenergize and are signaled to open.
CVCS-T06	Yes	None	Flooding in some areas of the RXB may challenge the ability of the CVCS makeup pumps to add inventory to the RPV. The pumps are modeled as being unavailable to mitigate flooding events in the RXB. CVCS pipe breaks resulting in a LOCA are considered in the internal events analysis. CVCS makeup line pipe breaks which may challenge the CVCS makeup pumps do not credit the CVCS makeup pumps, so flooding of these pumps is not relevant to the accident progression. Internal flooding in the TGB does not affect system availability.
CFDS-T01	Yes	None	Flooding in some areas of the RXB may challenge the ability of the CFDS injection pumps to add inventory to the CNV. The pumps are modeled as being unavailable to mitigate flooding events in the RXB. Internal flooding in the TGB does not affect system availability.
CNTS-T01	None	None	The mechanical portions of this system are not susceptible to the effects of internal flooding. If an internal flood challenges the control or power for these valves, they deenergize and are signaled to open.

Table 19.1-53: Significant Cutsets (Internal Flooding, Full Power, Single Module)

Cutset	Prob/Freq	Contribution	Basic Event	Description
CDF Cutsets				
1	1.78E-11	29.8%		
	1.93E-2		IE-FLOOD-RXB	Internal Flooding Event in the RXB
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	7.32E-4		RCS---RSV-0003A-FTC-S	RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
2	1.24E-11	20.8%		
	1.93E-2		IE-FLOOD-RXB	Internal Flooding Event in the RXB
	1.38E-5		DHRS--HOV-1CC44-FTO-S	CCF OF 4 OF 4 DHRS ACTUATION VALVES FAIL TO OPEN
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
3	8.78E-12	14.7%		
	1.93E-2		IE-FLOOD-RXB	Internal Flooding Event in the RXB
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	7.32E-4		RCS---RSV-0003A-FTC-S	RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
4	5.91E-12	9.9%		
	1.93E-2		IE-FLOOD-RXB	Internal Flooding Event in the RXB
	6.55E-6		CRDS--ROD-1CC316FOP-S	GIVEN ACTUATION, AT LEAST 3 OF 16 RODS FAIL TO INSERT
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
5	2.94E-12	4.9%		
	1.93E-2		IE-FLOOD-RXB	Internal Flooding Event in the RXB
	3.26E-6		MPS---APL-6CC22-FOP-S	CCF OF 2 OF 2 APL MODULES IN TOP BRANCH REACTOR TRIP BREAKERS
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
6	2.94E-12	4.9%		
	1.93E-2		IE-FLOOD-RXB	Internal Flooding Event in the RXB
	3.26E-6		MPS---APL-7CC22-FOP-S	CCF OF 2 OF 2 APL MODULES IN BOTTOM BRANCH REACTOR TRIP BREAKERS
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
7	2.32E-12	3.9%		
	1.93E-2		IE-FLOOD-RXB	Internal Flooding Event in the RXB
	2.57E-6		DHRS--HTX-1CC22-PLG-S	CCF OF 2 OF 2 DHRS HEAT EXCHANGERS PLUGGING
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
8	1.15E-12	1.9%		

Table 19.1-53: Significant Cutsets (Internal Flooding, Full Power, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	1.93E-2		IE-FLOOD-RXB	Internal Flooding Event in the RXB
	1.00E-1		ECCS--HOV-0002A-FOP-N	HOV 0002A ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.00E-1		ECCS--HOV-0002B-FOP-N	HOV 0002B ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.63E-5		ECCS--SOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS RRV TRIP VALVES FAIL TO OPEN
	7.32E-4		RCS---RSV-0003A-FTC-S	RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
9	7.86E-13	1.3%		
	1.93E-2		IE-FLOOD-RXB	Internal Flooding Event in the RXB
	8.71E-7		MPS---APL-4CC44-FOP-S	CCF OF 4 OF 4 APL MODULES IN DHRS ACTUATION VALVES
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
10	7.06E-13	1.2%		
	1.93E-2		IE-FLOOD-RXB	Internal Flooding Event in the RXB
	1.00E-7		ECCS--SYS-0001X-PTH-S	HEAT TRANSFER TO REACTOR POOL FAILS
	7.32E-4		RCS---RSV-0003A-FTC-S	RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
11	6.68E-13	1.1%		
	1.93E-2		IE-FLOOD-RXB	Internal Flooding Event in the RXB
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
	7.40E-7		RTS---RTB-2CC22-FTO-S	CCF OF 2 OF 2 BOTTOM BRANCH REACTOR TRIP BREAKERS FAIL TO OPEN
12	6.68E-13	1.1%		
	1.93E-2		IE-FLOOD-RXB	Internal Flooding Event in the RXB
	4.68E-5		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
	7.40E-7		RTS---RTB-1CC22-FTO-S	CCF OF 2 OF 2 TOP BRANCH REACTOR TRIP BREAKERS FAIL TO OPEN
LRF Cutsets				
N/A	N/A	N/A	N/A	There are no LRF cutsets with a calculated frequency greater than the truncation frequency of 1E-15

Table 19.1-54: Key Assumptions for the Internal Flooding PRA

Assumption	Basis
Buildings that are not expected to contain flood sources or are not expected to result in a plant trip are not considered.	Engineering judgment
Pipe routing and physical locations of some equipment are not defined at the design certification stage; flood locations are assumed from plant drawings.	Engineering judgment
An internal flood is capable of resulting in a plant upset and transient initiating event.	Engineering judgment
Flooding frequencies are based on generic data for turbine and auxiliary buildings, including human-induced mechanisms. A lognormal distribution is assumed.	Engineering judgment
No credit is taken for floor drains therefore, maximum flood heights are considered.	Bounding assumption
Operator actions to isolate a flooding event are not modeled. The time required to isolate a flood, however, is used to establish the volume of water involved in the event and establish the depth of water involved in the flood.	Engineering judgment
Flooding effects for equipment located inside the containment are not considered.	Equipment located in containment is designed to operate in harsh environments, including LOCAs.
Safety-related and risk significant equipment is protected from flooding effects.	Although not defined at design certification, flood protection (e.g., flood door, splash protection) for safety-related and risk significant equipment is a design requirement.
Equipment that is not safety-related or risk significant is exposed to flooding in the area where it is located; flood-induced failure mechanisms include spray and submergence.	Bounding assumption
Passive components such as piping, tanks, heat exchangers, manual valves, check valves, relief valves, strainers and filters are not susceptible to flood damage	Passive equipment does not require control to operate
Electrical equipment is susceptible to flood damage which occurs instantaneously when the lowest portion of the equipment is submerged. The most likely failure mechanism for flood water damage is a short-to ground, which results in an open-circuit failure mode.	Bounding assumption
If subjected to a flood, motor operated valves fail as-is and solenoid and air-operated valves fail to their de-energized position.	Engineering judgment
A flood in the RXB will prevent operations from establishing makeup with the CVCS or CFDS.	Bounding assumption
Consistent with the internal events analysis, high stress was considered for operator actions.	Engineering judgment
Equipment affected by a flood is based on the analysis summarized in Section 3.4.1.	Common engineering practice

Table 19.1-55: Applicability of Internal Initiating Events to External Flooding Probabilistic Risk Assessment

Internal Event PRA Initiating Event	Applicability to External Flood PRA	Basis
CVCS Charging Line LOCA Inside Containment (CVCS--ALOCA-CIC)	No	Passive components are not susceptible to flood damage; an external flood does not result in a LOCA inside containment.
CVCS Charging Line Break Outside Containment (CVCS--ALOCA-COC)	No	Passive components are not susceptible to flood damage; an external flood does not result in a pipe break outside containment.
CVCS Letdown Line Break Outside Containment (CVCS--ALOCA-LOC)	No	Passive components are not susceptible to flood damage; an external flood does not result in a pipe break outside containment.
Spurious Opening of an ECCS Valve (ECCS--ALOCA-RV1)	No	An external flood does not result in spurious operation of the ECCS valves. The LOOP event tree captures the loss of power and de-energization of the ECCS solenoid valves after a loss of AC power for 24 hours.
Loss of DC Power (EDSS--LODC-----)	Bounded	A flood-induced loss of DC is bounded by a flood-induced LOOP; the event trees are identical when including equipment that is susceptible to flood damage (including the DC switchgear).
Loss Of Offsite Power (EHVS--LOOP-----)	Yes	In cases where operators do not have warning time to shut down the plant, an external flood is expected to cause a LOOP; the AC power equipment is susceptible to an external flood.
Steam Generator Tube Failure (MSS---ALOCA-SG-)	No	Passive components are not susceptible to flood damage; an external flood does not result in an SGTF.
LOCA Inside Containment (RCS---ALOCA-IC-)	No	Passive components are not susceptible to flood damage; an external flood does not result in a LOCA inside containment.
Secondary Side Line Break (TGS---FMSLB-UD-)	No	Passive components are not susceptible to flood damage; an external flood does not result in a secondary line break.
General Reactor Trip (TGS---TRAN-NPC)	Bounded	A flood-induced reactor trip is bounded by a flood-induced LOOP. The accident progression following a reactor trip is identical to that following a loss of power when not crediting AC power.
Loss of Support System (TGS---TRAN-NSS)	Bounded	A flood-induced loss of a support system (e.g., AC bus) is bounded by a flood-induced LOOP. The accident progression following a support system trip is identical to that following a loss of power when not crediting AC power.

Table 19.1-56: Evaluation of External Flooding on Mitigating Systems

Top Event for EHVS-LOOP[1]	External Flooding Susceptibility Evaluation	
EHVS-T01, Combustion turbine generator	Yes	The CTG is located in the yard between the turbine buildings and switchyard; it is susceptible to damage from an external flood.
ELVS-T01, Backup diesel generators	Yes	The backup diesel generators are located in separate structures west of the turbine buildings; they are susceptible to damage from an external flood.
RTS-T01, Reactor trip system	Indirect effect	The RTS provides power to the reactor trip breakers through the MPS to keep them closed. It delivers power from the EDNS to the CRDS breakers within the MPS. Although the CRDS is not susceptible to damage from an external flood, the loss of EDNS results in the control rods dropping into the core.
DHRS-T01, DHRS	Indirect effect	The MPS provides power to keep the DHRS actuation valves closed and associated feedwater and main steam CIVs open. A loss of normal DC power system (EDSS) power causes the DHRS actuation valves to open and the associated CIVs to close.
RCS-T05 and RCS-T01, Reactor safety valve opens	No	The reactor safety valves (RSVs) are pilot-operated relief valves located on the RPV head; the design and location preclude flood susceptibility.
RCS-T02, Reactor safety valves cycling	No	The RSVs are pilot-operated relief valves located on the RPV head; the design and location preclude flood susceptibility.
EHVS-T02, Offsite power recovered	Yes	Recovery of offsite power is not credited based on the nature and possible duration of an external flooding hazard.
ECCS-T01, ECCS Rx vent valves and Rx recirculation valves open	Indirect effect	The MPS provides power to keep the ECCS valves closed. A loss of EDSS power de-energizes the ECCS solenoid valves. The main valves open when the solenoid is de-energized. Although the main valves open when the solenoid is de-energized, the valves include an inadvertent actuation block that prevents opening until a low differential pressure is reached between the RPV and CNV.
CNTS-T01, Containment isolation - CIVs close	Indirect effect	The CIVs are hydraulically operated to open and the EDSS provides power to the solenoids to maintain the valves in the open position. Upon a loss of power, the hydraulic pressure is relieved by de-energizing the solenoid valve, and the on-board nitrogen accumulator closes the valve.

Notes:

1. All top events listed, except CNTS-T01, are in the LOOP event tree; CNTS-T01 is in the Level 2 event tree.

Table 19.1-57: Significant Cutsets (External Flooding, Full Power, Single Module)

Cutset	Prob/Freq	Contribution	Basic Event	Description
CDF Cutsets				
1	2.52E-10	31.2%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
2	2.52E-10	31.2%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
3	1.24E-10	15.4%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
4	1.24E-10	15.4%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
5	1.63E-11	2.0%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	1.00E-1		ECCS--HOV-0002A-FOP-N	HOV 0002A ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.00E-1		ECCS--HOV-0002B-FOP-N	HOV 0002B ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.63E-5		ECCS--SOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS RRV TRIP VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
6	1.63E-11	2.0%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	1.00E-1		ECCS--HOV-0002A-FOP-N	HOV 0002A ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.00E-1		ECCS--HOV-0002B-FOP-N	HOV 0002B ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS

Table 19.1-57: Significant Cutsets (External Flooding, Full Power, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	1.63E-5		ECCS--SOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS RRV TRIP VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
7	1.00E-11	1.2%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	1.00E-7		ECCS--SYS-0001X-PTH-S	HEAT TRANSFER TO REACTOR POOL FAILS
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
8	1.00E-11	1.2%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	1.00E-7		ECCS--SYS-0001X-PTH-S	HEAT TRANSFER TO REACTOR POOL FAILS
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
LRF Cutsets				
1	1.30E-14	16.7%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	5.14E-5		CES---HOV-1CC22-FTC-S	CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
2	1.30E-14	16.7%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	5.14E-5		CES---HOV-1CC22-FTC-S	CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
3	1.30E-14	16.7%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
4	1.30E-14	16.7%		

Table 19.1-57: Significant Cutsets (External Flooding, Full Power, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
5	6.39E-15	8.3%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	5.14E-5		CES---HOV-1CC22-FTC-S	CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
6	6.39E-15	8.3%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	5.14E-5		CES---HOV-1CC22-FTC-S	CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
7	6.39E-15	8.3%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
8	6.39E-15	8.3%		
	2.00E-3		IE-EXTNL-FLOOD-FP-	External Flood
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	1.00E-1		EXTERNALFLOOD_LOOP	External Flood Results in LOOP
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open

Table 19.1-58: Key Assumptions for the External Flooding PRA

Assumption	Basis
An external flood that exceeds the design basis flood level has a recurrence interval of 500 years; external flooding frequency is 2 E-3/yr.	Engineering judgment and consistent with the ASME/ANS PRA Standard expected range of between 0.01 to 0.001 per year.
Forecasting information is used to take mitigative actions; operators are assumed to cease refueling and crane operations, and perform a controlled shutdown when forecasts or conditions indicate the potential for SSC susceptibility to an external flood. Ninety percent of external floods are assumed to include significant warning time to take action; the remaining 10% are assumed to result in a LOOP. Additional and temporary mitigative actions (e.g., sandbags) are not credited in the analysis.	Engineering judgment
An external flood that results in a LOOP is assumed to extend beyond the PRA 72 hour mission time; recovery of offsite power is not considered.	Engineering judgment
Electrical equipment is susceptible to flood damage which occurs instantaneously when the lowest portion of the equipment is submerged. The most likely failure mechanism for flood water damage is a short-to-ground, which results in an open-circuit failure mode. Failure occurs instantaneously when the lowest portion of the equipment is submerged.	Bounding assumption
Passive components such as piping, tanks, heat exchangers, manual valves, check valves, relief valves, strainers and filters are not susceptible to flood damage.	Engineering judgment
Following a loss of power, motor operated valves are assumed to fail "as-is" and air and solenoid-operated valves are assumed to fail in the de-energized position.	Engineering judgment
Flooding effects for equipment located inside the containment are not considered.	Equipment located in containment is isolated from external flooding.
Flooding exceeding the design basis flood level is assumed not to structurally damage the Seismic Category I reactor building.	Engineering judgment

Table 19.1-59: Applicability of Internal Initiating Events to High-Winds Probabilistic Risk Assessment

Initiating Event	Applicability to HW PRA	Comments
CVCA Charging Line LOCA Inside Containment (IE-CVCS-ALOCA-CIC)	No	The CVCS is located in the RXB and therefore protected from high winds.
CVCS Charging Line Break Outside Containment (IE-CVCS-ALOCA-COC)	No	The CVCS is located in the RXB and therefore protected from high winds.
CVCS Letdown Line LOCA Outside Containment (IE-CVCS-ALOCA-LOC)	No	The CVCS is located in the RXB and therefore protected from high winds.
Spurious Opening of an ECCS Valve (IE-ECCS-ALOCA-RV1)	No	A high-winds event does not result in spurious operation of the ECCS valves. The LOOP event tree captures the loss of power and eventual de-energization of the ECCS solenoid valves.
Loss of DC Power (IE-EDSS-LODC----)	Bounded	The EDSS is located in the RXB and therefore protected from high winds. The eventual loss of DC power, due to the loss of AC power, is bounded by a LOOP.
Loss Of Offsite Power (IE-EHVS-LOOP----)	Yes	High winds are assumed to result in a LOOP.
SGTF (IE-MSS---ALOCA-SG)	No	The steam generators are located in the RXB and therefore protected from high winds.
LOCA Inside Containment (IE-RCS---ALOCA-IC	No	Reactor coolant system components are located in the RXB and therefore protected from high winds.
Secondary Side Line Break (IE-TGS---FMSLB-UD)	Screened	The RXB houses the feedwater and steam lines upstream of the CIVs and equipment in the RXB is protected from high winds. Although both lines exit the RXB, a high winds-induced break would be unlikely and easily mitigated by isolation valves inside the RXB; therefore high wind-induced secondary line breaks were screened.
General Reactor Trip (IE-TGS---TRAN-NPC)	Bounded	A high wind-induced transient is bounded by a LOOP. The accident progression following a transient is identical to that following a loss of power considering that systems that rely on AC power are not available.
Loss of Support System (IE-TGS---TRAN-NSS)	Bounded	A high-wind induced support system loss is bounded by a LOOP.

Table 19.1-60: Building Capability to Withstand High Winds

Tornado Intensity	Hurricane Intensity	Potential Building Effect		
Enhanced Fujita (EF) Scale	**Saffir-Simpson scale**	**Seismic Category I**	**Seismic Category II**	**Seismic Category III**
EF2 -EF3	3	NA		Missiles cause damage to the structure and SSC within the structure.
EF4	4	NA	Superficial damage to outer walls, air handlers, etc.	Significant wind and missile damage to the structure and to SSC within the structure.
EF5	5	Superficial damage to outer walls, air handlers, etc.	Significant wind and missile damage to the structure and to SSC within the structure.	Significant wind and missile damage to the structure and to SSC within the structure.

Table 19.1-61: Key Assumptions for the High-Winds Probabilistic Risk Assessment

Assumption	Basis
Extratropical straight winds, tornadoes = EF0 and EF1 (i.e., ≤ 110 mph), and hurricanes = Category 1 and 2 (i.e., ≤ 110 mph) are covered by the weather related LOOP initiator in the internal events PRA.	Engineering judgment
A LOOP is assumed for all extreme high-winds events.	Engineering judgment
Recovery of offsite power within 24 hours following a high-winds event is based on generic weather-related offsite power recovery events. Additional recovery or mitigative actions are not credited in the analysis.	Engineering judgment
A tornado strike hazard is determined from methods described in NUREG/CR-4661 and based on a central U.S. geographic region. A lognormal distribution and error factor of 10 is assumed.	Bounding assumption
A hurricane strike hazard is determined from NUREG-6890 industry data and based on a coastal U.S geographic region. A lognormal distribution and error factor of 10 is assumed.	Bounding assumption
Seismic Category I structures and SSC in Seismic Category I structures are not susceptible to damage from high-winds events, wind-generated missiles, or damage from other buildings or SSC.	Engineering judgment
Seismic Category II and III buildings and SSC within, and SSC located outside, are assumed inoperable with no consideration of recovery.	Bounding assumption
Following a loss of power, motor operated valves are assumed to fail “as-is” and air and solenoid-operated valves are assumed to fail in the de-energized position.	Engineering judgment
Extreme stress was considered for operator actions following a high winds event.	Engineering judgment

Table 19.1-62: Significant Cutsets (Hurricanes, Full Power, Single Module)

Cutset	Prob/Freq	Contribution	Basic Event	Description
CDF Cutsets				
1	2.07E-10	30.9%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
2	2.07E-10	30.9%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
3	1.02E-10	15.3%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
4	1.02E-10	15.3%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
5	1.33E-11	2.0%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	1.00E-1		ECCS--HOV-0002A-FOP-N	HOV 0002A ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.00E-1		ECCS--HOV-0002B-FOP-N	HOV 0002B ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.63E-5		ECCS--SOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS RRV TRIP VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open

Table 19.1-62: Significant Cutsets (Hurricanes, Full Power, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
6	1.33E-11	2.0%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	1.00E-1		ECCS--HOV-0002A-FOP-N	HOV 0002A ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.00E-1		ECCS--HOV-0002B-FOP-N	HOV 0002B ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.63E-5		ECCS--SOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS RRV TRIP VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
LRF Cutsets				
1	1.06E-14	16.7%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	5.14E-5		CES---HOV-1CC22-FTC-S	CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
2	1.06E-14	16.7%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
3	1.06E-14	16.7%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	5.14E-5		CES---HOV-1CC22-FTC-S	CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE

Table 19.1-62: Significant Cutsets (Hurricanes, Full Power, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
4	1.06E-14	16.7%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	5.14E-5		CES---HOV-1CC22-FTC-S	CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	2.52E-6		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
5	5.24E-15	8.3%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
6	5.24E-15	8.3%	1.49E-3	
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	5.14E-5		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
7	5.24E-15	8.3%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	5.14E-5		CES---HOV-1CC22-FTC-S	CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN

Table 19.1-62: Significant Cutsets (Hurricanes, Full Power, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
8	5.24E-15	8.3%		
	1.49E-3		IE-HURR-CAT3-5-FP-	Hurricane
	5.14E-5		CES---HOV-1CC22-FTC-S	CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.24E-6		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	4.00E-2		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+0		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	1.00E+0		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	5.00E-1		/RCS-T05	RCS Reactor Safety Valve Demanded to Open

Table 19.1-63: Significant Cutsets (Tornadoes, Full Power, Single Module)

Cutset	Prob/Freq	Contribution	Basic Event	Description
CDF Cutsets				
1	2.87E-11	30.9%		
	2.07E-04		IE-TORN--EF2-5-FP-	Tornado
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+00		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	5.00E-01		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
2	2.87E-11	30.9%		
	2.07E-04		IE-TORN--EF2-5-FP-	Tornado
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+00		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	5.00E-01		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
3	1.41E-11	15.3%		
	2.07E-04		IE-TORN--EF2-5-FP-	Tornado
	1.24E-06		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+00		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	5.00E-01		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
4	1.41E-11	15.3%		
	2.07E-04		IE-TORN--EF2-5-FP-	Tornado
	1.24E-06		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+00		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	5.00E-01		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
5	1.85E-12	2.0%		
	2.07E-04		IE-TORN--EF2-5-FP-	Tornado
	1.00E-01		ECCS--HOV-0002A-FOP-N	HOV 0002A ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.00E-01		ECCS--HOV-0002B-FOP-N	HOV 0002B ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.63E-05		ECCS--SOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS RRV TRIP VALVES FAIL TO OPEN
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE

Table 19.1-63: Significant Cutsets (Tornadoes, Full Power, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	2.75E+00		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	5.00E-01		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
6	1.85E-12	2.0%		
	2.07E-04		IE-TORN--EF2-5-FP-	Tornado
	1.00E-01		ECCS--HOV-0002A-FOP-N	HOV 0002A ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.00E-01		ECCS--HOV-0002B-FOP-N	HOV 0002B ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.63E-05		ECCS--SOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS RRV TRIP VALVES FAIL TO OPEN
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	2.75E+00		EHVS--SYS-0002X-FOP-N	LOOP Recovery Adjustment for Weather-Related Causes
	5.00E-01		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
LRF Cutsets				
N/A	N/A	N/A	N/A	There are no LRF cutsets with a calculated frequency greater than the truncation frequency of 1E-15.

Table 19.1-64: Listing of Candidate Risk Significant Structures, Systems, and Components: External Events

System	Description	CCDF	CLRF	FVCDF	FVLRF
ECCS	Emergency core cooling system	FI, EF, HW	FI		
MPS	Module protection system	FI, IF	FI, IF, EF, HW		
UHS	Ultimate heat sink	FI, EF, HW	FI		
Component	**Basic Event Description**	**CCDF**	**CLRF**	**FVCDF**	**FVLRF**
CES-HOV-0001X	HOV 0001X CNTS CES containment isolation valve	Not Met	Not Met	Not Met	EF[1], HW[1]
CES-HOV-0002X	HOV 0002X CNTS CES containment isolation valve	Not Met	Not Met	Not Met	EF[1], HW[1]
CVCS-HOV-0334X	HOV 0334X CNTS CVCS discharge line containment isolation valve	Not Met	Not Met	Not Met	FI[1], EF[1], HW[1]
CVCS-HOV-0335X	HOV 0335X CNTS CVCS discharge line containment isolation valve	Not Met	Not Met	Not Met	FI[1], EF[1], HW[1]
DHRS-HOV-0101A	HOV 0101A for DHRS HTX 0103X inlet	Not Met	Not Met	IF[1]	Not Met
DHRS-HOV-0101B	HOV 0101B for DHRS HTX 0103X inlet	Not Met	Not Met	IF[1]	Not Met
DHRS-HOV-0201A	HOV 0201A for DHRS HTX 0203X inlet	Not Met	Not Met	IF[1]	Not Met
DHRS-HOV-0201B	HOV 0201B for DHRS HTX 0203X inlet	Not Met	Not Met	IF[1]	Not Met
ECCS-HOV-0001A	HOV 0001A ECCS reactor vent valve	Not Met	Not Met	FI[1], EF[1], HW[1]	EF[1], HW[1]
ECCS-HOV-0001B	HOV 0001B ECCS reactor vent valve	Not Met	Not Met	FI[1], EF[1], HW[1]	EF[1], HW[1]
ECCS-HOV-0001C	HOV 0001C ECCS reactor vent valve	Not Met	Not Met	FI[1], EF[1], HW[1]	EF[1], HW[1]
ECCS-HOV-0002A	HOV 0002A ECCS reactor recirculation valve	Not Met	Not Met	FI[1], IF[1], EF[1], HW[1]	FI[1], EF[1], HW[1]
ECCS-HOV-0002B	HOV 0002B ECCS reactor recirculation valve	Not Met	Not Met	FI[1], IF[1], EF[1], HW[1]	FI[1], EF[1], HW[1]
ECCS-SOV-0101A	SOV 0101A ECCS trip valve	Not Met	Not Met	FI	Not Met
RCS-RSV-0003A	RCS reactor safety valve 0003A	Not Met	Not Met	FI[1], IF	FI[1]
RCS-RSV-0003B	RCS reactor safety valve 0003B	Not Met	Not Met	FI[1], IF[1]	FI[1]
Initiator	**Description**	**CCDF**	**CLRF**	**FVCDF**	**FVLRF**
IE-FIRE-2-LOOP	Fire causes loss of offsite power			FI	Not Met
IE-FIRE-3-ECCS	Fire induces spurious ECCS actuation - division I & II affected			FI	Not Met
IE-FLOOD-RXB	Internal flooding event in the reactor building			IF	Not Met
IE-FIRE-1-LOCA	Fire spuriously operates CVCS makeup pump			Not Met	FI
IE-FIRE-27-TRANSIENT	Multi-compartment scenario - fire spread results in transient - division I & II ESFAS failed			Not Met	FI

Notes:
- Spaces that are grayed out' indicate categories in which the criteria do not apply, as described in TR-0515-13952-A.
- As stated in the DCA text, no human actions are risk significant.
- Abbreviations: FI is internal fires PRA; IF is internal flooding PRA; EF is external flooding PRA; HW is high-winds PRA.

[1] The criterion is 'Met' with CCFs conservatively included in the calculation of the single component FV.

Table 19.1-65: Plant Operating States for Low Power and Shutdown Probabilistic Risk Assessment

POS	Description	Time Entering POS (hours after shutdown)	Module Configuration Entering POS	Time Exiting POS (hours after shutdown)	Module Configuration Exiting POS
1	Shutdown and Initial Cooling	0.0	Turbine tripped	14.0	CNV flood complete
2	Cooling Through Containment	14	CNV flood complete	47.25	Module lifted by RBC
3	Transport and Disassembly	47.25	Module lifted by RBC	70.25	Upper vessels moved into dry dock
4	Refueling and Maintenance	70.25	Upper vessels moved into dry dock	145.25	Upper vessels moved out of dry dock
5	Reassembly, Transport, and Reconnection	145.25	Upper vessels moved out of dry dock	219	CNV drain begins
6	Heatup	219	CNV drain begins	232	Control rods withdrawn to criticality
7	Low Power Operation	232	Control rods withdrawn to criticality	244.75	Turbine synchronized with grid

Table 19.1-66: Low Power and Shutdown Initiating Events

Full Power Initiating Event	Applicability	Basis
All	POS1, POS6 and POS7	Module configuration is similar to normal operation
IE-CVCS--ALOCA-CIC	Screened for POS2, POS3, POS4, and POS5	CNV is already flooded (POS2, POS3, POS5); Module is disassembled and open to reactor pool (POS4)
IE-CVCS--ALOCA-COC	Screened for POS3 and POS4; Retained for portions of POS2 and POS5 in which CVCS is in service	CVCS is isolated when out of service (POS2, POS3, POS5); Module is disassembled and open to reactor pool (POS4)
IE-CVCS--ALOCA-LOC	Screened for POS3 and POS4; Retained for portions of POS2 and POS5 where CVCS is in service	CVCS is isolated when out of service (POS2, POS3, POS5); Module is disassembled and open to reactor pool (POS4)
IE-ECCS--ALOCA-RV1	Screened for POS2, POS3, POS4, and POS5	CNV is already flooded (POS2, POS3, POS5); Module is disassembled and open to reactor pool (POS4)
IE-EDSS--LODC-----	Screened for POS2, POS3, POS4, and POS5	Cooling is passive and unaffected by LOOP (POS2); RBC operation is not reliant on DC busses modeled in PRA (POS3, POS5); Module is disassembled and open to reactor pool (POS4)
IE-EHVS--LOOP-----	Screened for POS2, POS3, POS4, and POS5	Cooling is passive and unaffected by LOOP (POS2); LOOP is included in RBC initiating event frequency (POS3, POS5); Module is disassembled and open to reactor pool (POS4)
IE-MSS---ALOCA-SG-	Screened for POS2, POS3, POS4, and POS5	Cooling is passive, secondary cooling is isolated and not in service (POS2, POS3, POS5); Module is disassembled and open to reactor pool (POS4)
IE-RCS---ALOCA-IC-	Screened for POS2, POS3, POS4, and POS5	CNV is already flooded (POS2, POS3, POS5); Module is disassembled and open to reactor pool (POS4)
IE-TGS---FMSLB-UD-	Screened for POS2, POS3, POS4, and POS5	Cooling is passive, secondary cooling is isolated and not in service (POS2, POS3, POS5); Module is disassembled and open to reactor pool (POS4)
IE-TGS---TRAN--NPC	Screened for POS2, POS3, POS4, and POS5	Cooling is passive, module not affected by general transient (POS2, POS3, POS5); Module is disassembled and open to reactor pool (POS4)
IE-TGS---TRAN--NSS	Screened for POS3 and POS4	Support systems are not in use during POS3 and POS4

Table 19.1-67: Module Drop Initiating Events and Mitigating Features

Type	Item	Module Drop Initiating Event	Mitigating Feature	Failure End State
NPM (NuScale Power Module)	1	BRIDGE-OS (Bridge overspeed)	DET-BRIDGE-OS (Overspeed detection); SS-BRIDGE (Safety stop for bridge traverse)	Module Drop
	2	BRIDGE-OT (Bridge travel)	DET-BRIDGE-OT (Overtravel detection); SS-BRIDGE (Safety stop for bridge traverse)	Module Drop
	3	GMD-2DT (Both drive trains fail)	None	Module Drop
	4	GWD-2WR (Both wire ropes fail)	None	Module Drop
	5	LOP (Loss of Power)	SS-LOP (Shoe brakes fail to clamp)	Module Drop
	6	(MR) Misreeving	DET-MR (Misreeving detection); SS-HOIST (Safety stop for hoist);	Module Drop
	7	OL (Overload)	DET-OL (Overload detection); SS-HOIST (Safety stop for hoist); OL-PROT (Main hoist motor overload protection)	Module Drop
	8	OS (Hoist overspeed)	DET-OS (Hoist overspeed detection); SS-HOIST (Safety stop for hoist)	Module Drop
	9	OTL (Hoist overtravel lower)	DET-OTL-EXT (Detection of extreme overtravel); SS-HOIST (Safety stop for hoist)	Module Drop
	10	OTR (Hoist overtravel raise)	DET-OTR-EXT (Detection of extreme overtravel); SS-HOIST (Safety stop for hoist)	Module Drop
	11	UB (Unbalanced Load)	DET-UB (SS actuation signal fails); SS-HOIST (Safety stop for hoist)	Module Drop
	12	(TROLLEY-OS) Trolley overspeed	DET-TROLLEY-OS (Detection of trolley overspeed SS-TROLLEY (Safety stop for trolley)	Module Drop
	13	(TROLLEY-OT) Trolley overtravel	DET-TROLLEY-OT (Detection of trolley overtravel; SS-TROLLEY (Safety stop for trolley)	Module Drop

Table 19.1-68: Module Drop Initiating Event Frequency

Initiating Event	Point Estimate Probability per Lift	Lift Frequency per Year	Initiating Event Frequency per Year	Error Factor
IE-POS3-RBC-DROP-OP-FTS	5 E-08	0.5	2.5 E-08	10
IE-POS3-RBC-DROP-RF-FTS	6 E-08	0.5	3.1 E-08	10
IE-POS5-RBC-DROP-OP-FTS	5 E-08	0.5	2.5 E-08	10
IE-POS5-RBC-DROP-RF-FTS	6 E-08	0.5	3.1E-08	10

Table 19.1-69: Significant Cutsets (Low Power and Shutdown, Single Module)

Cutset	Prob/Freq	Contribution	Basic Event	Description
CDF Cutsets - Internal Events				
1	3.29E-14	7.3%		
	3.26E-06		IE-POS1-ECCS--ALOCA-RV1	Spurious Opening of an ECCS Valve - POS1
	1.00E+00		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
2	3.05E-14	6.8%		
	3.03E-06		IE-POS6-ECCS--ALOCA-RV1	Spurious Opening of an ECCS Valve - POS6
	1.00E+00		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
3	2.05E-14	4.6%		
	3.76E-08		IE-POS1-EDSS--LODC-----	Loss of DC Power - POS1
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	2.16E-01		EDSS--EBD-1CC44-FOP-N	INITIATOR IS CCF OF 4 OF 4 EDSS DC BUSSES TO OPERATE
4	1.90E-14	4.2%		
	3.49E-08		IE-POS6-EDSS--LODC-----	Loss of DC Power - POS6
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	2.16E-01		EDSS--EBD-1CC44-FOP-N	INITIATOR IS CCF OF 4 OF 4 EDSS DC BUSSES TO OPERATE
5	1.86E-14	4.1%		
	3.42E-08		IE-POS7-EDSS--LODC-----	Loss of DC Power - POS7
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	2.16E-01		EDSS--EBD-1CC44-FOP-N	INITIATOR IS CCF OF 4 OF 4 EDSS DC BUSSES TO OPERATE
6	1.62E-14	3.6%		
	3.26E-06		IE-POS1-ECCS--ALOCA-RV1	Spurious Opening of an ECCS Valve - POS1
	1.00E+00		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	1.24E-06		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
7	1.61E-14	3.6%		
	1.60E-06		IE-POS1-RCS---ALOCA-IC-	LOCA Inside Containment - POS1
	1.00E+00		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN

Table 19.1-69: Significant Cutsets (Low Power and Shutdown, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
8	1.51E-14	3.4%		
	3.03E-06		IE-POS6-ECCS--ALOCA-RV1	Spurious Opening of an ECCS Valve - POS6
	1.00E+00		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	1.24E-06		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
9	1.49E-14	3.3%		
	1.48E-06		IE-POS6-RCS---ALOCA-IC-	LOCA Inside Containment - POS6
	1.00E+00		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
10	1.47E-14	3.3%		
	1.46E-06		IE-POS7-RCS---ALOCA-IC-	LOCA Inside Containment - POS7
	1.00E+00		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
CDF Cutsets - Module Drop				
1	3.13E-08	35.8%		
	3.13E-08		IE-POS3-RBC-DROP-RF-FTS	Module Drop in Refueling Area - POS3
	1.00E+00		LPSD-TRUE-FT	Transfer top event for LPSD ET
2	3.13E-08	35.8%		
	3.13E-08		IE-POS5-RBC-DROP-RF-FTS	Module drop in refueling area - POS5
	1.00E+00		LPSD-TRUE-FT	Transfer top event for LPSD ET
3	1.25E-08	14.2%		
	2.49E-08		IE-POS3-RBC-DROP-OP-FTS	Module Drop in Operating Area - POS3
	5.00E-01		RBC-OP--FRU	RBC fails to remain upright in operating area
4	1.25E-08	14.2%		
	2.49E-08		IE-POS5-RBC-DROP-OP-FTS	Module Drop in Operating Area - POS5
	5.00E-01		RBC-OP--FRU	RBC fails to remain upright in operating area
LRF Cutsets - Internal Events				
1	4.61E-15	20.0%		
	2.24E-07		IE-POS1-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside CNV - POS1
	1.00E+00		CFDS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CFDS INJECTION

Table 19.1-69: Significant Cutsets (Low Power and Shutdown, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	5.14E-05		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
2	4.28E-15	18.6%		
	2.08E-07		IE-POS6-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside CNV - POS6
	1.00E+00		CFDS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CFDS INJECTION
	5.14E-05		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
3	4.20E-15	18.2%		
	2.04E-07		IE-POS7-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside CNV - POS7
	1.00E+00		CFDS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CFDS INJECTION
	5.14E-05		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
4	1.38E-15	6.0%		
	2.24E-07		IE-POS1-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside CNV - POS1
	1.20E-03		CFDS--HOV-0021X-FTO-N	HOV 0021X CNTS CFDS CONTAINMENT ISOLATION VALVE FAILS TO OPEN
	5.14E-05		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
5	1.38E-15	6.0%		
	2.24E-07		IE-POS1-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside CNV - POS1
	1.20E-03		CFDS--HOV-0022X-FTO-N	HOV 0022X CNTS CFDS CONTAINMENT ISOLATION VALVE FAILS TO OPEN
	5.14E-05		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
6	1.28E-15	5.6%		
	2.08E-07		IE-POS6-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside CNV - POS6
	1.20E-03		CFDS--HOV-0021X-FTO-N	HOV 0021X CNTS CFDS CONTAINMENT ISOLATION VALVE FAILS TO OPEN

Table 19.1-69: Significant Cutsets (Low Power and Shutdown, Single Module) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	5.14E-05		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
7	1.28E-15	5.6%		
	2.08E-07		IE-POS6-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside CNV - POS6
	1.20E-03		CFDS--HOV-0022X-FTO-N	HOV 0022X CNTS CFDS CONTAINMENT ISOLATION VALVE FAILS TO OPEN
	5.14E-05		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
8	1.26E-15	5.5%		
	2.04E-07		IE-POS7-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside CNV - POS7
	1.20E-03		CFDS--HOV-0021X-FTO-N	HOV 0021X CNTS CFDS CONTAINMENT ISOLATION VALVE FAILS TO OPEN
	5.14E-05		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
9	1.26E-15	5.5%		
	2.04E-07		IE-POS7-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside CNV - POS7
	1.20E-03		CFDS--HOV-0022X-FTO-N	HOV 0022X CNTS CFDS CONTAINMENT ISOLATION VALVE FAILS TO OPEN
	5.14E-05		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
10	1.10E-15	4.8%		
	2.24E-07		IE-POS1-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside CNV - POS1
	9.51E-04		CFDS0AAOV-0010X-FTO-N	AOV 0010X CFDS MODULE 1 ISOLATION VALVE FAILS TO OPEN
	5.14E-05		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE

Table 19.1-70: Listing of Candidate Risk Significant Structures, Systems, and Components (Single Module): Low Power and Shutdown Probabilistic Risk Assessment

System	Description	CCDF	CLRF	FVCDF	FVLRF
MPS	Module protection system	Not Met	Met		
Component	**Basic Event Description**	**CCDF**	**CLRF**	**FVCDF**	**FVLRF**
CVCS-HOV-0334X	HOV 0334X CNTS CVCS discharge line containment isolation valve	Not Met	Not Met	Not Met	Met[1]
CVCS-HOV-0335X	HOV 0335X CNTS CVCS discharge line containment isolation valve	Not Met	Not Met	Not Met	Met[1]
ECCS-HOV-0001A	HOV 0001A ECCS reactor vent valve	Not Met	Not Met	Met[1]	Not Met
ECCS-HOV-0001B	HOV 0001B ECCS reactor vent valve	Not Met	Not Met	Met[1]	Not Met
ECCS-HOV-0001C	HOV 0001C ECCS reactor vent valve	Not Met	Not Met	Met[1]	Not Met
ECCS-HOV-0002A	HOV 0002A ECCS reactor recirculation valve	Not Met	Not Met	Met[1]	Not Met
ECCS-HOV-0002B	HOV 0002B ECCS reactor recirculation valve	Not Met	Not Met	Met[1]	Not Met
Human Action	**Description**	**CCDF**	**CLRF**	**FVCDF**	**FVLRF**
CFDS-HFE-0001C	Operator fails to initiate CFDS injection	Not Met	Not Met	Not Met	Met
CVCS-HFE-0001C	Operator fails to initiate CVCS injection	Not Met	Not Met	Met	Not Met
Other Events	**Description**	**CCDF**	**CLRF**	**FVCDF**	**FVLRF**
RBC	Reactor Building crane - POS3, POS5			Met	N/A[2]
Initiator	**Description**	**CCDF**	**CLRF**	**FVCDF**	**FVLRF**
IE-ECCS--ALOCA-RV1	Spurious opening of an ECCS valve - POS1, POS6			Met	Not Met
IE-EDSS--LODC-----	Loss of DC power - POS1, POS6, POS7			Met	Not Met
IE-RCS---ALOCA-IC-	LOCA inside containment - POS1, POS6, POS7			Met	Not Met
IE-CVCS--ALOCA-COC	CVCS LOCA charging line outside CNV - POS1, POS6, POS7			Not Met	Met

Notes:

- Spaces that are greyed out indicate categories in which the criteria do not apply, as described in TR-0515-13952-A.

[1] The criterion is 'Met' with CCFs conservatively included in the calculation of the single component FV.

[2] N/A indicates this event does not result in a large release.

Table 19.1-71: Key Assumptions for the Low Power and Shutdown Probabilistic Risk Assessment

Assumption	Applicable POS	Basis
The refueling cycle of a module is two years, giving a frequency of 0.5 refueling outages per year.	All	Design characteristic
Only the refueling outage is analyzed quantitatively in the LPSD PRA; evolutions such as turbine bypass and controlled shutdown are only discussed qualitatively. Seven POSs are identified for LPSD conditions.	All	Common engineering practice
No credit is taken for heat transfer through containment during containment flooding (i.e., POS1-shutdown and initial cooling) or containment draining (POS6 - heatup).	POS1, POS6	Bounding assumption
Control rod withdrawal and reactivity insertion is not credible during LPSD.	POS1, POS2, POS3, POS4, POS5, POS6	Control rods are disconnected from their drive mechanisms after insertion to prevent premature withdrawal.
Spurious closure of the ECCS valves is not credible after they are opened.	POS2, POS5	Spurious closure is precluded by valve design; separate actions are required to pressurize the control chamber and close the pilot valve. Closure of the valves is also not possible when CVCS is not in service because CVCS flow is required to close the valves.
The inadvertent actuation block (IAB) of the ECCS valves is not credited for reducing the frequency of a spurious valve opening when the module is subcritical (i.e., POS1 and POS6).	POS1, POS6	The IAB is active when the RPV pressure is near operating pressure (i.e., POS7).
Scheduled testing and maintenance on module-specific components (i.e., CVCS pumps) is performed during a POS in which the component is not required.	POS1, POS6	Common engineering practice
The module is transported by the RBC to the refueling area in POS3 and back to the operating bay in POS5; postulated module drops are only considered in the operating area or refueling area of the reactor pool.	POS3, POS5	Bounding assumption that gives the greatest probability of striking another module and tipping horizontally. Also gives the lowest probability that a dropped module lands upright.
If dropped from a height of one foot or less, the probability that the module tips is 0.5, with uncertainty uniformly distributed between 0 and 1. When dropped from greater than one foot, the module is assumed to tip.	POS3, POS5	Engineering judgment based on the design of the CNV support skirt and seismic amplification margin.
A dropped module that tips, falls horizontally to the reactor pool floor and experiences core damage. The CNV is assumed to be damaged and is not credited with preventing the release of radionuclides. The resulting source term is evaluated 48 hours after shutdown, which is approximately the beginning of POS3.	POS3, POS5	Conservative analysis
After the bottom of the CNV is removed, primary coolant communicates with water in the reactor pool through the open RVVs and RRVs and keeps the core covered and cooled.	POS3, POS4, POS5	Engineering judgment
During an RBC lift, the module is kept below the height that could damage the UHS if dropped.	POS3, POS5	Design characteristic
Seismic events during LPSD conditions are only a concern during module transport when the RBC is under load. The seismic risk from a dropped module, however, is overestimated because the fragility analysis was performed with loaded module weighting.	POS3, POS5	Bounding assumption

Table 19.1-71: Key Assumptions for the Low Power and Shutdown Probabilistic Risk Assessment (Continued)

Assumption	Applicable POS	Basis
Internal fires and internal floods have a minimal impact on LPSD conditions because of the limited frequency and duration in each POS, the fail-safe nature of NuScale safety systems, and the very low conditional core damage probability during LPSD conditions.	All	Engineering judgment
External floods have a minimal impact on LPSD conditions because of the limited frequency and duration in each POS, the fail-safe nature of NuScale safety systems, forecasting tools provide ample warning time in most cases to perform a controlled shutdown, and the very low conditional core damage probability during LPSD conditions.	All	Engineering judgment
High winds have a minimal impact on LPSD conditions because of the limited frequency and duration in each POS, the fail-safe nature of NuScale safety systems, forecasting tools provide ample warning time to move a module from the RBC and place it in a safe position, and the very low conditional core damage probability during LPSD conditions.	All	Engineering judgment
Administrative controls will ensure that RBC safety features (e.g., limit switches, interlocks to prevent undesired movement) are functional during module movement	POS3, POS4, POS5	Engineering judgment

Table 19.1-72: Internal Fire Susceptibility During Low Power and Shutdown Plant Operating States

Plant Operating State	Internal Fire Susceptibility
POS1, Shutdown and initial cooling	Systems credited for mitigation of events that occur in this POS are susceptible to fire-induced failures. The probability of a randomly induced internal fire occurring during the short duration of the POS is judged to be sufficiently small to warrant not modeling it explicitly. A challenge associated with this POS is the potential for fire-induced spurious operation of the CVCS makeup pumps that may result in RPV overpressurization at low pressure. Fires are not expected to be capable of causing the spurious operations of the CVCS makeup pump and the valves providing LTOP in the same fire compartments.
POS2, Cooling through containment and module disconnection	Once the ECCS is actuated, reclosing them to terminate passive cooling requires the spurious operation of two solenoid valves for each of the ECCS valves and also requires the spurious operation of a CVCS makeup pump. The components are not expected to be affected by a fire in the same compartment. Similarly, draining the inventory in the CNV would require spurious operation of the CFDS. This would require the spurious operation of multiple solenoid valves, the CFDS pumps, and the nitrogen distribution system. The components are not expected to be affected by a fire in the same compartment.
POS3, Transport and disassembly	An internal fire event may result in a loss of power the crane; however the crane is designed to fail-safe on a loss of power. Mechanical failures dominate the crane failure probability and are not expected to be induced by internal fires. Spurious operation of the crane does not pose a credible threat to an NPM.
POS4, Refueling and maintenance	In this POS all decay heat is being removed by the UHS and accordingly there is no effect from an internal fire during this POS.
POS5, Reassembly, transport, and reconnection	An internal fire event may result in a loss of power the crane; however the crane is designed to fail-safe on a loss of power. Mechanical failures dominate the crane failure probability and are not expected to be induced by internal fires. Spurious operation of the crane does not pose a credible threat to an NPM.
POS6, Heatup	Systems credited for mitigation of events that occur in this POS are susceptible to fire-induced failures. The probability of a randomly induced internal fire occurring during the short duration of the POS is judged to be sufficiently small to warrant not modeling it explicitly. A challenge associated with this POS is the potential for fire-induced spurious operation of the CVCS makeup pumps that may result in RPV overpressurization at low pressure. Fires are not expected to be capable of causing the spurious operations of the CVCS makeup pump and the valves providing LTOP in the same fire compartments.
POS7, Low power operation	Systems credited for mitigation of events that occur in this POS are susceptible to fire-induced failures. The probability of a randomly induced internal fire occurring during the short duration of the POS is judged to be sufficiently small to warrant not modeling it explicitly.

Table 19.1-73: Internal Flooding Susceptibility During Low Power and Shutdown Plant Operating States

Plant Operating State	Internal Flooding Susceptibility
POS1, Shutdown and initial cooling	Systems credited for mitigation of events that occur in this POS are susceptible to flood-induced failures. The probability of a randomly induced internal flood occurring during the short duration of the POS is judged to be sufficiently small to warrant not modeling it explicitly.
POS2, Cooling through containment and module disconnection	In this POS, ECCS is actuated; decay heat is removed by passive core cooling and conduction through the walls of the CNV to the reactor pool. Therefore, there is no effect from an internal flood during this POS.
POS3, Transport and disassembly	An internal flooding event may result in a loss of power the crane, however the crane is designed to fail-safe on a loss of power. Mechanical failures dominate the crane failure probability and are not expected to be induced by internal flooding.
POS4, Refueling and maintenance	This POS involves refueling operations; the core remains in the RPV lower head and the upper vessels are sufficiently distant from the refueling area that the core is not affected by crane operation. In this POS all decay heat is being removed by the UHS and accordingly there is no effect from an internal flood during this POS.
POS5, Reassembly, transport, and reconnection	This POS involves moving the upper vessels out of dry dock for module reassembly. It includes transport to the operating bay. An internal flooding event may result in a loss of power the crane; however the crane is designed to fail-safe on a loss of power. Mechanical failures dominate the crane failure probability and are not expected to be induced by internal flooding.
POS6, Heatup	In this POS, ECCS is isolated. It includes draining the CNV, establishing chemical volume and control system flow, aligning secondary coolant flow, and withdrawing the control rods. Systems credited for mitigation of events that occur in this POS are susceptible to flood-induced failures. The probability of a randomly induced internal flood occurring during the short duration of the POS is judged to be sufficiently small to warrant not modeling it explicitly.
POS7, Low power operation	In POS7, the core reaches criticality and all systems that support power operations are in service except that the turbine is bypassed. Systems credited for mitigation of events that occur in this POS are susceptible to flood-induced failures. The probability of a randomly induced internal flood occurring during the short duration of the POS is judged to be sufficiently small to warrant not modeling it explicitly.

Table 19.1-74: External Flooding Susceptibility During Low Power and Shutdown Plant Operating States

Plant Operating State	External Flooding Susceptibility
POS1, Shutdown and initial cooling	Although this POS is similar in terms of plant response to the full-power PRA, because the time in this POS is limited, the module can be cooled down and in POS2 before any equipment is susceptible to a flood-induced failure. In the event flood levels exceed expectations, secondary cooling can be provided by the passive DHRS to reach POS2. Therefore, external flooding effects were not evaluated for this POS.
POS2, Cooling through containment and module disconnection	Because the module can be maintained in POS2 indefinitely without electric power or operator action, there is no effect from an external flood during this POS.
POS3, Transport and disassembly	In the event of loss of AC power, the RBC brakes will set and stop motion. The RBC is designed with redundant holding brakes so that if one set fails to engage, the other brake automatically holds the load. Because both brake systems are designed and rated to maintain a hoisted load at the maximum allowable crane load, a loss of power will halt operations but not result in a load drop. The module can be maintained in position suspended by the RBC until power is restored and the lift can resume; therefore, external flooding effects were not evaluated for this POS.
POS4, Refueling and maintenance	The RBC operates with the wet hoist in the vicinity of the core to remove reactor vessel internals, and the fuel handling machine moves fuel assemblies between the core and fuel storage racks in the spent fuel pool. Both have fail-safe, redundant brakes so that in the event of loss of AC power, the brakes set and hold the load. The load can be maintained in position suspended by the RBC and wet hoist or fuel handling machine until power is restored and refueling operations can resume; therefore, external flooding effects were not evaluated for this POS.
POS5, Reassembly, transport, and reconnection	In the event of loss of AC power, the RBC brakes will set and stop motion. The RBC is designed with redundant holding brakes so that if one set fails to engage, the other brake automatically holds the load. Because both brake systems are designed and rated to maintain a hoisted load at the maximum allowable crane load, a loss of power will halt operations, but not result in a load drop. The module can be maintained in position suspended by the RBC until power is restored and the lift can resume; therefore, external flooding effects were not evaluated for this POS.
POS6, Heatup	Based on the limited duration of this POS, and the fail-safe nature of the passive NuScale design, external flooding effects were not evaluated for this POS.
POS7, Low power operation	Based on the limited duration of this POS, and the fail-safe nature of the passive NuScale design, external flooding effects were not evaluated for this POS.

Table 19.1-75: High-Wind Susceptibility during Low Power and Shutdown Plant Operating States

Plant Operating State (POS)	Tornado and Hurricane Susceptibility
POS1 Shutdown and Cooling	High-winds events are evaluated in POS1.
POS 2: Cooling through containment	Because the module can be maintained in POS2 indefinitely without electric power or operator action, no SSC are susceptible to high winds in this POS.
POS 3: Transport and disassembly	In the event of loss of AC power, the RBC brakes will set and stop motion. The RBC is designed with redundant holding brakes so that if one set fails to engage, the other brake automatically holds the load. Because both brake systems are designed and rated to maintain a hoisted load at the maximum allowable crane load, a loss of power will halt operations, but not result in a load drop. The module can be maintained in position suspended by the RBC until power is restored and the lift can resume; therefore, high wind effects were not evaluated for this POS.
POS 4: Refueling and maintenance	The RBC operates with the wet hoist in the vicinity of the core to remove reactor vessel internals, and the fuel handling machine moves fuel assemblies between the core and fuel storage racks in the spent fuel pool. Both have fail-safe, redundant brakes so that in the event of loss of AC power, the brakes set and hold the load. The load can be maintained in position suspended by the RBC and wet hoist or fuel handling machine until power is restored and refueling operations can resume; therefore, high wind effects were not evaluated for this POS.
POS 5: Reassembly, transport, and reconnection	In the event of loss of AC power, the RBC brakes will set and stop motion. The RBC is designed with redundant holding brakes so that if one set fails to engage, the other brake automatically holds the load. Because both brake systems are designed and rated to maintain a hoisted load at the maximum allowable crane load, a loss of power will halt operations, but not result in a load drop. The module can be maintained in position suspended by the RBC until power is restored and the lift can resume; therefore, high wind effects were not evaluated for this POS.
POS 6: Heatup	Based on the limited duration of this POS, and the fail-safe nature of the passive NuScale design, high wind effects were not evaluated for this POS.
POS 7: Low power operation	High-winds events are evaluated in POS7.

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.	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 CVCS to replenish lost inventory for certain beyond design basis events. Although the PRA currently models the DWS as the supply source to the 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.	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.	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.	Yes[1]
Liquid Radioactive Waste Management System	12	Collects, processes, and stores liquid waste; includes radioactive and nonradioactive subsystems.	Liquid radwaste is associated with the ability to inject boron and demineralized water into a module when needed during normal operation. An inability to inject boron when needed constitutes a loss of defense-in-depth for the safety function of reactivity control. In an emergency, boron could be added without the support of liquid radwaste letdown. Furthermore, reactivity control is ultimately provided by the RTS in the event of a plant upset.	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
Gaseous Radioactive Waste Management System	12	Collects, processes, and stores gaseous waste.	This system does not serve a function related to the avoidance of core damage.	No
Solid Radioactive Waste Management System	12	Collects, processes, and stores solid waste.	This system does not serve a function related to the avoidance of core damage.	No
Radioactive Waste Drain System	12	Collects fluid from potentially radioactive drains.	This system does not serve a function related to the avoidance of core damage.	No
Radwaste Building HVAC System	12	Provides heating, ventilation, and air conditioning for the Radioactive Waste Building.	This system does not serve a function related to the avoidance of core damage.	No
Spent Fuel Pool Cooling System	12	Cooling water system transferring heat generated by spent fuel assemblies in the spent fuel pool to the site cooling water system.	Spent fuel pool cooling serves an indirect, supporting function for fuel assembly heat removal by providing heat transfer from the spent fuel pool.	No
Pool Cleanup System	12	Draws water from the RXB pool and the spent fuel pool and removes impurities to reduce radiation dose and maintain water chemistry and clarity.	This system does not serve a function related to the avoidance of core damage.	No
Reactor Pool Cooling System	12	Cooling water system transferring heat from the reactor pool to the site cooling water system.	Reactor pool cooling serves a supporting function for fuel assembly heat removal by offering heat transfer away from the reactor pool in the event the reactor pool is needed as the UHS. Thermal-hydraulic analyses do not credit the system.	No
Pool Surge Control System	12	Controls the volume of water in the RXB pool and spent fuel pool.	This system does not serve a function related to the avoidance of core damage.	No
Ultimate Heat Sink (UHS)	12	Provides a heat sink for the dissipation of residual heat after reactor shutdown or an accident. Includes reactor pool, refueling pool, spent fuel pool and pool liners.	The reactor pool is the source of passive cooling for transferring heat from the fuel to the UHS through the DHRS, ECCS or water that accumulates in the CNV during an accident. The reactor pool also provides cooling to the spent fuel.	Yes
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

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

System	Modules Served	Multiple module function	Accident Mitigation Implication	Credited in model for single module
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	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. 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
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 safe shutdown equipment.	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
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
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 will cause closure of the secondary main steam isolation valves and is considered an initiating event with a trip on all modules. In addition, because each module's makeup combining valve fails to the BAS following a loss of instrument air, the 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

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

System	Modules Served	Multiple module function	Accident Mitigation Implication	Credited in model for single module
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. The auxiliary AC power source can also 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
Low Voltage AC Electrical Distribution System (ELVS)	12	Provides power at 120 VAC and 480 VAC to busses servicing low voltage loads.	The ELVS, although associated with a single module, has loads like DWS which are associated with multiple modules. 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
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.	No (common plant system is not modeled)

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

System	Modules Served	Multiple module function	Accident Mitigation Implication	Credited in model for single module
Normal DC Power 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
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.	Yes[1]
Plant Protection System (PPS)	12	Plant-wide or shared important to safety instrumentation and control systems (e.g., control room habitability actuation).	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

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

System	Modules Served	Multiple module function	Accident Mitigation Implication	Credited in model for single module
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
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).

Table 19.1-77: Multi-Module Adjustment Factors for Initiating Events

Initiating Event	MMAF Description	MMAF	Basis
CVCS--ALOCA-CIC CVCS--ALOCA-COC CVCS--ALOCA-LOC TGS---FMSLB-UD- MSS---ALOCA-SG-	Loss of RCS Inventory, LOCA or pipe break	0.01	These are initiating events associated with a pipe breach, either inside or outside of the CNV. Potential coupling mechanisms include pipe age, manufacturing defects, similar phase transformations, environmental conditions, and water chemistry effects. A MMAF of one percent is assigned to each initiating event based on engineering judgment.
ECCS--ALOCA-RV1 RCS---ALOCA-IC-	Loss of RCS Inventory, not from pipe break	0.1	These are initiating events in which there is a loss of RCS inventory that is not caused by a pipe breach. Examples of events include spurious opening of valves or induced leaks. Potential coupling mechanisms (or items which reduce coupling) include environmental conditions, manufacturing errors, maintenance errors, and mechanical or electrical deficiencies for control or performance purposes. A MMAF of ten percent is assigned to each initiating event based on engineering judgment.
EDSS-LODC-----	CCF initiating event	0.3	Transients that result from CCFs within one module are represented by this category. Such a transient is represented by a loss of DC power caused by a CCF to at least two DC power busses that provide power to one module. These failures satisfy the reactor trip logic causing a reactor trip and the initiation of the ECCS. Potential coupling mechanisms include electronic and mechanical functional faults, environmental and site wide conditions, spatial considerations, and test and maintenance issues. A commonly used beta factor for CCF analysis is ten percent. Therefore, a conservative estimate of thirty percent for the MMAF is applied as a conditional probability of CCF extension to two or more modules given a CCF in one module.
EHVS--LOOP-----	Site-wide event	1.0	Initiating events that the site are grouped into this classification, e.g., a LOOP. Coupling mechanisms are due to weather-related outages (e.g., same location or conditions), grid-related issues (e.g., shared equipment), switchyard centered issues (e.g., shared equipment, spatial considerations, human activities) and plant-centered (e.g., shared component failures, electromagnetic interference, environmental conditions, human activities, and spatial considerations). A MMAF of one hundred percent is assigned.
TGS---TRAN-NPC	General Reactor Trip	0.1	Transients causing an upset condition involving an unplanned reactor trip are represented by the “general reactor trip”; such events include loss of component cooling water, loss of feedwater, loss of service water, loss of condenser heat sink, and general transients. Component cooling water and service water are shared systems. The FWS is largely specific to each module, but there is a shared water supply outside of the reactor and turbine generator buildings. The condenser heat sinks on each turbine are module specific. General transients are deemed to primarily impact individual modules. Because the “general reactor trip” initiating event frequency dominates this group, a factor of ten percent is assigned to the MMAF. The ten percent factor is a commonly used beta factor used to account for coupling mechanisms in CCF analysis.

Table 19.1-78: MMAFs and MMPSF for Basic Events

Multi-Module Classification	MMAF Value	Basis
Single Failure Basic Event	0.1	Potential coupling of independent single failures in each module affecting multiple modules; value based on commonly used beta factor.
CCF Basic Event	0.3	Potential coupling of failures in a short time period due to a single shared cause; value based on conservative application of commonly used beta factor.
Shared SSC Failure Basic Event	1.0	To be classified as a shared SSC for the MM PRA, the failure event affects two or more modules simultaneously. The MMAF is 1.0 by definition.
CCF Involving Shared Equipment Basic Event	1.0	The MMAF is used to model shared redundant SSC. The MMAF is 1.0 by definition.
HFE Involving Shared Systems	1.0	The MMAF represents operator action affecting shared equipment. The MMAF is 1.0 by definition.
Similar Plant Response Basic Events	1.0	Represents similar response of all modules. There is one event recovery of offsite power prior to depletion of backup battery power. The MMAF is 1.0 by definition.
Physical Parameter Basic Events	1.0	Represents common deterministic design response, e.g., actuation setpoint. The MMAF is 1.0 by definition.
Passive Safety System Reliability ECCS events	1.0	Represents passive ECCS MMAF for multiple modules. The MMAF is 1.0 based on engineering judgment.
Passive Safety System Reliability DHRS events	0.1	Represents passive DHRS MMAF for multiple modules. The MMAF is based on engineering judgment.
Test and Maintenance	0.1 to 1.0	Represents coupling of test and maintenance activities. The MMAF is the same as the MMAF applied to equipment for which test and maintenance events are associated (As indicated below, the MMAF associated with human errors committed as a result of test and maintenance activities corresponds to the equipment for which it pertains. Events categorized as an HFE MMPSF are an HFE MMPSF for test and maintenance events as well).
SGTF basic event	0.1	Represents common SGTF causes. Based on engineering judgment of uncertainty associated with the causes, the MMAF is an order of magnitude higher than pipe break MMAF.
CVCS Pipe Break Location/Size Events	1.0	Represents common physical conditions and response. The MMAF is based on engineering judgment.
RSV Demand Probability Event	1.0	Represents common physical conditions and response. The MMAF is based on engineering judgment.
Multi-module Classification	**MMPSF Value**	**Basis**
Human Failure Events	10	Performance shaping factor to account for additional stresses or complexities of servicing a multiple module configuration.

Table 19.1-79: Significant Cutsets (Multi-Module, Full-Power)

Cutset	Prob/Freq	Contribution	Basic Event	Description
MM-CDF Cutsets				
1	6.05E-12	17.0%		
	2.00E-03		IE-RCS---ALOCA-IC-	LOCA Inside Containment
	1.00E+00		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	3.00E-01		MM-ECCS--HOV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: ECCS--HOV-1CC22-FTO-S
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E-01		MM-IE-RCS---ALOCA-IC-	LOCA-NPBK MMAF FOR BASIC EVENT: IE-RCS---ALOCA-IC-
	1.00E+01		MMPSF-HFE-IND	HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
2	2.98E-12	8.4%		
	2.00E-03		IE-RCS---ALOCA-IC-	LOCA Inside Containment
	1.00E+00		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	1.24E-06		ECCS--HOV-1CC33-FTO-S	CCF OF 3 OF 3 ECCS REACTOR VENT VALVES FAIL TO OPEN
	3.00E-01		MM-ECCS--HOV-1CC33-FTO-S	CCF MMAF FOR BASIC EVENT: ECCS--HOV-1CC33-FTO-S
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E-01		MM-IE-RCS---ALOCA-IC-	LOCA-NPBK MMAF FOR BASIC EVENT: IE-RCS---ALOCA-IC-
	1.00E+01		MMPSF-HFE-IND	HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
3	9.28E-13	2.6%		
	1.60E-02		IE-TGS---TRAN--NSS	Loss of Support System
	1.38E-05		DHRS--HOV-1CC44-FTO-S	CCF OF 4 OF 4 DHRS ACTUATION VALVES FAIL TO OPEN
	3.00E-01		MM-DHRS--HOV-1CC44-FTO-S	CCF MMAF FOR BASIC EVENT: DHRS--HOV-1CC44-FTO-S
	1.00E+00		MM-IE-TGS---TRAN--NSS	NSSIE MMAF FOR BASIC EVENT: IE-TGS---TRAN--NSS
	4.68E-05		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
	3.00E-01		MM-RCS---RSV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: RCS---RSV-1CC22-FTO-S
4	8.00E-13	2.3%		
	2.00E-03		IE-RCS---ALOCA-IC-	LOCA Inside Containment
	1.00E+00		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	1.00E-07		ECCS--SYS-0001X-PTH-S	HEAT TRANSFER TO REACTOR POOL FAILS
	1.00E+00		MM-ECCS--SYS-0001X-PTH-S	SHARED MMAF FOR BASIC EVENT: ECCS--SYS-0001X-PTH-S
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E-01		MM-IE-RCS---ALOCA-IC-	LOCA-NPBK MMAF FOR BASIC EVENT: IE-RCS---ALOCA-IC-
	1.00E+01		MMPSF-HFE-IND	HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS

Table 19.1-79: Significant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
5	6.91E-13	1.9%		
	4.70E-05		IE-EDSS--LODC-----	Loss of DC Power
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	3.00E-01		MM-ECCS--HOV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: ECCS--HOV-1CC22-FTO-S
	2.16E-01		EDSS--EBD-1CC44-FOP-N	INITIATOR IS CCF OF 4 OF 4 EDSS DC BUSSES TO OPERATE
	3.00E-01		MM-EDSS--EBD-1CC44-FOP-N	CCF MMAF FOR BASIC EVENT: EDSS--EBD-1CC44-FOP-N
	3.00E-01		MM-IE-EDSS--LODC-----	CCFIE MMAF FOR BASIC EVENT: IE-EDSS--LODC-----
6	5.61E-13	1.6%		
	3.10E-02		IE-EHVS--LOOP-----	Loss Of Offsite Power
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	3.00E-01		MM-ECCS--HOV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: ECCS--HOV-1CC22-FTO-S
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	1.00E+00		MM-EHVS--SYS-0001X-FOP-N	PLANT RESPONSE MMAF FOR BASIC EVENT: EHVS--SYS-0001X-FOP-N
	2.94E-01		EHVS00CTG-0003X-FR2-N	CTG 0003X COMBUSTION TURBINE GENERATOR FAILS TO RUN (HOURS 2 - 48)
	1.00E+00		MM-EHVS00CTG-0003X-FR2-N	SHARED MMAF FOR BASIC EVENT: EHVS00CTG-0003X-FR2-N
	4.08E-03		ELVS00DGN-2CC22-FR2-N	CCF OF 2 OF 2 ELVS STANDBY DIESEL GENERATORS FAILING TO RUN (HOURS 2 - 48)
	1.00E+00		MM-ELVS00DGN-2CC22-FR2-N	SHARED CCF MMAF FOR BASIC EVENT: ELVS00DGN-2CC22-FR2-N
	1.00E+00		MM-IE-EHVS--LOOP-----	SITE-WIDE MMAF FOR BASIC EVENT: IE-EHVS--LOOP-----
	5.00E-01		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
7	5.61E-13	1.6%		
	3.10E-02		IE-EHVS--LOOP-----	Loss Of Offsite Power
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	3.00E-01		MM-ECCS--HOV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: ECCS--HOV-1CC22-FTO-S
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	1.00E+00		MM-EHVS--SYS-0001X-FOP-N	PLANT RESPONSE MMAF FOR BASIC EVENT: EHVS--SYS-0001X-FOP-N
	2.94E-01		EHVS00CTG-0003X-FR2-N	CTG 0003X COMBUSTION TURBINE GENERATOR FAILS TO RUN (HOURS 2 - 48)
	1.00E+00		MM-EHVS00CTG-0003X-FR2-N	SHARED MMAF FOR BASIC EVENT: EHVS00CTG-0003X-FR2-N
	4.08E-03		ELVS00DGN-2CC22-FR2-N	CCF OF 2 OF 2 ELVS STANDBY DIESEL GENERATORS FAILING TO RUN (HOURS 2 - 48)
	1.00E+00		MM-ELVS00DGN-2CC22-FR2-N	SHARED CCF MMAF FOR BASIC EVENT: ELVS00DGN-2CC22-FR2-N
	1.00E+00		MM-IE-EHVS--LOOP-----	SITE-WIDE MMAF FOR BASIC EVENT: IE-EHVS--LOOP-----
	5.00E-01		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
	1.00E+00		MM-RCS---RSV-0003A-OPN-S	PARAMETER MMAF FOR BASIC EVENT: RCS---RSV-0003A-OPN-S

Table 19.1-79: Significant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
8	5.51E-13	1.6%		
	3.10E-02		IE-EHVS--LOOP-----	Loss Of Offsite Power
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	3.00E-01		MM-ECCS--HOV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: ECCS--HOV-1CC22-FTO-S
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	1.00E+00		MM-EHVS--SYS-0001X-FOP-N	PLANT RESPONSE MMAF FOR BASIC EVENT: EHVS--SYS-0001X-FOP-N
	2.94E-01		EHVS00CTG-0003X-FR2-N	CTG 0003X COMBUSTION TURBINE GENERATOR FAILS TO RUN (HOURS 2 - 48)
	1.00E+00		MM-EHVS00CTG-0003X-FR2-N	SHARED MMAF FOR BASIC EVENT: EHVS00CTG-0003X-FR2-N
	1.00E+00		ELVS--HFE-0001C-FTS-N	OPERATOR FAILS TO START/LOAD BACKUP DIESEL GENERATORS
	1.00E+00		MM-ELVS--HFE-0001C-FTS-N	SHARED HFE MMAF FOR BASIC EVENT: ELVS--HFE-0001C-FTS-N
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E+00		MM-IE-EHVS--LOOP-----	SITE-WIDE MMAF FOR BASIC EVENT: IE-EHVS--LOOP-----
	5.00E-01		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
9	5.51E-13	1.6%		
	3.10E-02		IE-EHVS--LOOP-----	Loss Of Offsite Power
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	3.00E-01		MM-ECCS--HOV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: ECCS--HOV-1CC22-FTO-S
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	1.00E+00		MM-EHVS--SYS-0001X-FOP-N	PLANT RESPONSE MMAF FOR BASIC EVENT: EHVS--SYS-0001X-FOP-N
	2.94E-01		EHVS00CTG-0003X-FR2-N	CTG 0003X COMBUSTION TURBINE GENERATOR FAILS TO RUN (HOURS 2 - 48)
	1.00E+00		MM-EHVS00CTG-0003X-FR2-N	SHARED MMAF FOR BASIC EVENT: EHVS00CTG-0003X-FR2-N
	1.00E+00		ELVS--HFE-0001C-FTS-N	OPERATOR FAILS TO START/LOAD BACKUP DIESEL GENERATORS
	1.00E+00		MM-ELVS--HFE-0001C-FTS-N	SHARED HFE MMAF FOR BASIC EVENT: ELVS--HFE-0001C-FTS-N
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E+00		MM-IE-EHVS--LOOP-----	SITE-WIDE MMAF FOR BASIC EVENT: IE-EHVS--LOOP-----
	5.00E-01		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
	1.00E+00		MM-RCS---RSV-0003A-OPN-S	PARAMETER MMAF FOR BASIC EVENT: RCS---RSV-0003A-OPN-S
10	4.84E-13	1.4%		
	3.10E-02		IE-EHVS--LOOP-----	Loss Of Offsite Power
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	3.00E-01		MM-ECCS--HOV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: ECCS--HOV-1CC22-FTO-S
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	1.00E+00		MM-EHVS--SYS-0001X-FOP-N	PLANT RESPONSE MMAF FOR BASIC EVENT: EHVS--SYS-0001X-FOP-N

Table 19.1-79: Significant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	2.94E-01		EHVS00CTG-0003X-FR2-N	CTG 0003X COMBUSTION TURBINE GENERATOR FAILS TO RUN (HOURS 2 - 48)
	1.00E+00		MM-EHVS00CTG-0003X-FR2-N	SHARED MMAF FOR BASIC EVENT: EHVS00CTG-0003X-FR2-N
	5.93E-02		ELVS00DGN-0001X-FR2-N	DGN 0001X ELVS STANDBY DIESEL GENERATOR I FAILS TO RUN (HOURS 2 - 48)
	1.00E+00		MM-ELVS00DGN-0001X-FR2-N	SHARED MMAF FOR BASIC EVENT: ELVS00DGN-0001X-FR2-N
	5.93E-02		ELVS00DGN-0002X-FR2-N	DGN 0002X ELVS STANDBY DIESEL GENERATOR II FAILS TO RUN (HOURS 2 - 48)
	1.00E+00		MM-ELVS00DGN-0002X-FR2-N	SHARED MMAF FOR BASIC EVENT: ELVS00DGN-0002X-FR2-N
	1.00E+00		MM-IE-EHVS--LOOP-----	SITE-WIDE MMAF FOR BASIC EVENT: IE-EHVS--LOOP-----
	5.00E-01		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
11	4.84E-13	1.4%		
	3.10E-02		IE-EHVS--LOOP-----	Loss Of Offsite Power
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	3.00E-01		MM-ECCS--HOV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: ECCS--HOV-1CC22-FTO-S
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	1.00E+00		MM-EHVS--SYS-0001X-FOP-N	PLANT RESPONSE MMAF FOR BASIC EVENT: EHVS--SYS-0001X-FOP-N
	2.94E-01		EHVS00CTG-0003X-FR2-N	CTG 0003X COMBUSTION TURBINE GENERATOR FAILS TO RUN (HOURS 2 - 48)
	1.00E+00		MM-EHVS00CTG-0003X-FR2-N	SHARED MMAF FOR BASIC EVENT: EHVS00CTG-0003X-FR2-N
	5.93E-02		ELVS00DGN-0001X-FR2-N	DGN 0001X ELVS STANDBY DIESEL GENERATOR I FAILS TO RUN (HOURS 2 - 48)
	1.00E+00		MM-ELVS00DGN-0001X-FR2-N	SHARED MMAF FOR BASIC EVENT: ELVS00DGN-0001X-FR2-N
	5.93E-02		ELVS00DGN-0002X-FR2-N	DGN 0002X ELVS STANDBY DIESEL GENERATOR II FAILS TO RUN (HOURS 2 - 48)
	1.00E+00		MM-ELVS00DGN-0002X-FR2-N	SHARED MMAF FOR BASIC EVENT: ELVS00DGN-0002X-FR2-N
	1.00E+00		MM-IE-EHVS--LOOP-----	SITE-WIDE MMAF FOR BASIC EVENT: IE-EHVS--LOOP-----
	5.00E-01		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
	1.00E+00		MM-RCS---RSV-0003A-OPN-S	PARAMETER MMAF FOR BASIC EVENT: RCS---RSV-0003A-OPN-S
12	4.43E-13	1.3%		
	1.60E-02		IE-TGS---TRAN--NSS	Loss of Support System
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	3.00E-01		MM-ECCS--HOV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: ECCS--HOV-1CC22-FTO-S
	1.00E+00		MM-IE-TGS---TRAN--NSS	NSSIE MMAF FOR BASIC EVENT: IE-TGS---TRAN--NSS
	7.32E-04		RCS---RSV-0003A-FTC-S	RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
	1.00E-01		MM-RCS---RSV-0003A-FTC-S	SINGLE MMAF FOR BASIC EVENT: RCS---RSV-0003A-FTC-S
	5.00E-01		RCS---RSV-0003A-OPN-S	PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
	1.00E+00		MM-RCS---RSV-0003A-OPN-S	PARAMETER MMAF FOR BASIC EVENT: RCS---RSV-0003A-OPN-S

Table 19.1-79: Significant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
13	4.41E-13	1.2%		
	1.60E-02		IE-TGS---TRAN--NSS	Loss of Support System
	6.55E-06		CRDS--ROD-1CC316FOP-S	GIVEN ACTUATION, AT LEAST 3 OF 16 RODS FAIL TO INSERT
	3.00E-01		MM-CRDS--ROD-1CC316FOP-S	CCF MMAF FOR BASIC EVENT: CRDS--ROD-1CC316FOP-S
	1.00E+00		MM-IE-TGS---TRAN--NSS	NSSIE MMAF FOR BASIC EVENT: IE-TGS---TRAN--NSS
	4.68E-05		RCS---RSV-1CC22-FTO-S	CCF 2 OF 2 RCS REACTOR SAFETY VALVES FAIL TO OPEN
	3.00E-01		MM-RCS---RSV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: RCS---RSV-1CC22-FTO-S
14	3.91E-13	1.1%		
	2.00E-03		IE-RCS---ALOCA-IC-	LOCA Inside Containment
	1.00E+00		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	1.00E-01		ECCS--HOV-0002A-FOP-N	HOV 0002A ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.00E+00		MM-ECCS--HOV-0002A-FOP-N	PARAMETER MMAF FOR BASIC EVENT: ECCS--HOV-0002A-FOP-N
	1.00E-01		ECCS--HOV-0002B-FOP-N	HOV 0002B ECCS REACTOR RECIRCULATION VALVE PASSIVE ACTUATION TO OPEN VALVE FAILS
	1.00E+00		MM-ECCS--HOV-0002B-FOP-N	PARAMETER MMAF FOR BASIC EVENT: ECCS--HOV-0002B-FOP-N
	1.63E-05		ECCS--SOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS RRV TRIP VALVES FAIL TO OPEN
	3.00E-01		MM-ECCS--SOV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: ECCS--SOV-1CC22-FTO-S
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E-01		MM-IE-RCS---ALOCA-IC-	LOCA-NPBK MMAF FOR BASIC EVENT: IE-RCS---ALOCA-IC-
	1.00E+01		MMPSF-HFE-IND	HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
15	3.53E-13	1.0%		
	3.10E-02		IE-EHVS--LOOP-----	Loss Of Offsite Power
	2.52E-06		ECCS--HOV-1CC22-FTO-S	CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
	3.00E-01		MM-ECCS--HOV-1CC22-FTO-S	CCF MMAF FOR BASIC EVENT: ECCS--HOV-1CC22-FTO-S
	4.00E-02		EHVS--SYS-0001X-FOP-N	OFFSITE POWER NOT RESTORED BEFORE BATTERIES DEPLETE
	1.00E+00		MM-EHVS--SYS-0001X-FOP-N	PLANT RESPONSE MMAF FOR BASIC EVENT: EHVS--SYS-0001X-FOP-N
	2.94E-01		EHVS00CTG-0003X-FR2-N	CTG 0003X COMBUSTION TURBINE GENERATOR FAILS TO RUN (HOURS 2 - 48)
	1.00E+00		MM-EHVS00CTG-0003X-FR2-N	SHARED MMAF FOR BASIC EVENT: EHVS00CTG-0003X-FR2-N
	5.93E-02		ELVS00DGN-0001X-FR2-N	DGN 0001X ELVS STANDBY DIESEL GENERATOR I FAILS TO RUN (HOURS 2 - 48)
	1.00E+00		MM-ELVS00DGN-0001X-FR2-N	SHARED MMAF FOR BASIC EVENT: ELVS00DGN-0001X-FR2-N
	4.32E-02		ELVS00DGN-0002X-FTS-N	DGN 0002X ELVS STANDBY DIESEL GENERATOR II FAILS TO START
	1.00E+00		MM-ELVS00DGN-0002X-FTS-N	SHARED MMAF FOR BASIC EVENT: ELVS00DGN-0002X-FTS-N
	1.00E+00		MM-IE-EHVS--LOOP-----	SITE-WIDE MMAF FOR BASIC EVENT: IE-EHVS--LOOP-----

Table 19.1-79: Significant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	5.00E-01		/RCS-T05	RCS Reactor Safety Valve Demanded to Open
MM-LRF Cutsets				
1	1.73E-13	87.9%		
	2.80E-04		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	1.00E+00		CFDS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CFDS INJECTION
	5.14E-05		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	3.00E-01		MM-CVCS--HOV-3CC22-FTC-S	CCF MMAF FOR BASIC EVENT: CVCS--HOV-3CC22-FTC-S
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E-02		MM-IE-CVCS--ALOCA-COC	LOCA-PBK MMAF FOR BASIC EVENT: IE-CVCS--ALOCA-COC
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	1.00E+01		MMPSF-HFE-IND	HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
2	1.30E-14	6.6%		
	1.40E-04		IE-CVCS--ALOCA-LOC	CVCS LOCA Letdown Line Outside Containment
	1.00E+00		CFDS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CFDS INJECTION
	1.00E+00		CVCS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CVCS INJECTION
	5.14E-05		CVCS--HOV-3CC22-FTC-S	CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
	3.00E-01		MM-CVCS--HOV-3CC22-FTC-S	CCF MMAF FOR BASIC EVENT: CVCS--HOV-3CC22-FTC-S
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.50E-01		HEP02	HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
	1.00E-02		MM-IE-CVCS--ALOCA-LOC	LOCA-PBK MMAF FOR BASIC EVENT: IE-CVCS--ALOCA-LOC
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE
	1.00E+01		MMPSF-HFE-IND	HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
3	1.09E-14	5.6%		
	2.80E-04		IE-CVCS--ALOCA-COC	CVCS LOCA Charging Line Outside Containment
	1.00E+00		CFDS--HFE-0001C-FOP-N	OPERATOR FAILS TO INITIATE CFDS INJECTION
	1.00E-01		CVCS--PIP-0001X-BRK-N	CVCS LOCA DOES NOT INITIATE EXCESS FLOW CHECK VALVE
	4.00E-03		HEP01	HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
	1.00E-02		MM-IE-CVCS--ALOCA-COC	LOCA-PBK MMAF FOR BASIC EVENT: IE-CVCS--ALOCA-COC
	1.00E+00		LRCDSPLIT	CORE DAMAGE MAPPED TO RELEASE

Table 19.1-79: Significant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Prob/Freq	Contribution	Basic Event	Description
	1.00E+01		MMPSF-HFE-IND	HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
	3.26E-06		MPS---APL-5CC22-FOP-S	CCF OF 2 OF 2 APL MODULES IN CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES
	3.00E-01		MM-MPS---APL-5CC22-FOP-S	CCF MMAF FOR BASIC EVENT: MPS---APL-5CC22-FOP-S

Table 19.1-80: Summary of Results (Mean Values)

Hazard	CDF (per mcyr)	LRF (per mcyr)	Applicable Section
Full Power			
Internal Events	3.0E-10	2.3E-11	Section 19.1.4.1.2 and Section 19.1.4.2.2
Internal Fires	9.7E-10	4.3E-11	Section 19.1.5.2.2
Internal Floods	6.1E-11	<1E-15	Section 19.1.5.3.2
External Floods	8.7E-10	7.9E-14	Section 19.1.5.4.2
High Winds (Tornado)	9.9E-11	<1E-15	Section 19.1.5.5.2
High Winds (Hurricane)	7.2E-10	6.4E-14	Section 19.1.5.5.2
Seismic (SMA)	0.88g[1]	0.88g[1]	Section 19.1.5.1.2
Low Power and Shutdown			
Hazard	**CDF (per year)**	**LRF (per year)**	**Applicable Section**
Internal Events	4.9E-13	2.0E-14	Section 19.1.6.2
Module Drop	8.8E-08	N/A[2]	Section 19.1.6.2
Internal Fires	Negligible	Negligible	Section 19.1.6.3.2
Internal Floods	Negligible	Negligible	Section 19.1.6.3.3
External Floods	Negligible	Negligible	Section 19.1.6.3.4
High Winds (Tornado)	1.4E-13[4]	<1E-15[4]	Section 19.1.6.3.5
High Winds (Hurricane)	1.0E-12[4]	<1E-15[4]	Section 19.1.6.3.5
Seismic (SMA)	Negligible	Negligible	Section 19.1.6.3.1
Multi-Module			
Hazard	**Conditional Probability of Core Damage**	**Conditional Probability of Large Release**	**Applicable Section**
Multi-Module Factor	0.13[3]	0.01[3]	Section 19.1.7.2
Composite CCFP < 0.1			

Notes**:**

[1] A seismic margins assessment was performed; results are presented in terms of the HCLPF (i.e., peak ground acceleration at which there is 95% confidence that the conditional failure probability is less than 5 percent). Note that these results are driven by the bounding assumption that a structural failure results in both core damage and a large release.

[2] A module drop does not result in a large release.

[3] Results are presented in terms of a bounding estimate on the conditional probability that multiple modules would experience core damage (or large release) following core damage (or large release) in a single module.

[4] Results are point estimates.

Table 19.1-81: Multi-Module Considerations for External Events

SSC	Modules served	Seismic	Internal Fire	Internal Flood	External Flood	High Winds
CTG and BDG	12	Note 1	Yes	None	Yes	Yes
RTS	1	Note 1	None	None	None	None
DHRS	1	Note 1	Yes[2]	None	None	None
RSV	1	Note 1	None	None	None	None
ECCS	1	Note 1	None	None	None	None
CVCS	1	Note 1	Yes[3]	Yes[3]	Yes[4]	Yes[4]
CFDS	6 x 2	Note 1	Yes[5]	Yes[5]	Yes[4]	Yes[4]
CIV	1	Note 1	Yes[2]	None	None	None

Notes:

1. Seismic events have the potential to produce correlated SSC failures in multiple modules.
2. Multiple hot shorts could affect multiple modules.
3. Pumps for modules 1-6 are in one area; pumps for modules 7-12 are in another area. Suction is provided by systems shared across all modules.
4. If hazard results in a loss of all AC power, system is unavailable (e.g., pump motive power).
5. Modules 1-6 are serviced by one subsystem; modules 7-12 are serviced by a different subsystem.

Figure 19.1-1: Master Logic Diagram for Initiating Events

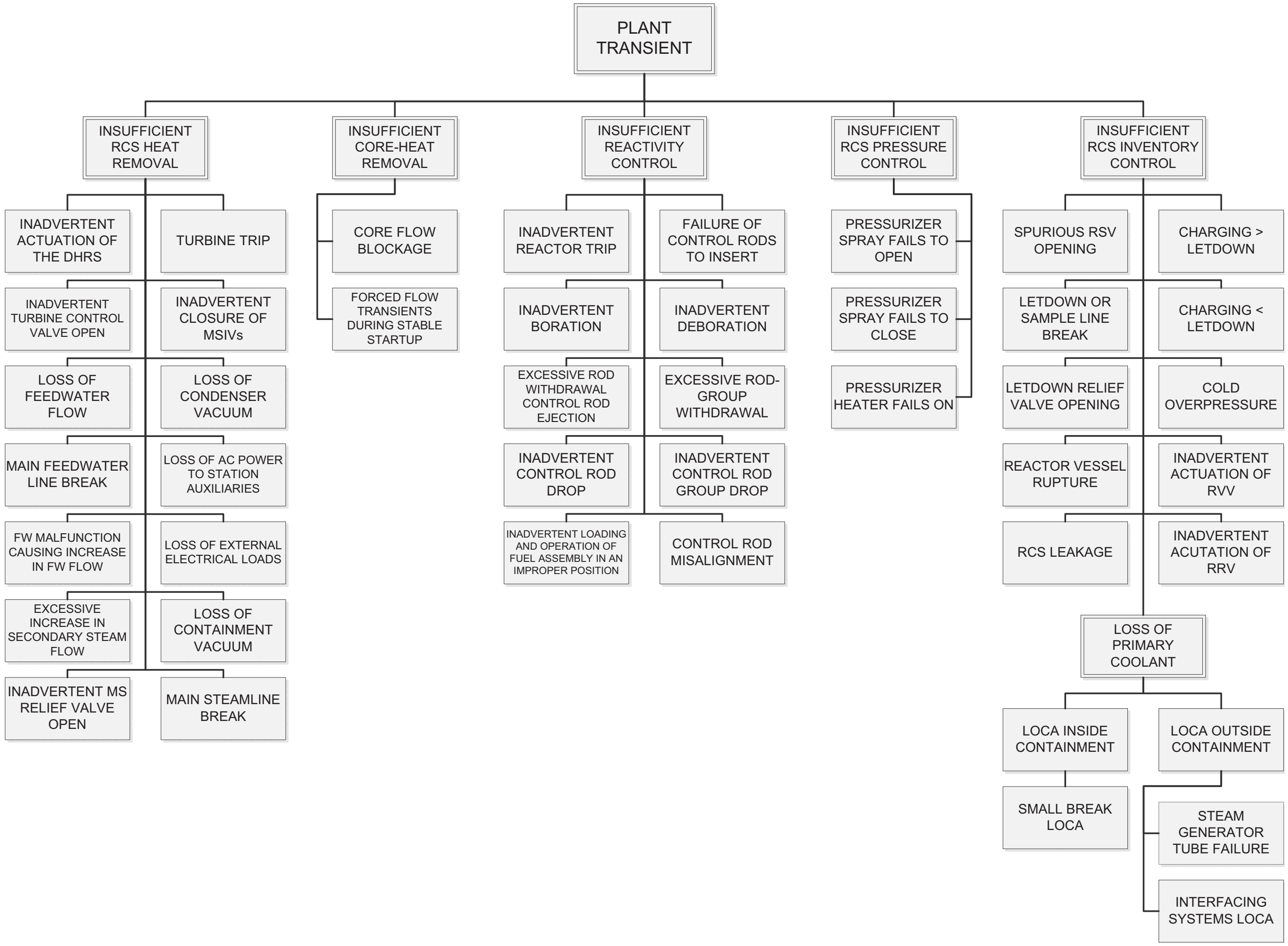


Figure 19.1-2: Event Tree for Chemical and Volume Control System Charging Line Pipe Break Outside Containment

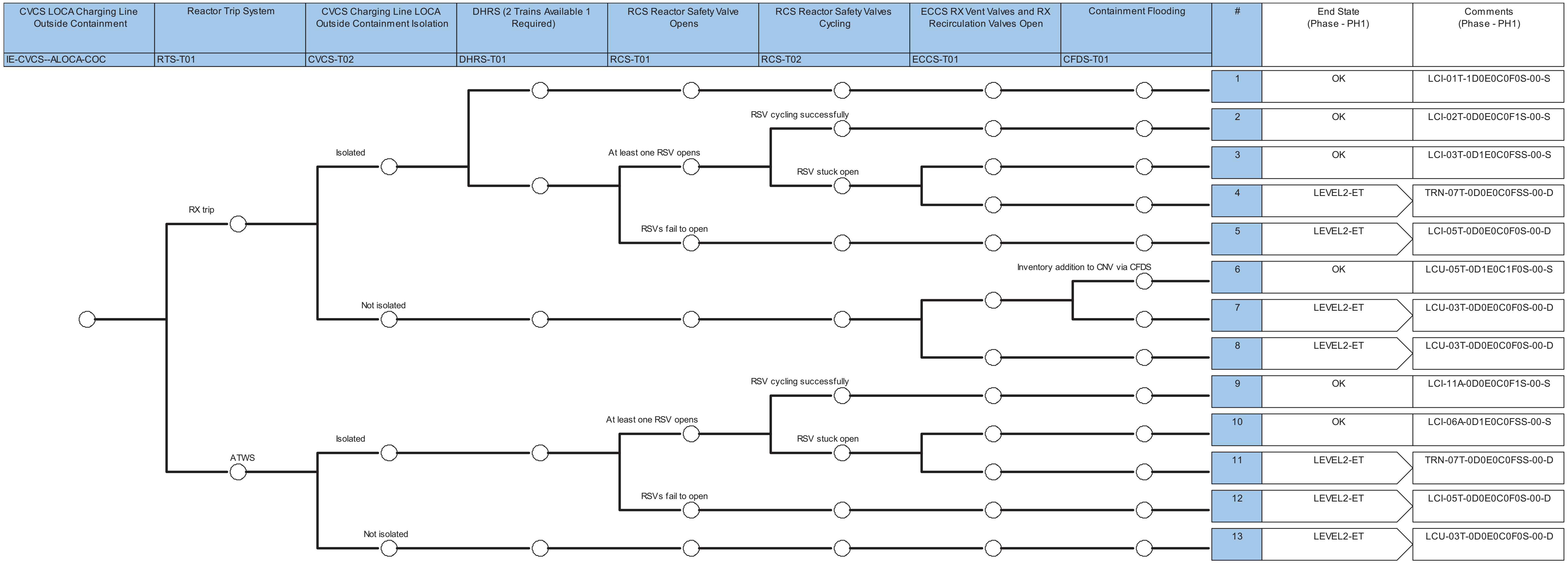


Figure 19.1-3: Event Tree for Chemical and Volume Control System Letdown Line Pipe Break Outside Containment

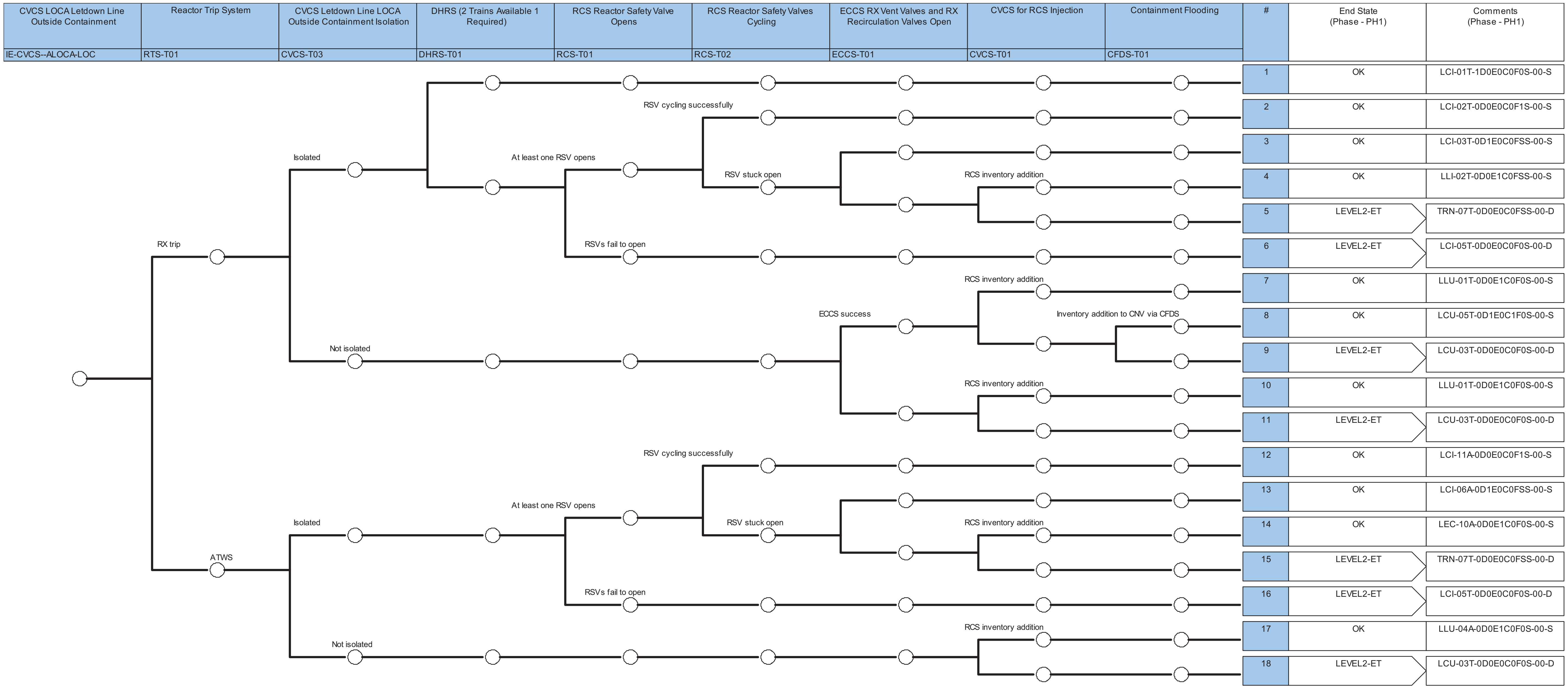


Figure 19.1-4: Event Tree for Chemical and Volume Control System Charging Line Loss-of-Coolant Accident Inside Containment

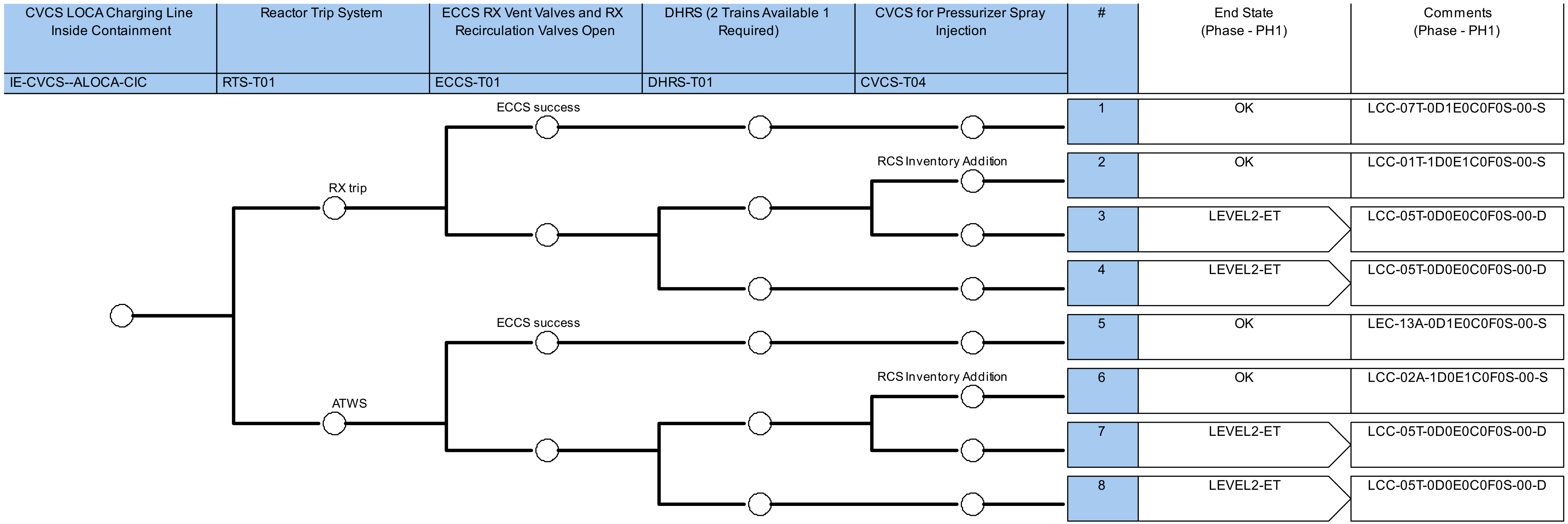


Figure 19.1-5: Event Tree for Reactor Coolant System Loss-of-Coolant Accident Inside Containment

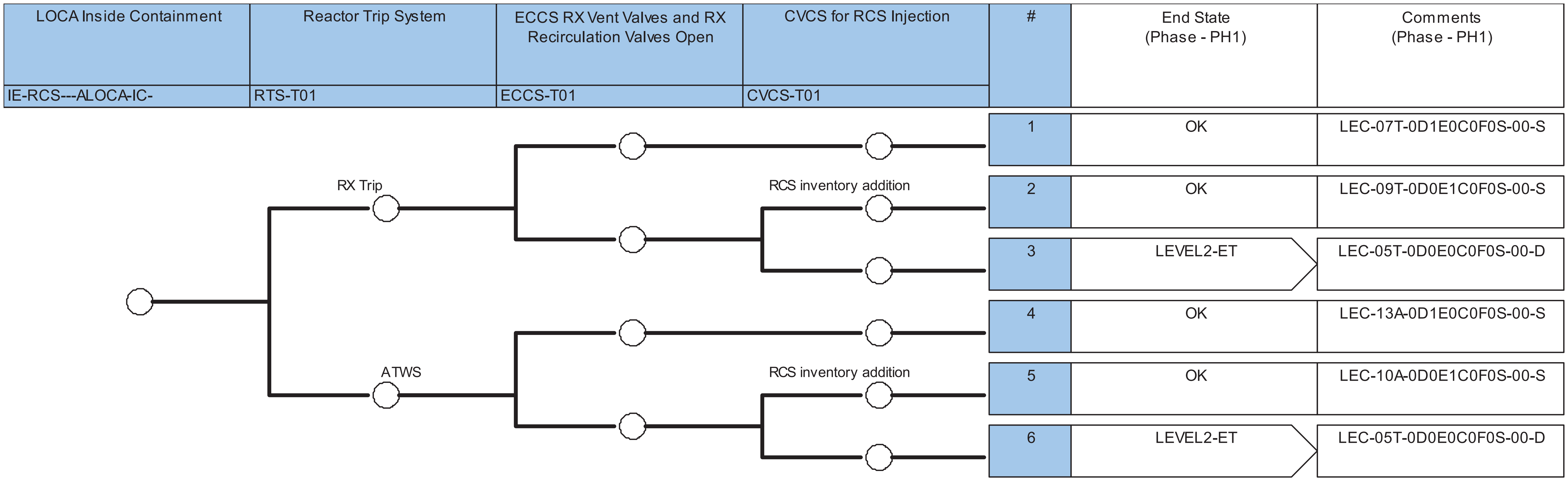


Figure 19.1-6: Event Tree for Spurious Opening of an Emergency Core Cooling System Valve

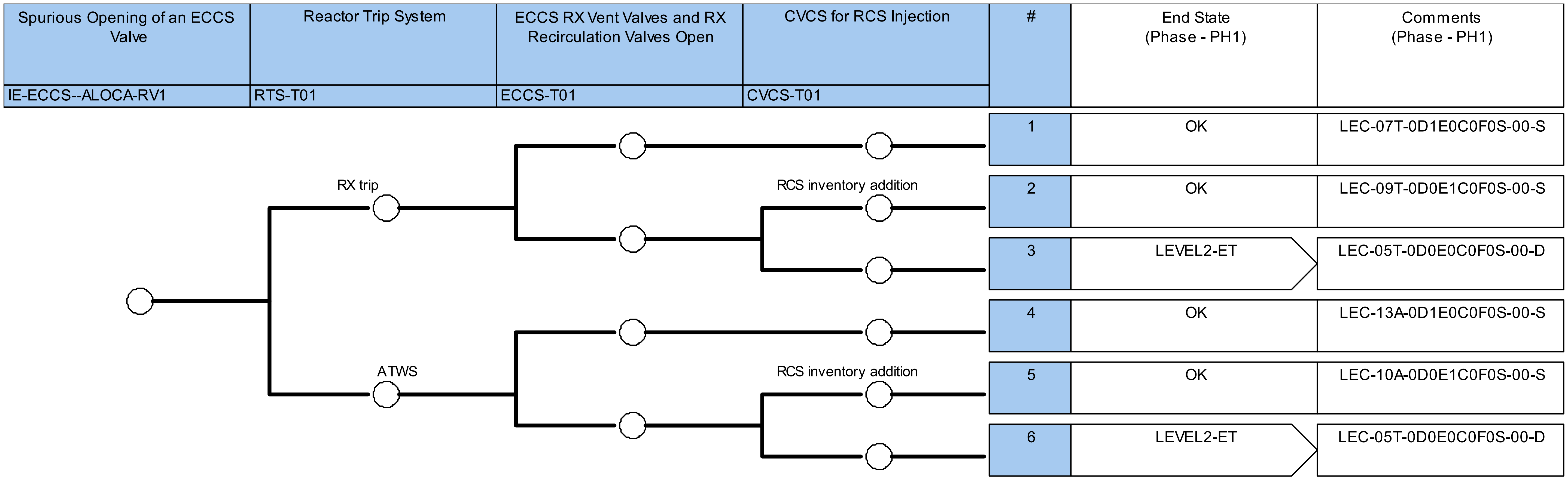


Figure 19.1-7: Event Tree for Steam Generator Tube Failure

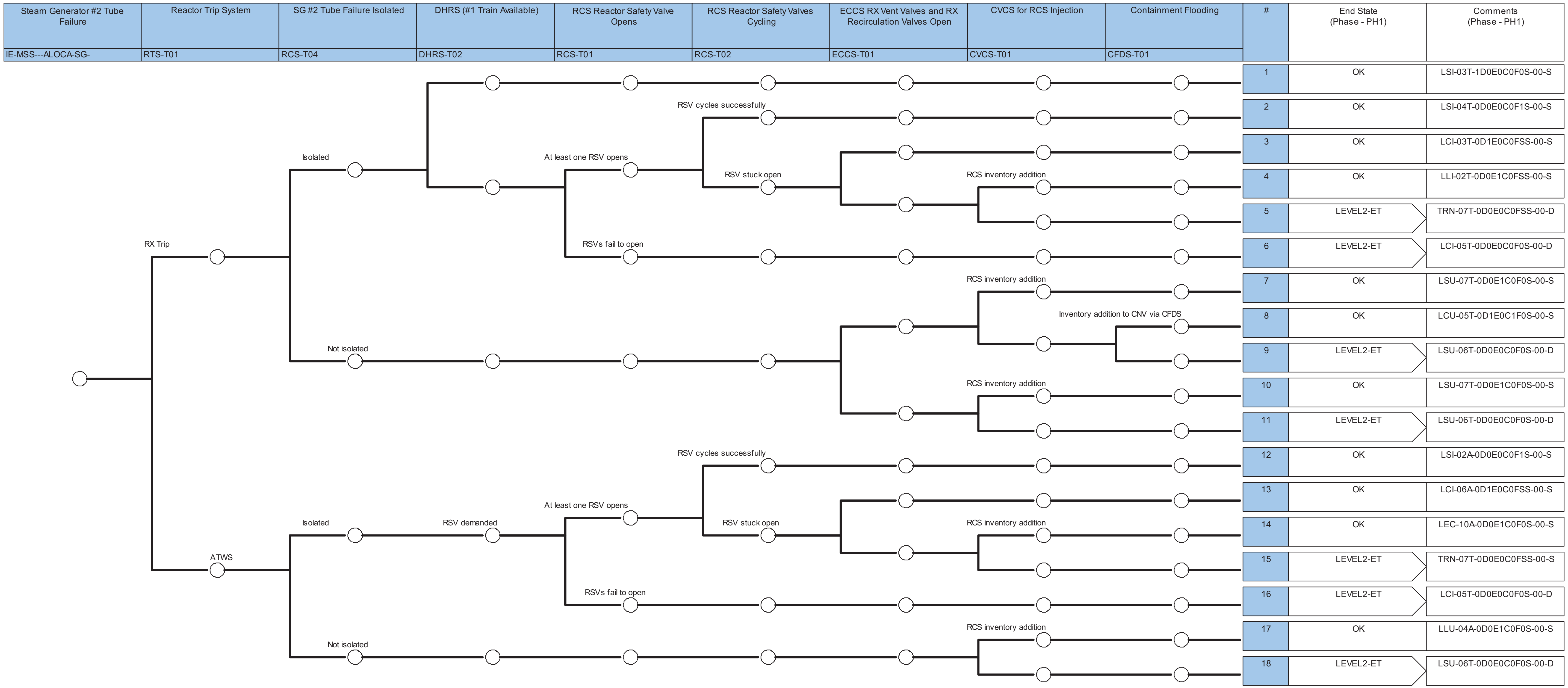


Figure 19.1-8: Event Tree for Secondary Line Break

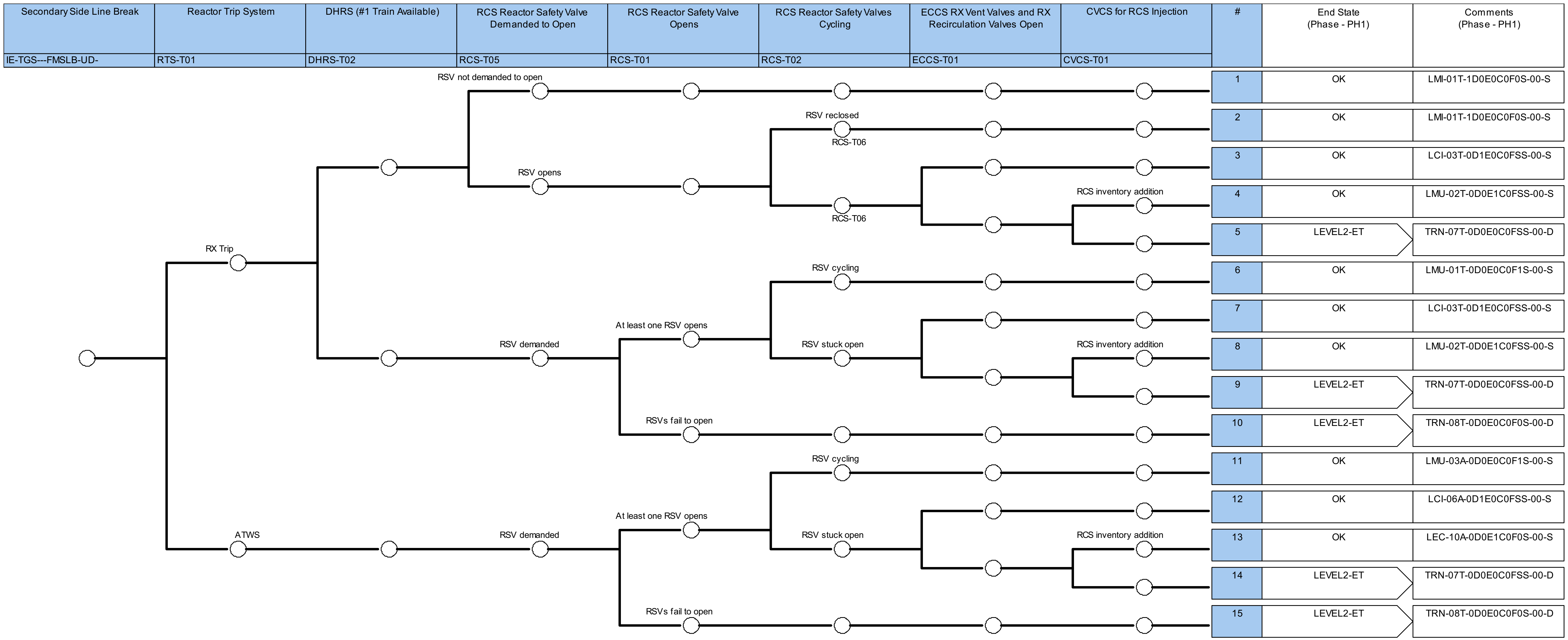


Figure 19.1-9: Event Tree for Loss of Offsite Power

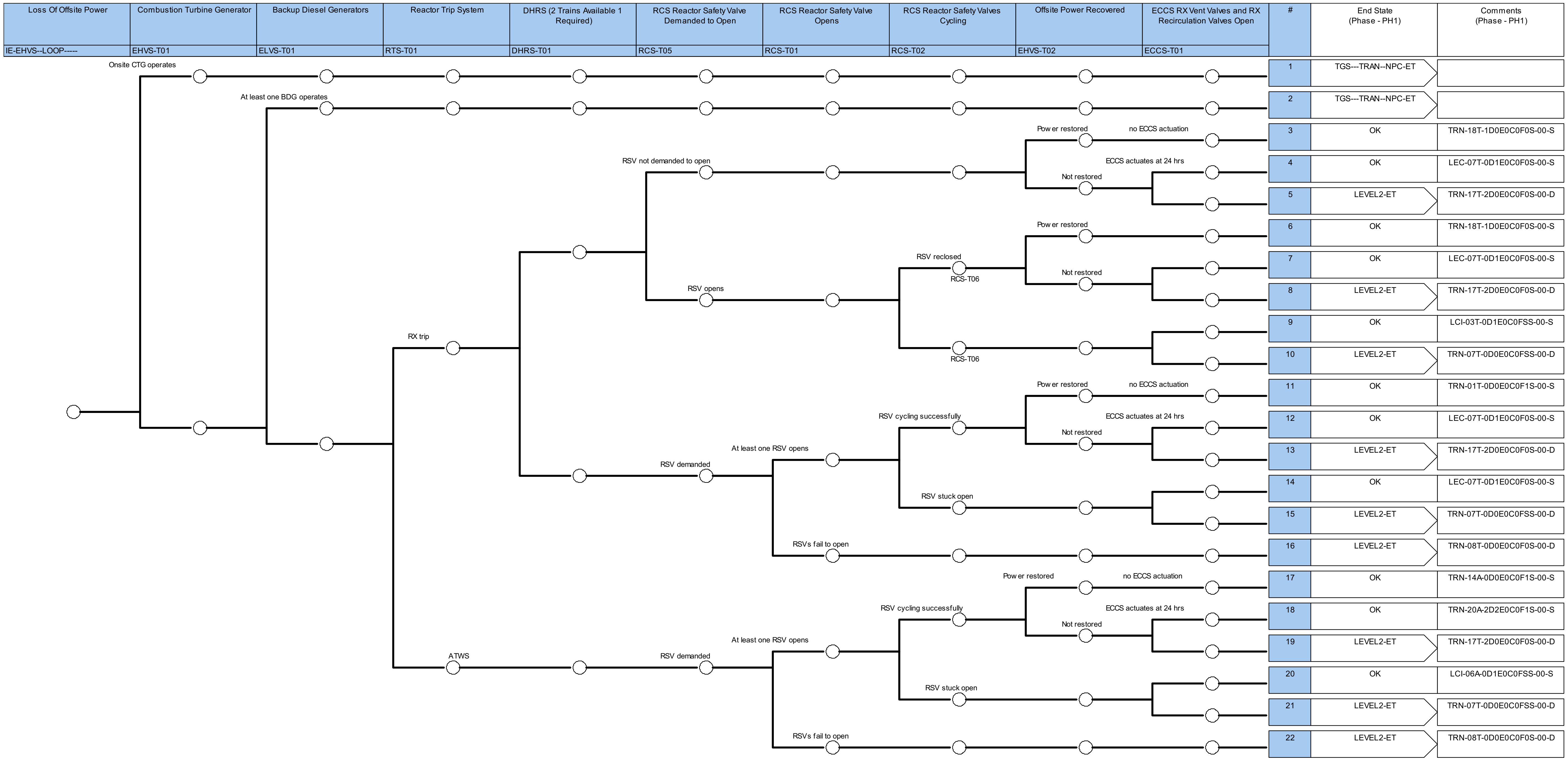


Figure 19.1-10: Event Tree for Loss of Direct Current Power

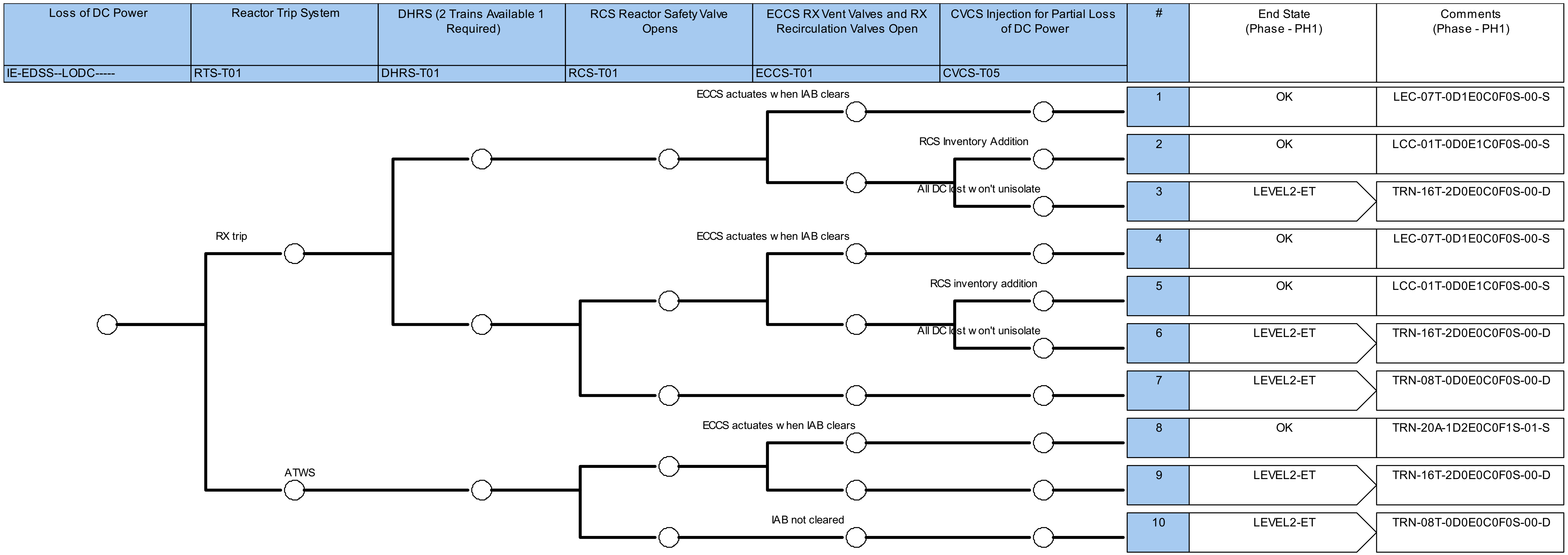


Figure 19.1-11: Event Tree for General Transient

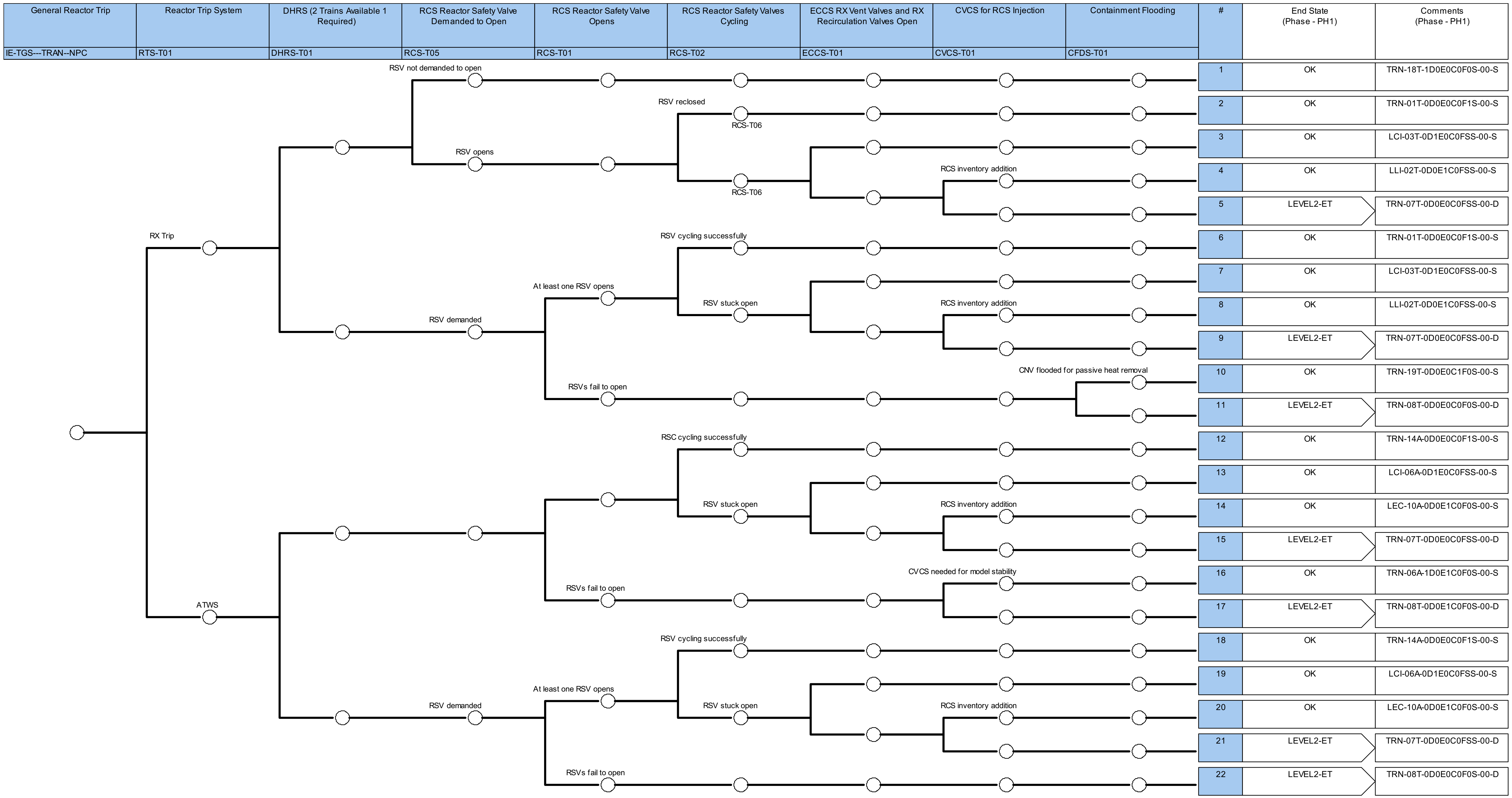


Figure 19.1-12: Event Tree for Loss of Support System

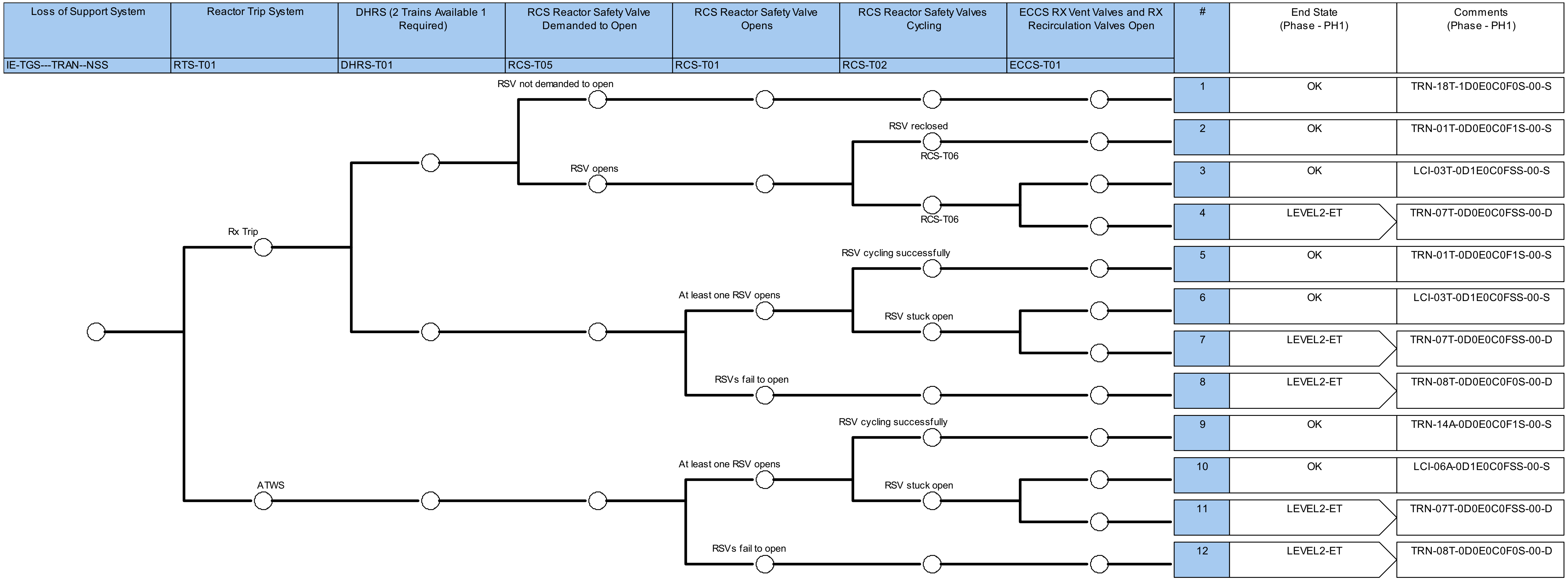


Figure 19.1-13: Contribution to Internal Events Core Damage Frequency by Initiator

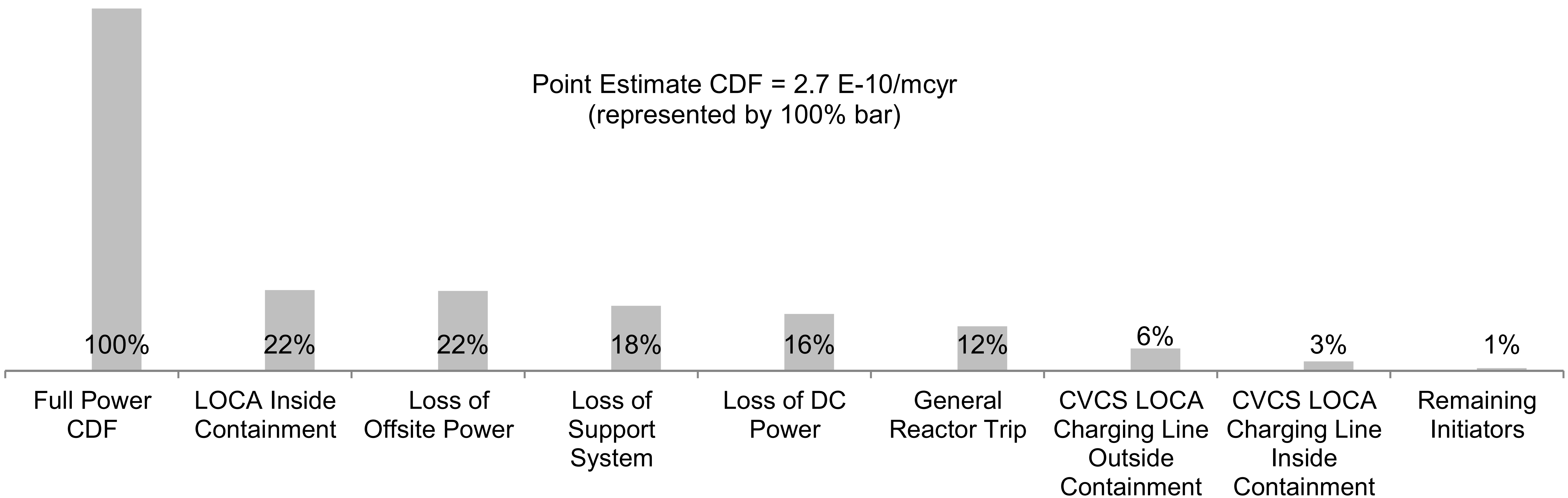


Figure 19.1-14: Contribution to Internal Events Large Release Frequency by Initiator

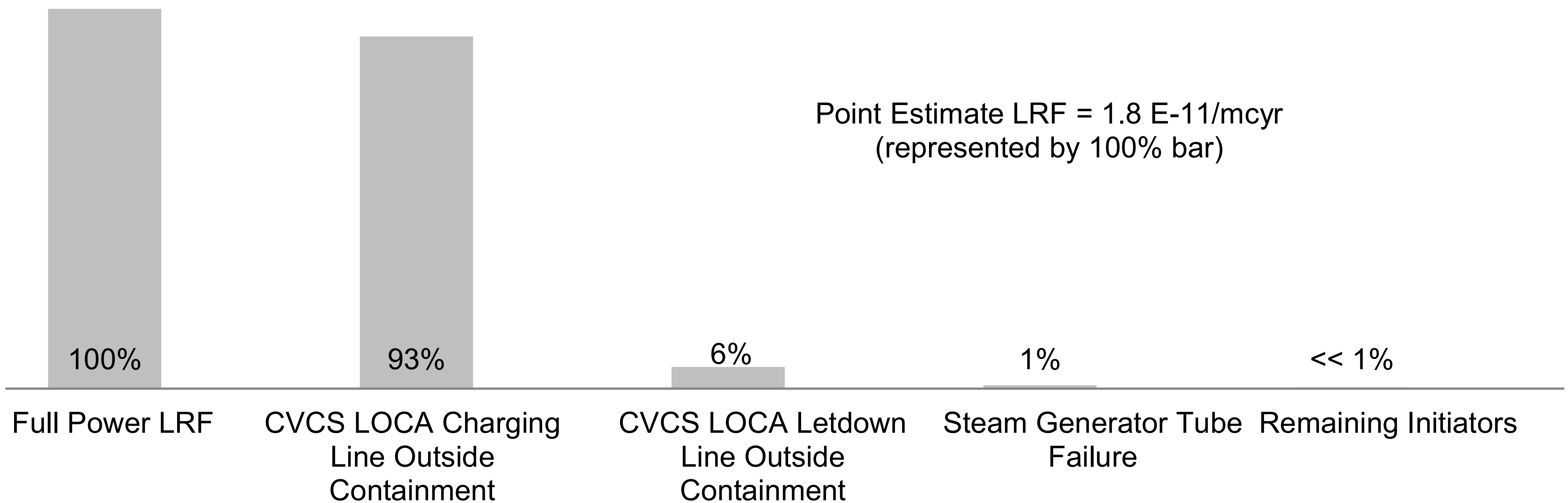


Figure 19.1-15: Containment Event Tree

Core Damage Sequences	Core Damage Cutset Mapped to Release Size	Containment Isolation - CIVs Close	#	End State (Phase - PH1)	Comments (Phase - PH1)
CD	CD-T01	CNTS-T01			
			1	CD	Core Damage
			2	NR	RC1:CD with Isolation
			3	LR	RC2:CD with Release

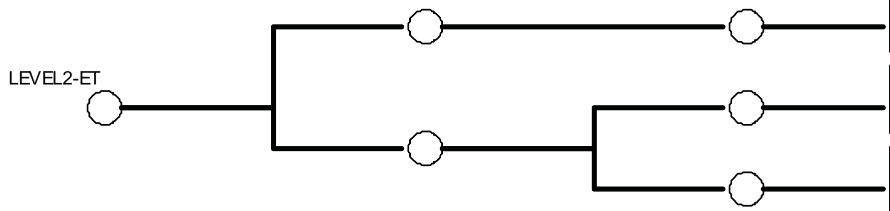


Figure 19.1-16: Representative Seismic Event Tree

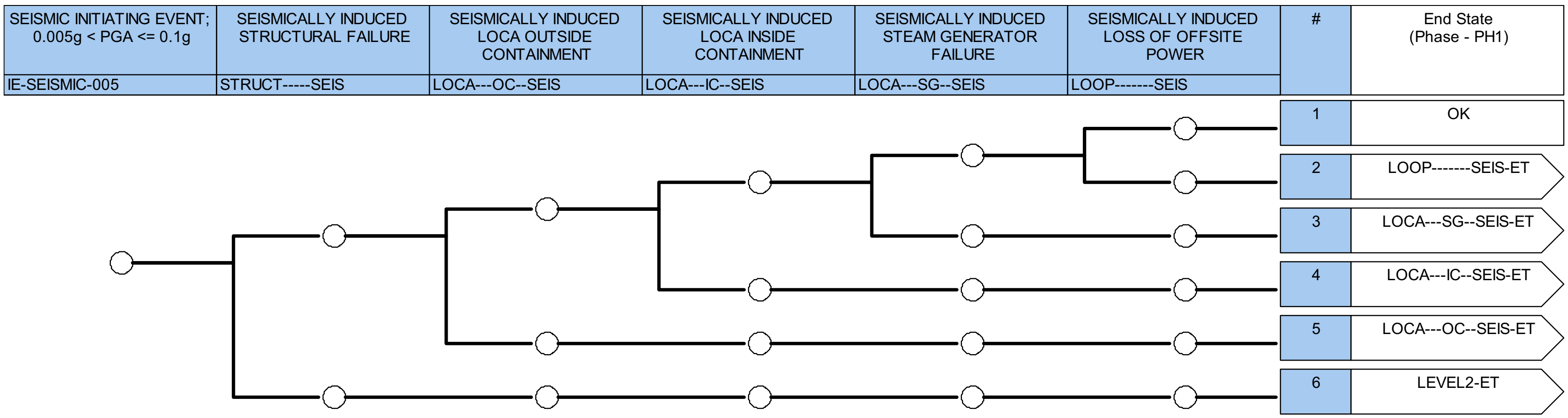


Figure 19.1-17: Seismically Induced Break Outside Containment Event Tree

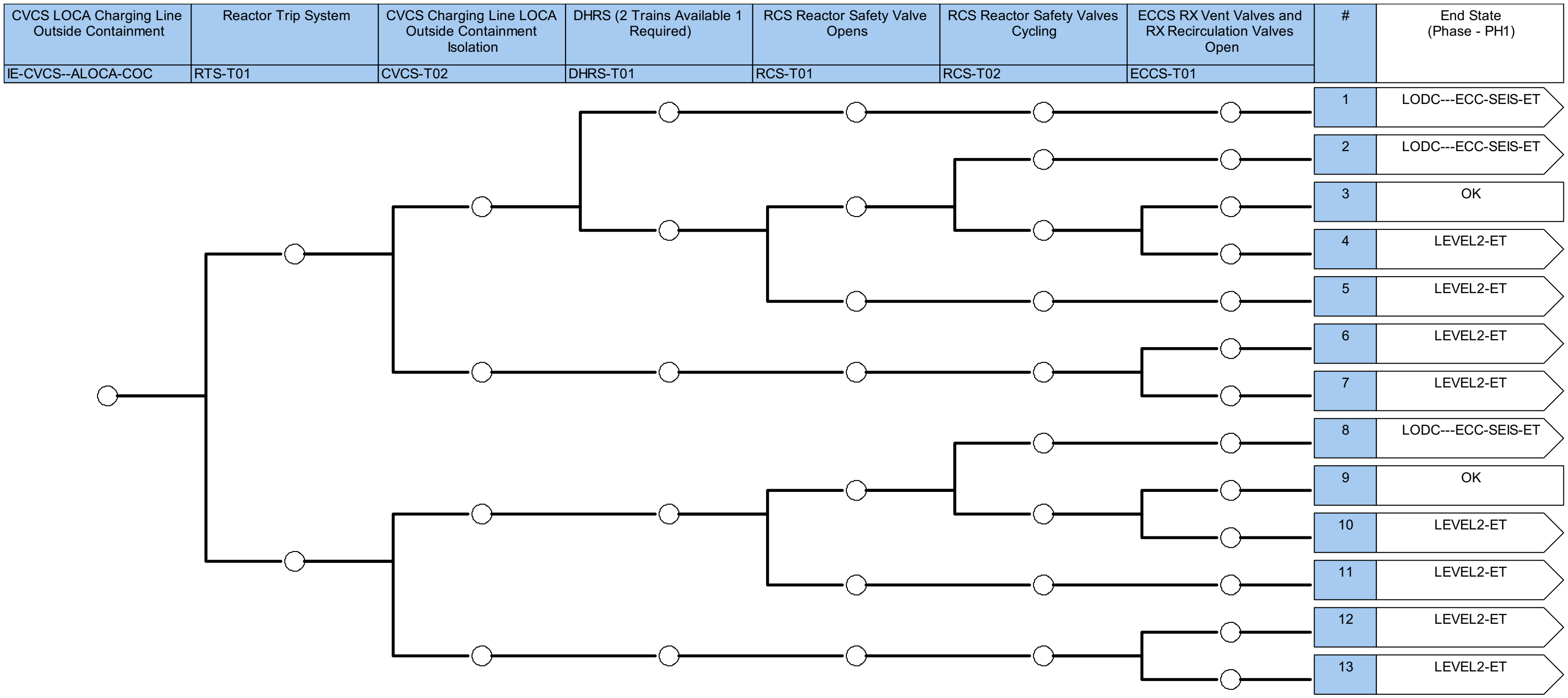


Figure 19.1-18: Seismically Induced Loss-of-Coolant Accident Inside Containment Event Tree

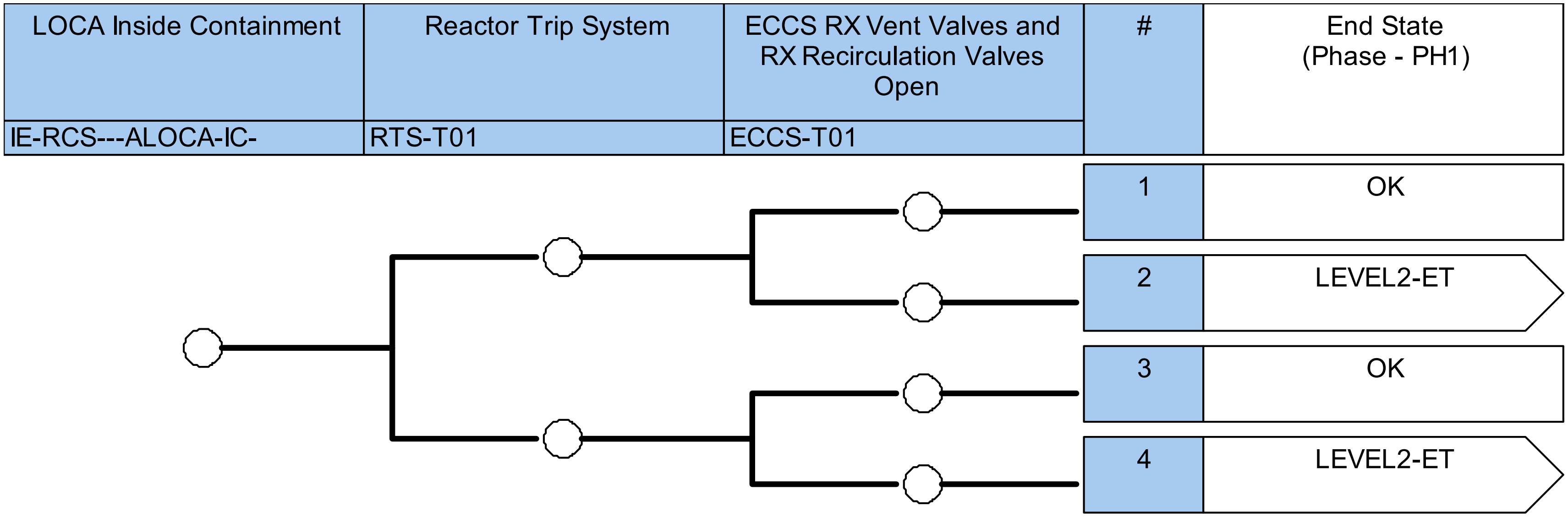


Figure 19.1-19: Seismically Induced Steam Generator Tube Failure Event Tree

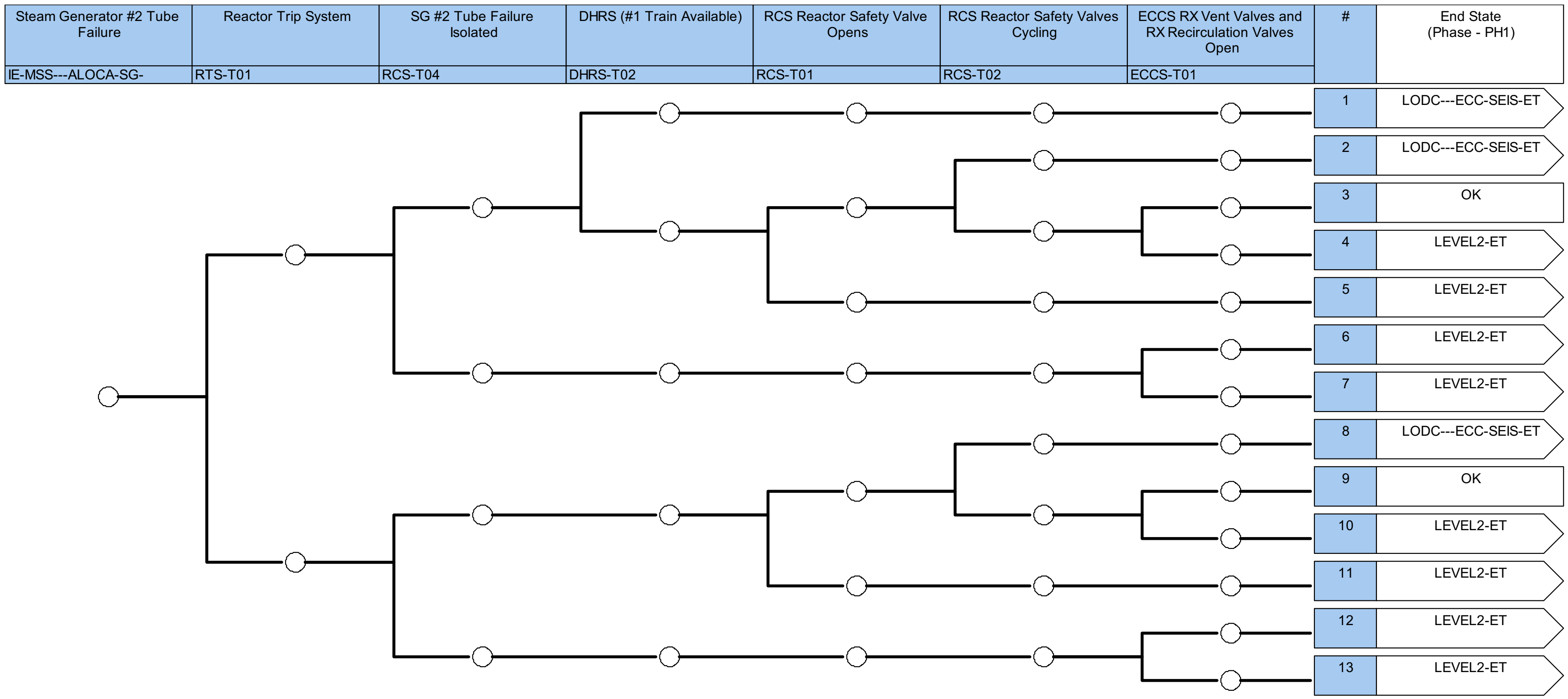


Figure 19.1-20: Seismically Induced Loss of Offsite Power Event Tree

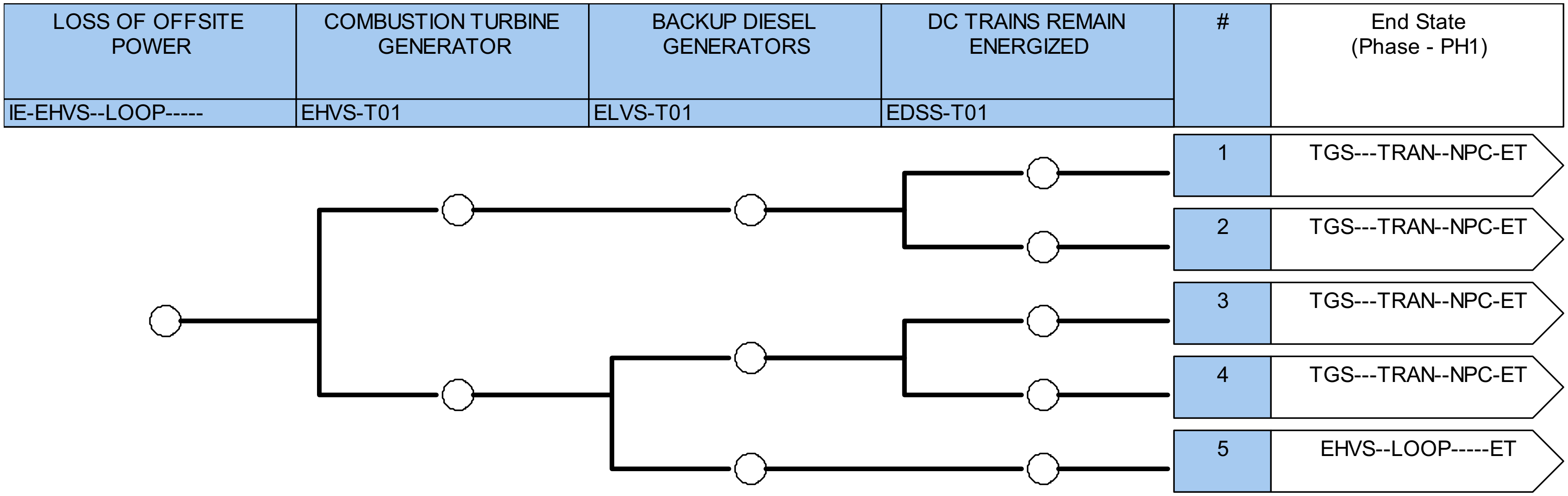


Figure 19.1-20a: Seismically Induced Loss of DC Power Event Tree

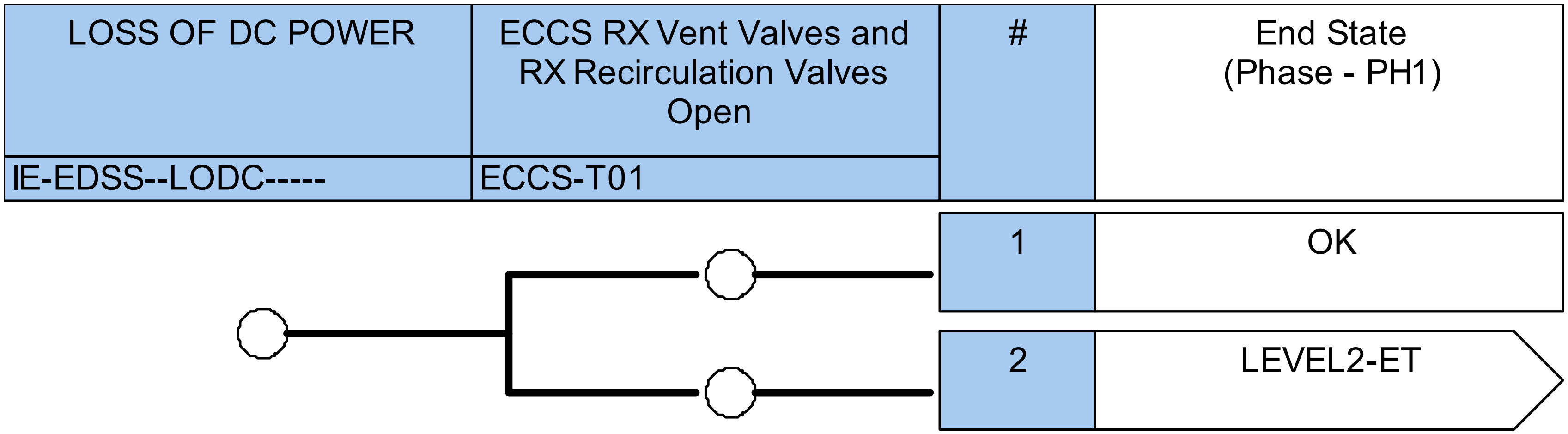


Figure 19.1-21: Fire Probabilistic Risk Assessment Event Tree FIRE1-Loss-of-Coolant Accident

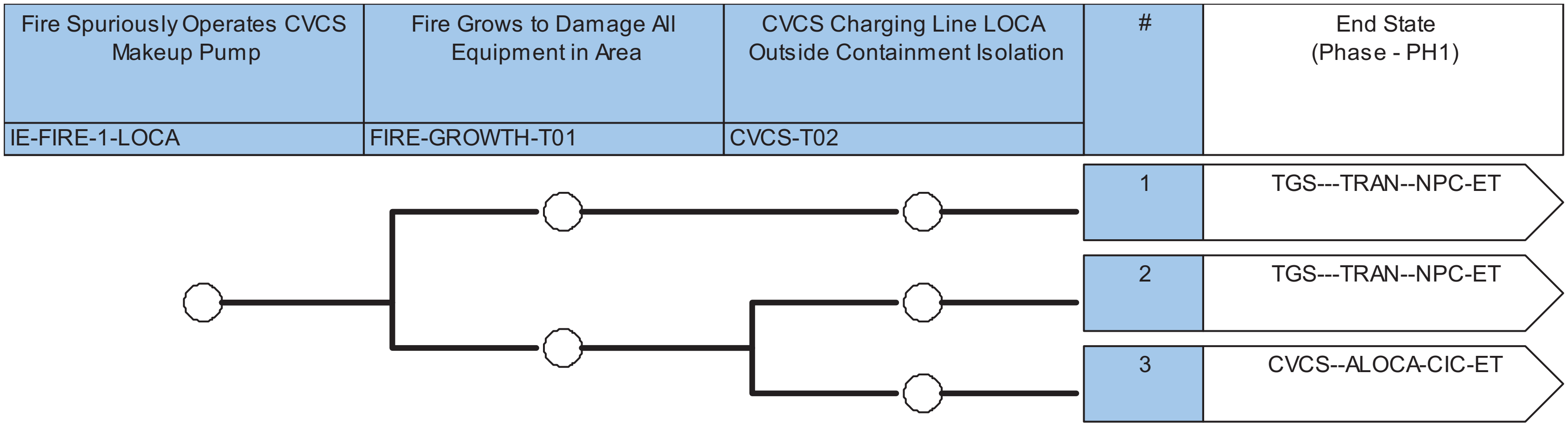


Figure 19.1-22: Fire Probabilistic Risk Assessment Event Tree FIRE2-Loss of Offsite Power

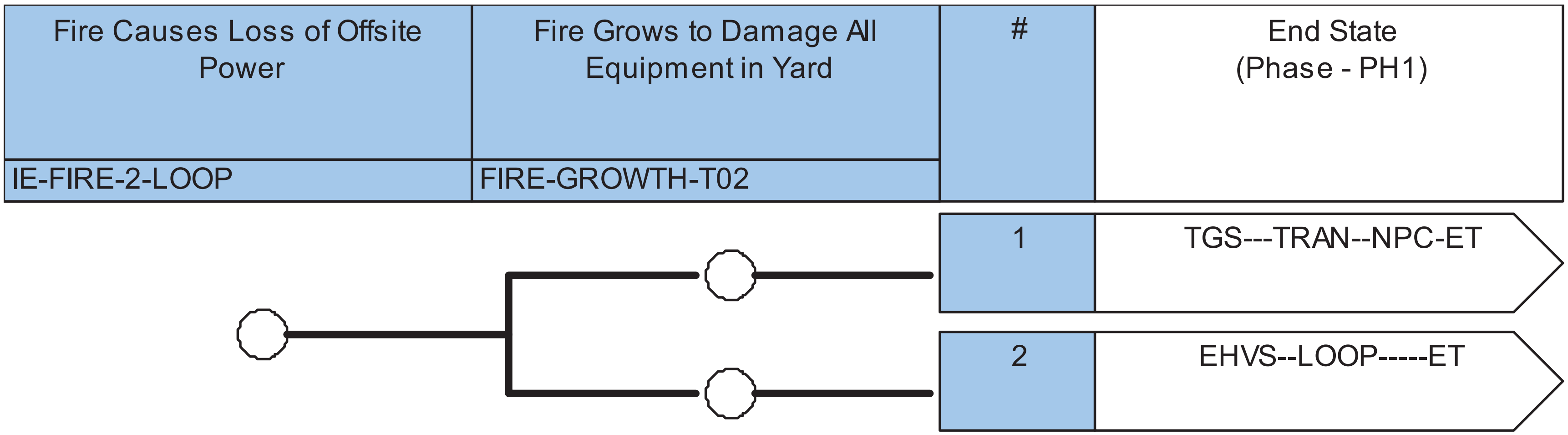


Figure 19.1-23: Fire Probabilistic Risk Assessment Event Tree FIRE3-Emergency Core Cooling System

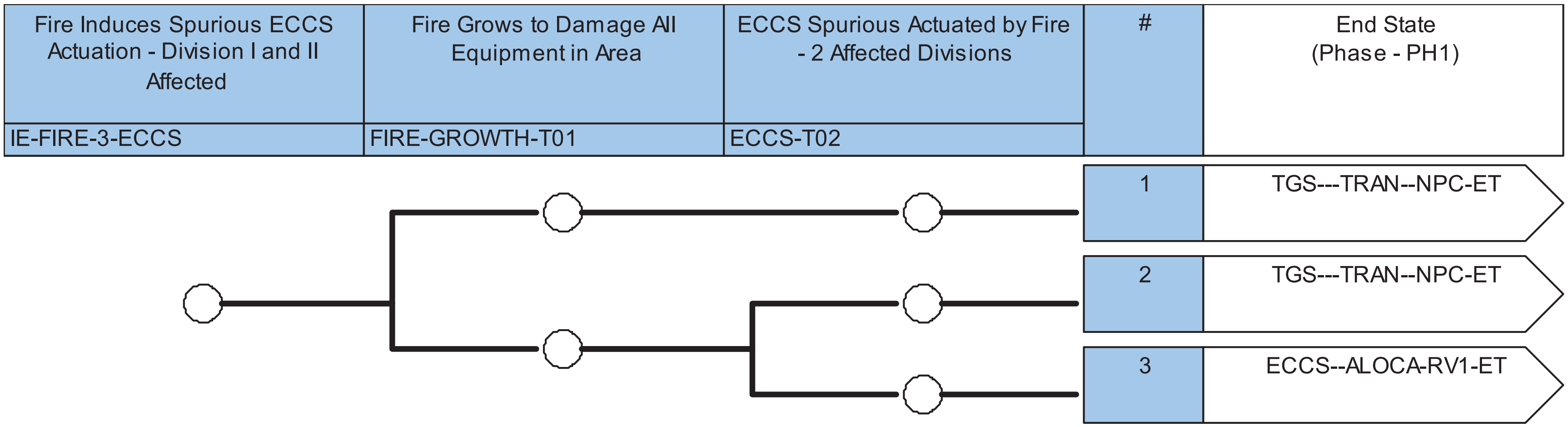


Figure 19.1-24: Fire Probabilistic Risk Assessment Event Tree FIRE-7-Transient

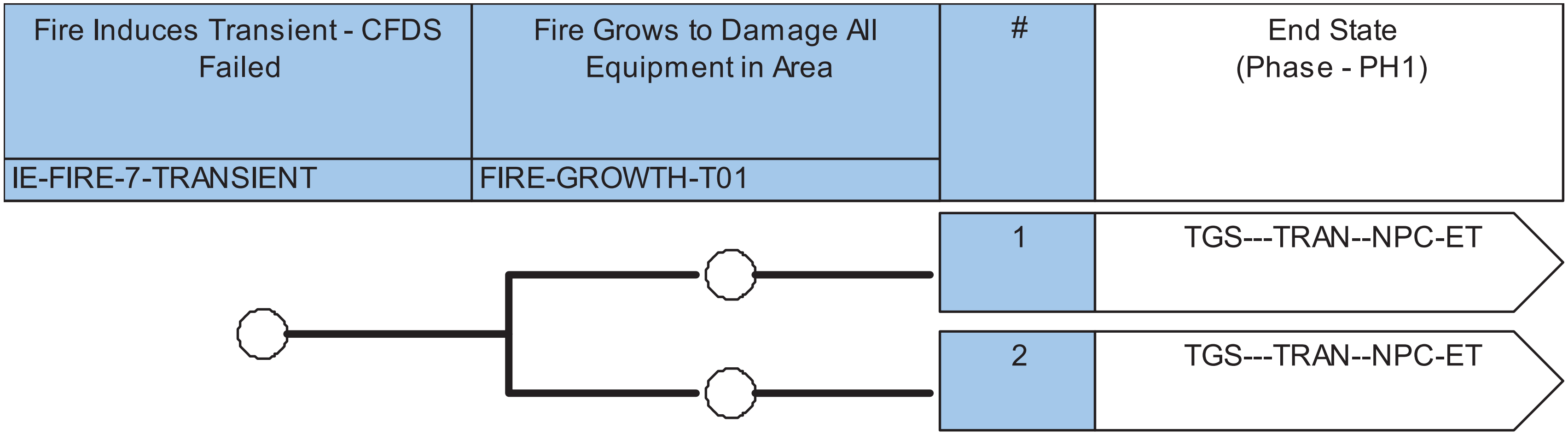


Figure 19.1-25: Internal Flooding in Reactor Building

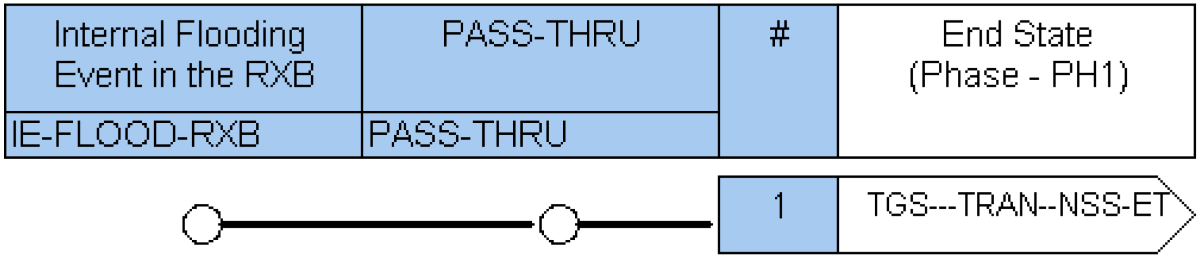


Figure 19.1-26: Internal Flooding in Turbine Generator Building

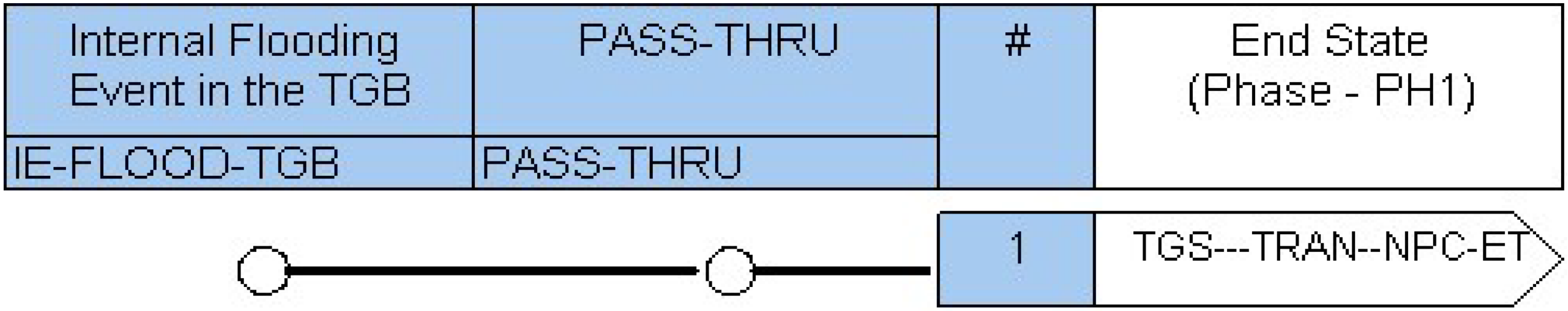


Figure 19.1-27: External Flooding Event Tree

External Flood	External Flood Results in LOOP	#	End State (Phase - PH1)
IE-EXTNL-FLOOD-FP-	EXT-FLD-LOOP		
		1	OK
		2	EHVS--LOOP-----ET

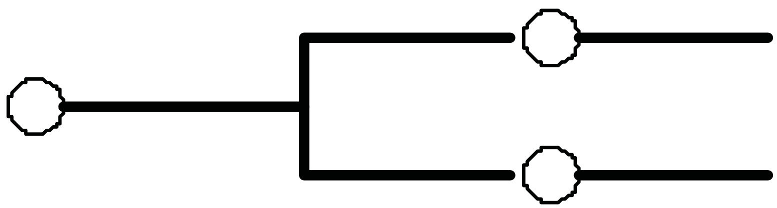


Figure 19.1-28: High-Winds (Tornado) Event Tree

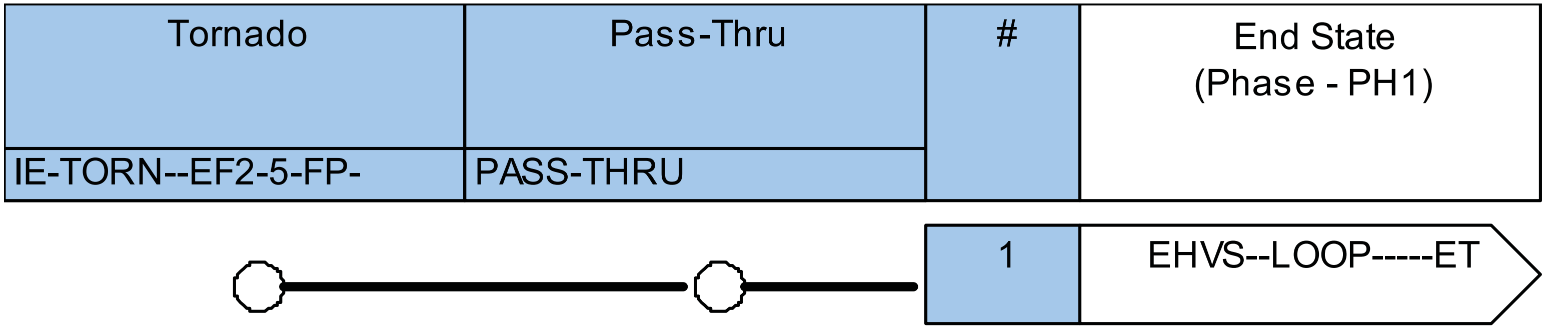


Figure 19.1-29: High-Winds (Hurricane) Event Tree

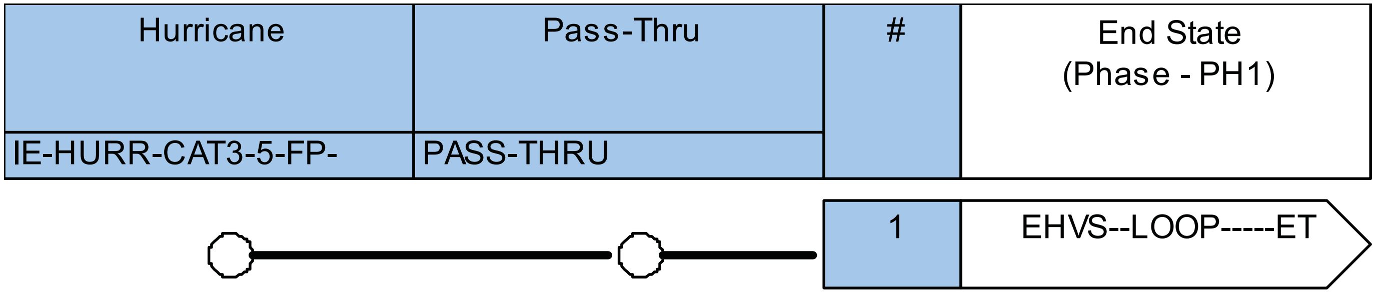


Figure 19.1-30: Crane Failure Event Tree (Representative)

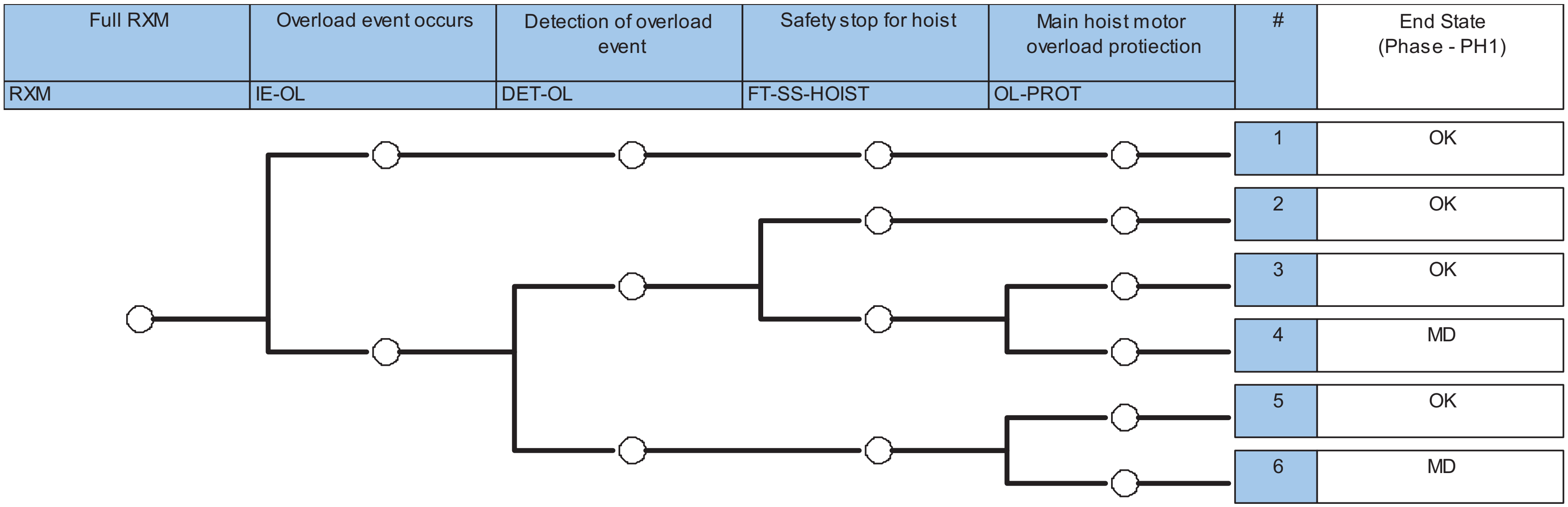


Figure 19.1-31: POS1 Transfer to Chemical and Volume Control System Charging Line Loss-of-Coolant Accident Inside Containment Event Tree (Representative)

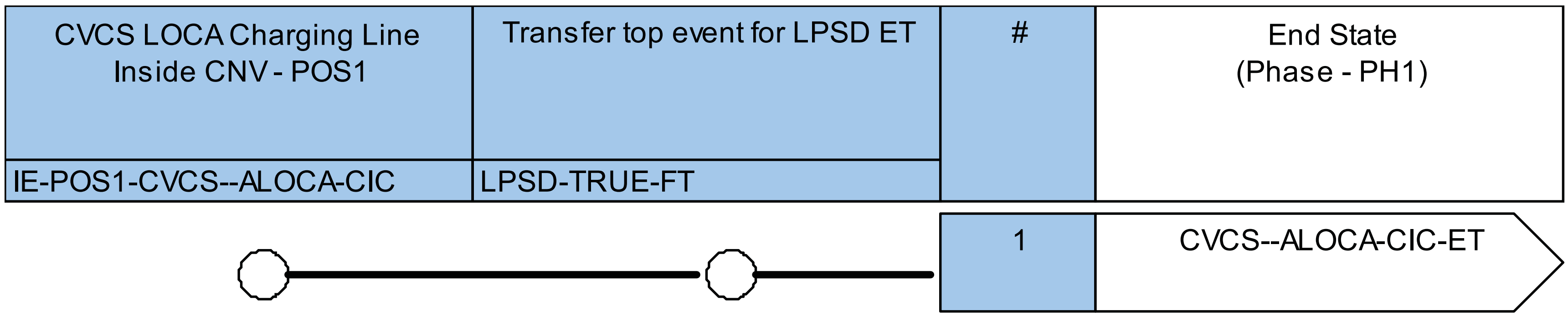


Figure 19.1-32: Transfer Event Tree for Module Drop in Operating Area, POS3

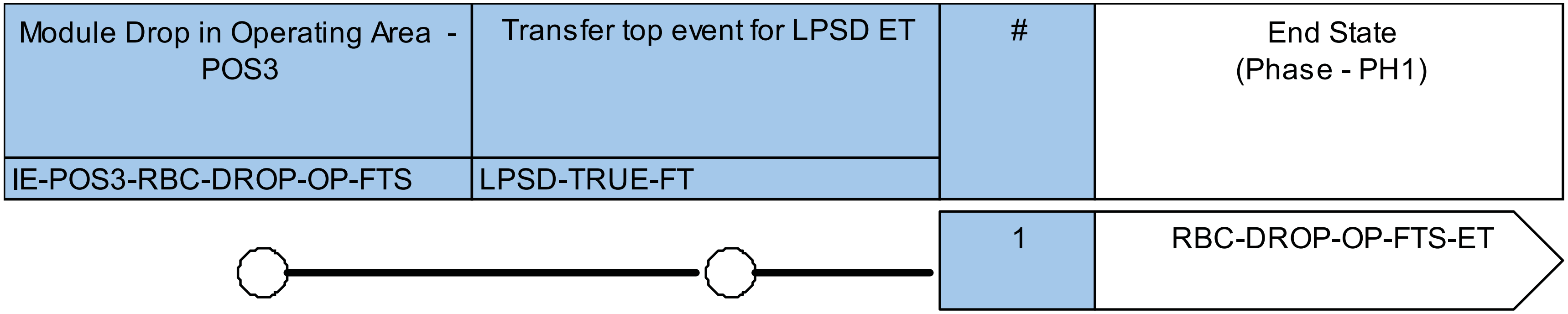


Figure 19.1-33: Transfer Event Tree for Module Drop in Refueling Area, POS3

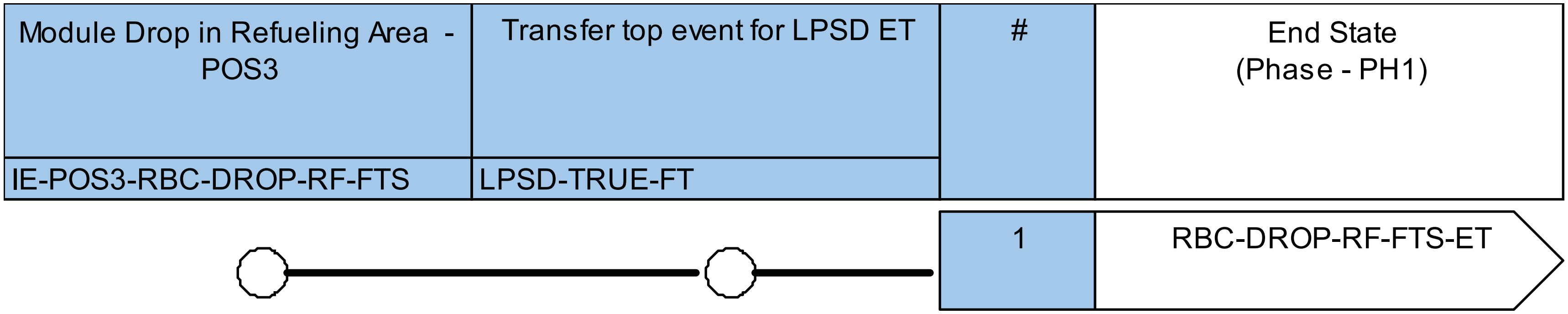


Figure 19.1-34: Transfer Event Tree for Module Drop in Operating Area, POS5

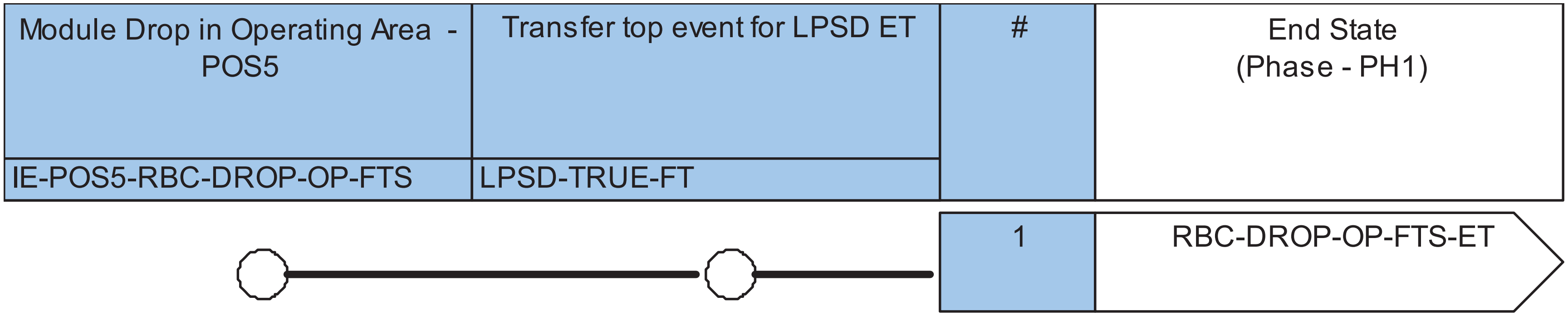


Figure 19.1-35: Transfer Event Tree for Module Drop in Refueling Area, POS5

Module drop in refueling area - POS5	Transfer top event for LPSD ET	#	End State (Phase - PH1)
IE-POS5-RBC-DROP-RF-FTS	LPSD-TRUE-FT		
		1	RBC-DROP-RF-FTS-ET

Figure 19.1-36: Event Tree for Module Drop in Operating Area

Module drop in operating area	DROPPED MODULE REMAINS UPRIGHT	#	End State (Phase - PH1)
IE-RBC-DROP-OP-FTS	RBC-T01		
		1	OK
		2	MD-CD

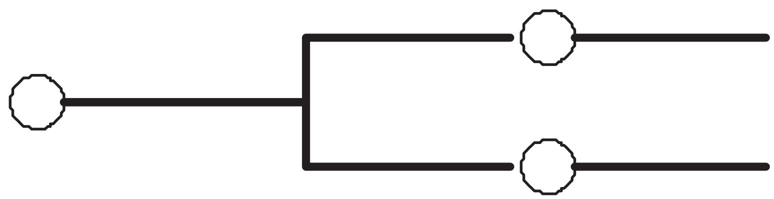


Figure 19.1-37: Event Tree for Module Drop in Refueling Area

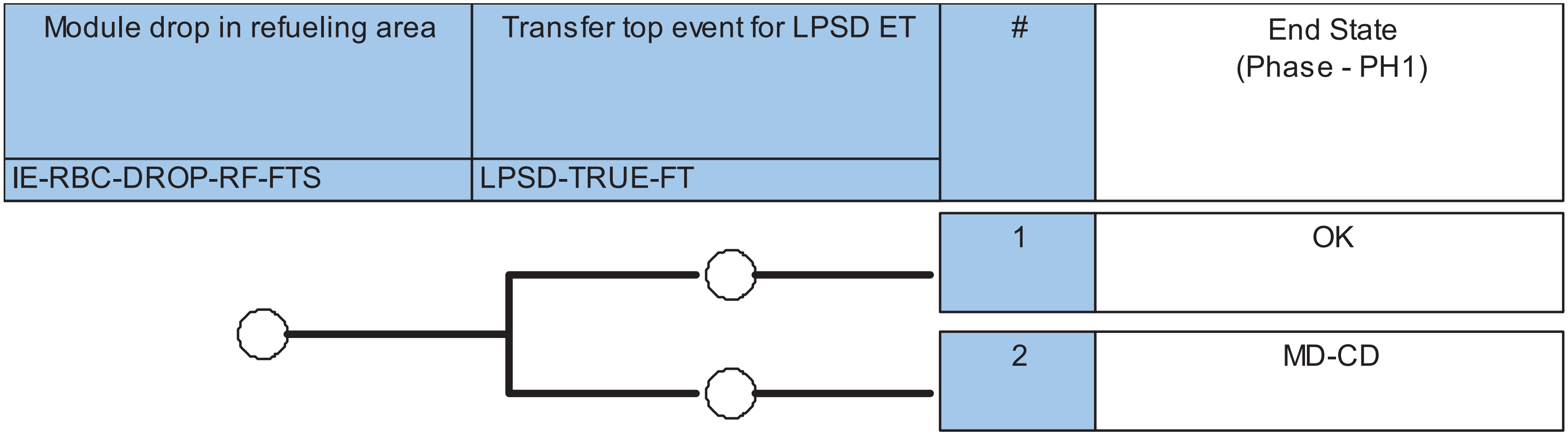


Figure 19.1-38: Multi-Module Assessment Approach

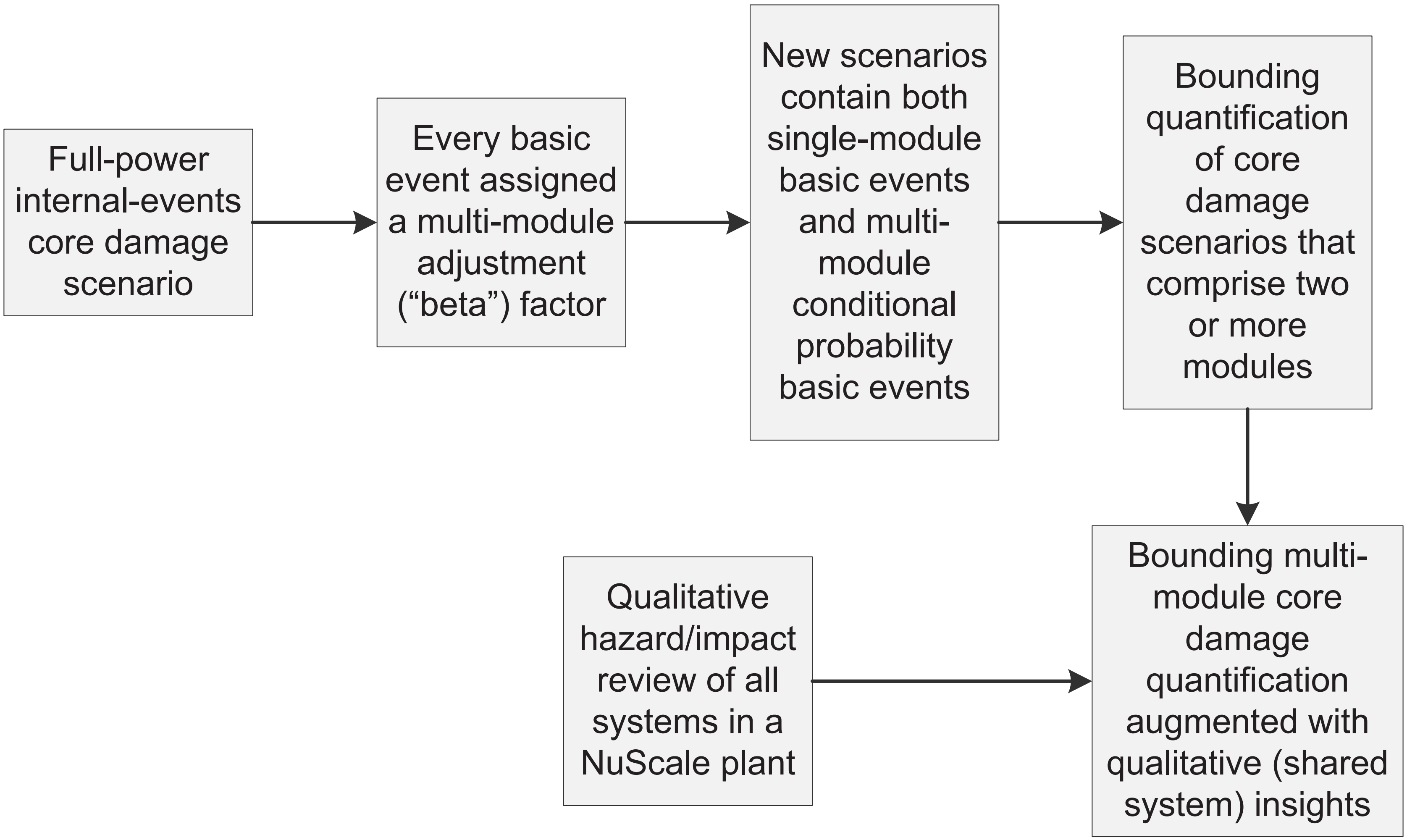


Figure 19.1-39: Contribution to Internal Events MM-CDF by Initiator

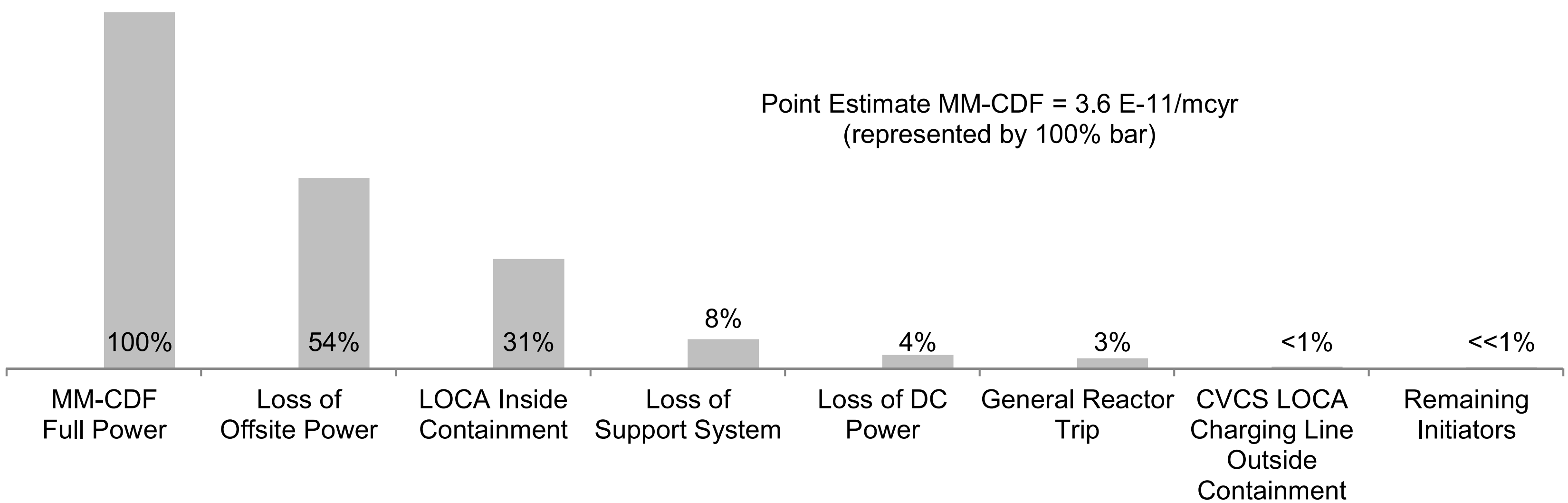


Figure 19.1-40: Contribution to Internal Events MM-LRF by Initiator

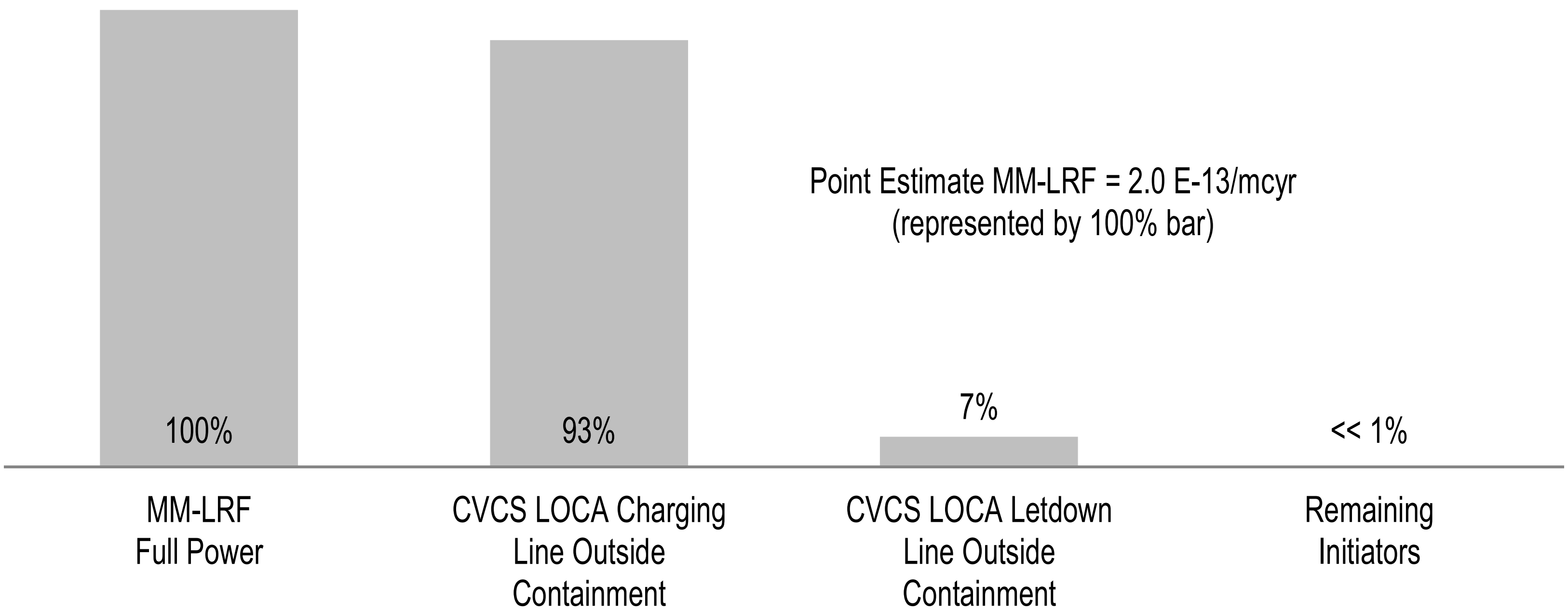


Figure 19.1-41: Potential Module Drop Configurations

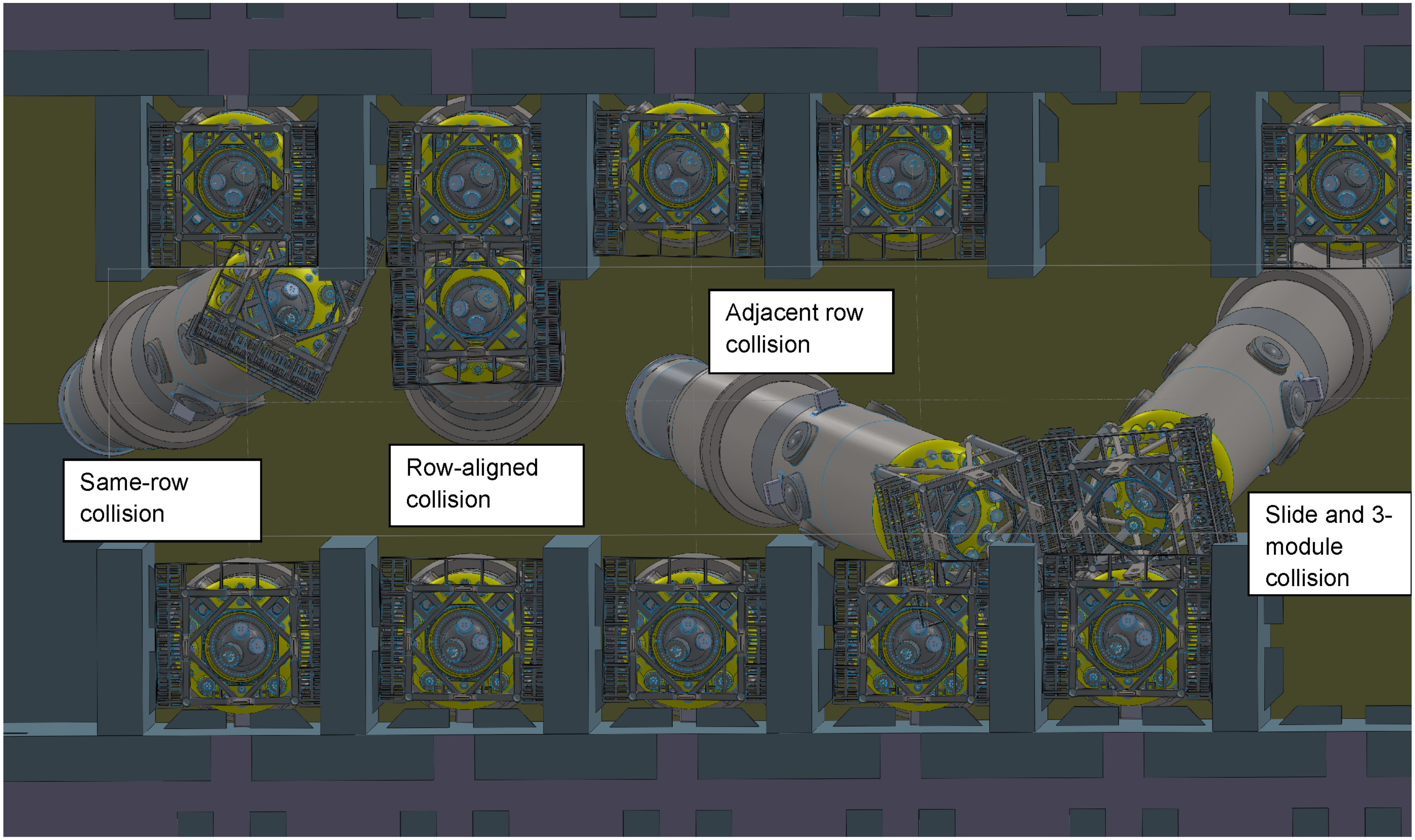
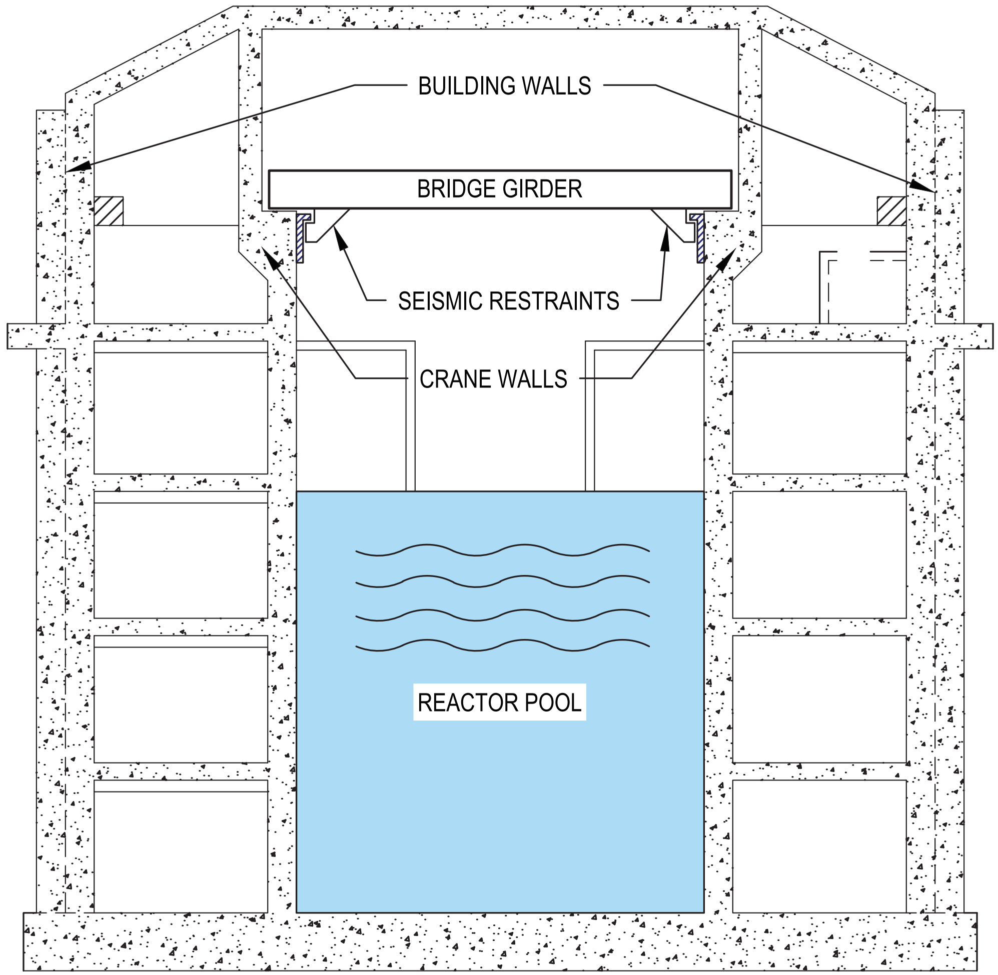


Figure 19.1-42: Simplified Reactor Building Section View



19.2 Severe Accident Evaluation

This section describes NuScale Power Plant design features to prevent and mitigate potential severe accidents in accordance with the requirements in 10 CFR 52.47(a)(23). Specific severe accident issues identified in SECY-90-016 (Reference 19.2-4) and SECY-93-087 (Reference 19.2-13) also are addressed. Consideration of severe accident phenomenology is presented on a NuScale Power Module (NPM) basis. Because each module is contained in its own containment vessel (CNV), multiple module configurations do not introduce unique severe accident progression phenomena within each CNV.

19.2.1 Introduction

As discussed in Section 19.1, severe accident sequences that result in core damage are evaluated in the Level 2 probabilistic risk assessment (PRA) for the likelihood of challenging containment and resulting in a large radionuclide release. Potential severe accident phenomena that could challenge containment and the containment capability are discussed in the following sections. The phenomena are evaluated using fundamental physics modeling with conservative assumptions. Potential challenges to containment integrity are identified from the following sources:

- Section 19.0 of the Standard Review Plan (NUREG-0800, Rev. 3)
- The ASME/ANS PRA Standard (Reference 19.2-1)
- NUREG/CR-2300 (Reference 19.2-2)
- NUREG/CR-6595 Reference 19.2-3)

Section 19.2.2 addresses the design capability to prevent specific severe accidents specified by regulation or regulatory guidance. Section 19.2.3 addresses the design capability to mitigate severe accidents in the unlikely event they should occur. Section 19.2.4 addresses the module containment capability, including the ultimate pressure capacity. Section 19.2.5 addresses accident management actions that are required to mitigate a severe accident. Section 19.2.6 considers potential design improvements in accordance with 10 CFR 50.34(f).

19.2.2 Severe Accident Prevention

A deterministic evaluation of a spectrum of beyond design basis accidents specified by regulation or regulatory guidance is summarized in Section 19.2.2.1 through Section 19.2.2.5 to illustrate the capability of a module with regard to these selected beyond design basis events. If the event is applicable to the design, it has also been addressed from a probabilistic perspective, as described in each discussion. The beyond design basis events evaluated in the following sections are:

- anticipated transient without scram (ATWS)
- mid-loop operations
- station blackout (SBO)
- fire protection
- interfacing systems loss-of-coolant accident

Section 19.2.2.6 addresses additional design capability with regard to severe accident prevention.

19.2.2.1 Anticipated Transient Without Scram

As described in Section 7.1 and Section 15.8, the underlying purpose of 10 CFR 50.62 is addressed through the use of a diverse, highly-reliable module protection system; this system results in a very low probability of an ATWS event. However, to provide insights on the module response to postulated ATWS events, initiating events with failure to shut down were modeled using NRELAP5. For beyond design basis accident sequences that do not result in core damage, these analyses demonstrate that

- the peak reactor coolant system (RCS) pressure does not exceed the ultimate reactor pressure vessel (RPV) failure pressure when one of the two reactor safety valves (RSVs) opens. The decay heat removal system (DHRS) and emergency core cooling system (ECCS) are not needed to respond.
- the peak containment pressure does not exceed the ultimate CNV failure pressure.
- return to power may occur, but fuel peak clad temperature remains below 2200 degrees F, thus, core damage does not occur.

Potential ATWS sequences are identified in the event trees, as discussed in Section 19.1. The ATWS sequences that do not result in core damage are annotated by “OK” as the end state. The ATWS sequences that result in core damage involve multiple failures in addition to the failure to scram.

19.2.2.2 Mid-Loop Operations

Reduced RPV water level such that RCS piping is only partially filled, i.e., a "mid-loop" configuration, is used in some pressurized water reactors to facilitate maintenance activities, notably on reactor coolant pumps. The time period when a plant is in the mid-loop configuration may be risk significant. The NuScale design incorporates a completely internal RCS and, because it is based on natural circulation, does not include reactor coolant pumps. Further, reactor coolant is circulated internally in the RPV and not through external loops. There is no module configuration which requires the RCS coolant inventory to be reduced to support maintenance. Thus, mid-loop operation is not applicable to the NuScale design and there is not an analogous configuration.

19.2.2.3 Station Blackout

Station blackout is defined by 10 CFR 50.63 as the loss of all alternating current (AC) power, which includes loss of offsite power and onsite emergency AC power. With respect to the NuScale design, Section 8.4 addresses the 10 CFR 50.63 requirements and the Nuclear Regulatory Commission policy for passive designs to withstand for a specified duration and recover from an SBO with no reliance on emergency onsite or offsite AC power.

The accident sequence discussions for the loss of DC power initiating event, EDSS--LODC, and the loss of offsite power initiating event, EHVS--LOOP, provided in

Section 19.1.4, illustrate the unique capability of the NuScale Power Plant design with respect to loss of all DC power and to loss of all AC power (i.e., all onsite and offsite sources), respectively.

19.2.2.4 Fire Protection

The NuScale design includes the following features to cope with potential fires that could affect module or plant safety:

- redundant safety systems to perform safety-related functions, such as reactor shutdown and core cooling
- physical separation between redundant trains of safety-related equipment used to mitigate the consequences of a design basis accident
- passive design which minimizes the need for support systems and the potential effects of "hot shorts"
- annunciation of fire indication in the main control room and in the security central alarm station to facilitate personnel response
- electrical power is not required for mitigating design basis events as safety systems are fail-safe on loss of power

As described in Section 9.5.1, the fire protection design conforms with National Fire Protection Association codes and standards in effect six months prior to the submittal of the Design Certification Application.

The risk associated with internal fires is addressed in Section 19.1.5.

19.2.2.5 Interfacing Systems Loss-of-Coolant Accident

Traditional use of the term “intersystem” loss-of-coolant accident (LOCA) or “interfacing systems” LOCA applies to low-pressure systems connected to the high-pressure RCS. Consistent with SECY-93-087, the NuScale design does not have low-pressure systems connected to the RCS. Hence, the term “interfacing systems LOCA” is not used in the PRA. The term "piping breaks outside containment" is applicable to the design. The NuScale design reduces the potential for a pipe break outside containment by minimizing system connections to the RCS of piping that is routed external to containment. As illustrated in Section 6.2.4 and Section 9.3.4, the only system with connections to the RCS and piping that runs outside containment is the chemical and volume control system (CVCS). These penetrations are isolated by dual-valve, single-body isolation valves, which have the capability to test for leakage past the inboard valve. Section 9.3.4 addresses conformance with the requirements of SECY-93-087.

Section 19.1.4 evaluates the possibility of a pipe break outside containment due to a break in CVCS piping from the probabilistic perspective. Specifically, initiating event CVCS--ALOCA-COC represents either an RCS injection line break or a pressurizer spray supply line break outside containment. Initiating event CVCS--ALOCA-LOC evaluates a discharge line break outside containment.

19.2.2.6 Other Severe Accident Preventive Features

The NuScale design includes additional features that are relevant to the prevention of severe accidents. In addition to the capabilities summarized in the prior sections, the design includes unique features.

- The integral primary system with natural circulation of primary coolant contributes to a low core damage frequency (CDF) due to the reduction of many potential accidents, such as LOCAs initiated by pipe breaks, because of the reduced number of components and limited external piping connections.
- The response to LOCAs is simplified because inventory makeup from external sources is not required to prevent core uncovery in the event of an inside-containment LOCA (i.e., only recirculation of RCS inventory from the CNV to the RPV through the ECCS is needed).
- The natural-circulation, primary-system flow design contributes to the low CDF by eliminating the possibility of reactor transients due to reactor coolant pump faults.
- The evacuated steel CNV contributes to the low CDF by eliminating vessel insulation and the associated possibility of sump blockage.
- The secondary-side passive DHRS contributes to the low CDF due to its simplified, fail-safe, electric power-independent, and highly-reliable design.
- The passive ECCS contributes to low CDF due to its simplified, fail-safe, electric power-independent, and highly-reliable design.
- The reactor pool contributes to low CDF by serving as the ultimate heat sink (UHS). With the modules immersed in this fully engineered and protected pool of water, the design eliminates the need for active heat transfer systems for safety system functions, such as service water or component cooling water, which would be dependent upon electric power.

19.2.3 Severe Accident Mitigation

The following sections summarize the design capabilities with regard to mitigation of a severe accident resulting in core damage. The capability of the CNV that encapsulates each RPV, the progression of a postulated core damage event, and the design characteristics that mitigate potential challenges to the CNV are discussed.

19.2.3.1 Overview of the Containment Design

The design of the CNV that encapsulates each RPV is described in Section 6.2. Each CNV is an evacuated, ASME Code Class 1 steel pressure vessel that houses the RPV and provides a barrier to the release of fission products. The CNV is maintained partially immersed in a below-grade, borated-water filled, stainless steel-lined, Seismic Category 1, reinforced concrete pool that serves as the UHS during off-normal operation.

The CNV provides for the retention of reactor coolant inventory to allow ECCS function. The reactor coolant that collects in the CNV is returned to the RPV by natural circulation through open ECCS vent and recirculation valves. Conductive and convective heat transfer result in transfer of core decay heat through the CNV walls to the UHS. The CNV may be flooded by using the nonsafety-related, active containment flooding and drain system (CFDS) to provide additional water to cool the core if inventory is lost due to a beyond design basis accident initiated by an unisolated break outside containment.

The CNV does not have internal subcompartments, which eliminates the potential for localized collection of combustible gases and differential pressures within the structure.

During normal power operations, the interior environment of the CNV is maintained dry at a near vacuum. As a result, the initial oxygen concentration is very low and limits the capability for combustion in the event of hydrogen generation due to a severe accident. The CNV is flooded with borated water from the reactor pool during shutdown, cooldown, and refueling operations.

19.2.3.2 Severe Accident Progression

The PRA identifies sequences that result in core damage. These sequences involve initiating events and combinations of mitigating system failures. Sequences in which the containment is intact, e.g., a pipe break inside containment or a spurious ECCS valve actuation, were evaluated to provide insights into the potential for RPV failure and resultant containment challenges, such as hydrogen generation, high-pressure melt ejection (HPME), fuel-coolant interaction (FCI), and core-concrete interaction. Additionally, two very low-probability containment bypass scenarios were evaluated to provide insights into the CNV lower-head performance and potential for mitigation. The thermal-hydraulic simulations, using the MELCOR code as discussed in Section 19.1.4.1.1.6, that were developed to model the potential severe accident sequences, were reviewed to identify the limiting challenges to the RPV and the CNV. In some situations, the sequence simulated for severe-accident considerations differs from the accident sequence with core damage in the Level 1 PRA. This is because the specific mode of a system failure may produce different characteristics that are limiting depending on the application of the result. An example is the ECCS may fail due to recirculation valve or vent valve failures. Both failure modes are considered in top event "ECCS-T01," but the module response differs depending on the failure mode. Failure of the ECCS vent valves to open results in a shorter time to core damage, whereas failure of the ECCS recirculation valves to open results in a longer time to core damage, but more severe core damage. In these instances, the case is given a unique numeric identification tag to differentiate the severe-accident simulation.

The set of sequences selected for simulation represents the full spectrum of conditions for analysis of potential severe accident phenomena, such as hydrogen generation, that may challenge containment integrity. Anticipated transient without scram sequences are not considered because a severe accident requires core uncovery which ensures sub-criticality from a lack of neutron moderation. Each severe accident simulation is summarized below and linked to a Level 1 event tree in Section 19.1, where appropriate. Table 19.2-2 summarizes the status of mitigating systems for each of the simulations.

Case LCC-05T-01

Case LCC-05T-01 is an inside-containment LOCA on the CVCS injection line at a high elevation in the CNV with success of the reactor trip system. Both trains of the DHRS are unavailable, and the ECCS has incomplete actuation upon demand with all three reactor vent valves (RVVs) opening while both reactor recirculation valves (RRVs) fail closed. No other mitigation systems are available. Case LCC-05T is contained in the PRA Level 1 event tree in Figure 19.1-4 and the added numeric tag identifies variation in ECCS failure mode, with RRV failure the most probable mode. This case provides a rapid liquid-space LOCA that transitions into a vapor-space LOCA once the RVVs open. (A liquid-space LOCA refers to a break in a region of the RPV which is completely covered by coolant and the material transferred out of the RPV is primarily liquid, whereas a vapor-space LOCA occurs above the baffle plate, thus the material transferred is primarily steam.)

Table 19.2-3 provides key events and associated timing. Core damage occurs at 4.8 hours with partial fuel relocation to the lower plenum at 9.4 hours. A total of 122.1 lbm of hydrogen is generated. Peak RPV and CNV pressures do not challenge vessel integrity, and by 72 hours there is a stable cooling configuration established by decay heat transfer through the flooded containment, retaining relocated debris in the RPV.

Case LCC-05T-02

Case LCC-05T-02 is a variation of LCC-05T-01, signified by the same initial identifier but a unique numeric tag. In this case the failure mode of the ECCS is complete failure with all five valves failing to open. This failure mode is the least credible mode. The two cases are otherwise identical. This case bounds the most rapid core damage for a liquid-space LOCA in containment.

Table 19.2-4 provides key events and associated timing. Core damage occurs at 2.6 hours with partial fuel relocation to the lower plenum at 6.8 hours, both the shortest times for intact containment cases. A total of 135.1 lbm of hydrogen is generated. Peak RPV and CNV pressures do not challenge vessel integrity, and by 72 hours there is a stable cooling configuration established by decay heat transfer through the flooded containment, retaining relocated debris in the RPV.

Case LCC-05T-03

Case LCC-05T-03 is a further variation of LCC-05T-02, signified by the same initial identifier, but a unique numeric tag. These two cases are identical, with the sole exception being a reduction of the LOCA flow area to 20 percent of the LCC-05T-02 flow area. The primary purpose of this simulation is to evaluate the potential for high RPV pressure after core damage to determine if there is a potential for HPME. Secondarily, this simulation provides insight into hydrogen production and relocated fuel mass for a slower accident progression.

Table 19.2-5 provides key events and associated timing. The accident progression is significantly delayed with core damage at 25.4 hours and relocation at 35.6 hours. Following core relocation, there is a small pressure differential between the RPV and CNV as the steam is not immediately transferred; the maximum pressure in the RPV is

205.6 psia and the maximum differential pressure is only 90.1 psid. A total of 211.7 lbm of hydrogen is produced, which is about 50 percent more than LCC-05T-02. There is essentially no difference in the mass of relocated fuel. By 72 hours, a stable cooling configuration is established by decay heat transfer through the flooded containment, retaining relocated debris in the RPV.

Case LEC-06T-00

Case LEC-06T-00 is initiated by the spurious actuation of a single RVV, creating a LOCA into the containment, with success of the reactor trip system. Both trains of the DHRS are unavailable. Upon demand, the ECCS has incomplete actuation with the remaining two RVVs opening while both RRVs fail to open. No other mitigation systems are available. Case LEC-06T is not explicitly included in the PRA Level 1 event trees, but is identical for event tree purposes to LEC-05T (Figure 19.1-6) with the numeric difference signifying which ECCS valve opens. The numeric tag "05T" is used for a reactor recirculation valve LOCA and "06T" is used for a reactor vent valve LOCA. This case simulates a rapid vapor-space LOCA with an intact containment.

Table 19.2-6 provides key events and associated timing. Core damage occurs at 7 hours with partial fuel relocation to the lower plenum at 11.6 hours, signifying that a vapor-space LOCA progresses slower than a liquid-space LOCA. A total of 124.7 lbm of hydrogen is generated. Peak RPV and CNV pressures do not challenge vessel integrity and by 72 hours there is a stable, cooling configuration established by decay heat transfer through the flooded containment, retaining relocated debris in the RPV.

Case TRN-07T-01

Case TRN-07T-01 is a general transient initiated by a reactor trip and containment isolation. Both trains of the DHRS are unavailable, thus the RPV pressurizes to the RSV setpoint. The RSV sticks open upon first demand, creating a vapor-space LOCA into containment. The ECCS fails completely upon demand and no other mitigating systems are available. In the Level 1 PRA event trees, TRN-07T is used to represent a number of system availabilities with a stuck open RSV. The numeric "01" tag signifies which variation of ECCS failure mode is simulated. This case is included to bound the slowest vapor-space, full-break LOCA to evaluate the impacts on hydrogen production and relocated fuel mass.

Table 19.2-7 provides key events and associated timing. Core damage occurs at 20.6 hours with partial fuel relocation to the RPV lower head at 31.4 hours, significantly slower than LEC-06T-00. Of all the intact containment cases, TRN-07T-01 has the most hydrogen produced (222.9 lbm) and the most relocated fuel (21 of 37 assemblies relocated). The RPV pressurizes to the RSV setpoint, but does not exceed design pressure, nor does the CNV; and by 72 hours, a stable cooling configuration is established by decay heat transfer through the flooded containment, retaining relocated debris in the RPV.

Case LCU-03T-01

Case LCU-03T-01 is initiated by a CVCS injection line LOCA outside containment. The reactor trip system is a success, but isolation of the CVCS fails. resulting in a containment bypass accident. Both trains of the DHRS are unavailable. Other mitigation systems are unavailable. In the Level 1 PRA event trees, LCU-03T is used to represent several variations of containment bypass LOCA scenarios. The numeric "01" tag signifies a failure of all ECCS valves to open, in the event of an actuation signal. Although very improbable and artificial (in the sense that the CNV is already bypassed and, hence, the containment function has already failed), this case is included primarily to evaluate the CNV performance when subjected to thermal attack from core debris, upon RPV lower-head failure.

Table 19.2-8 provides key events and associated timing. Core damage occurs at 2.6 hours, matching LCC-05T-02 for the shortest time to core damage. The first fuel relocation to the RPV lower plenum occurs at 5 hours, and by 10 hours, all fuel assemblies have relocated. A total of 174.1 lbm of hydrogen is produced. Failure of the RPV lower head occurs at 11.7 hours, transporting debris into the CNV. The debris cools rapidly in the CNV and CNV in-vessel retention is ensured. By 72 hours, a stable cooling configuration is established with decay heat transfer to the reactor pool.

Case LCU-01T-01

Case LCU-01T-01 is a variation of LCU-03T-01. In this case, the initial conditions and system availabilities are identical with the exception that an operator action to flood containment from the CFDS is successful. The action is performed 30 minutes after the RPV level reaches the bottom of the pressurizer. LCU-01T-01 is not included in the Level 1 PRA event trees in Section 19.1 as the mitigative action does not prevent core damage. However, it is considered to evaluate the potential to prevent RPV lower-head failure by containment flooding.

Table 19.2-9 provides key events and associated timing. Containment flooding does not prevent core damage, but it is delayed by 1.7 hours compared to LCU-03T-01. As in LCU-03T-01, all fuel assemblies eventually relocate to the RPV lower head, but as the progression is slightly delayed, more hydrogen is produced, with a total generation of 227.1 lbm. The RPV lower head inside surface heats up to a maximum of 1119 degrees F, but does not fail, providing the insight that containment flooding can help ensure RPV in-vessel retention. By 72 hours, a stable cooling configuration is established by decay heat transfer through the flooded containment, retaining relocated debris in the RPV.

Section 19.2.3.2.1 discusses severe accident sequences in which the core debris is cooled in the RPV and the progression of the accident is arrested in the RPV. Section 19.2.3.2.2 discusses severe accident sequences in which the core debris has penetrated the RPV and the progression of the accident is arrested in the CNV.

19.2.3.2.1 Core Damage Progression with Retention in the Reactor Pressure Vessel

In-vessel retention-RPV refers to the retention in the RPV lower head of relocated core debris resulting from a core damage event. Retaining the core material in the lower head of the RPV is relevant only during postulated severe accident sequences with an intact containment because sequences in which containment is failed are already (as a modeling convenience) classified as large release sequences. For sequences in which the core has been uncovered and damaged due to loss of coolant, the core debris could be relocated to the lower head as illustrated in Figure 19.2-1. Under these circumstances:

- the core debris in the RPV lower plenum imposes a heat flux on the inner surface of the vessel head.
- the external surface of the RPV lower head is cooled by the water in the CNV. Approximately half of the RPV is covered by the water in the CNV.
- the water in the CNV is cooled through the containment shell by the reactor pool (in which the CNV is partially immersed).

From the perspective of retaining a damaged core in the RPV, the concern is that the RPV bottom head, under thermal attack from the core debris, may reach a temperature that is sufficient for melt through (about 1600 degrees K for RPV steel). A related concern is that structural failure may occur at a temperature lower than the melting temperature of steel due to loss of strength of the steel wall. Thus, the in-vessel retention-RPV analysis considers the coolability of the relocated core material (self-heating body) resulting from a severe accident by heat transfer to water in the CNV through the RPV steel wall and then to the reactor pool through the CNV steel wall. The objectives of the in-vessel retention-RPV evaluation are to:

- evaluate the temperature distribution over the RPV lower head shell as heat is transferred from the relocated core debris to the water in the containment.
- assess if the maximum shell temperature is low enough that the RPV lower head retains sufficient strength to support itself and its contents.

The major elements associated with the evaluation are:

- identification of applicable severe accident sequences
- evaluation of core debris configuration
- evaluation of maximum heat flux and potential RPV failure

Identification of Applicable Severe Accident Sequences

The severe accident sequences ending in core damage, as defined in the Level 1 PRA evaluation provided in Section 19.1, were reviewed for applicability to the in-vessel retention-RPV evaluation. Only those sequences that involve both significant relocation of core debris into the RPV lower head and an intact containment are relevant for the evaluation. Sequences in which the CNV boundary is failed were not considered because the containment function is already failed and such sequences are already classified as large releases.

The simulations presented in Section 19.2.3.2 were reviewed to identify key characteristics such as core relocation time, core debris mass in the RPV lower head, peak temperature of the core debris, and containment thermal-hydraulic conditions. The results of these cases confirm that the boundary conditions used for the subsequent tasks in the in-vessel retention-RPV evaluation are representative or conservative.

Evaluation of Core Debris Configuration in the Reactor Pressure Vessel

The profile of the heat flux associated with the core debris bed is dependent on the configuration of the fuel materials and metals. The profile of the heat flux to the RPV lower head from solid core debris is highest near the center and opposite to that from liquid core debris due to convection flow patterns that develop within liquid debris. As will be shown later, the minimum critical heat flux (CHF) occurs at the bottom of the hemispherical head. Thus, the heat flux profile from solid core debris is judged to be more challenging for retaining core debris in the RPV than the heat profile of liquid debris of the same volume, shape, and decay power. Additionally, the MELCOR simulations presented in Section 19.2.3.2 support that relocated debris is solid, not molten.

Theofanous (Reference 19.2-7) and Rempe (Reference 19.2-8) provide a range of potential debris bed configurations, based on an assumed molten core, for which reference data are available. The configurations are summarized as follows:

Configuration 1- molten corium with metallic layer on top. Debris from the core relocates into the RPV lower head and continues to melt. Eventually, a molten configuration is established with a molten oxide pool at the center, surrounded by a solid oxide crust and a less dense metallic layer on the top of the oxidic materials (oxidic materials consist primarily of uranium dioxide, UO_2). The heat is generated in the UO_2 due to radioactive decay. The mechanism of heat transfer from the molten oxidic core to its surroundings (i.e., downward to the RPV lower head and upward to the metallic layer) is natural convection and conduction.

Configuration 2- crucible discharge. Occurs upon failure of a core-internal crucible, which had formed as a consequence of the melting-freezing phenomena; that is, melting in the inner, higher-power density region, and freezing as the melt relocates in the outer, colder boundaries. This creates the concern that a molten "jet" impinges on the side wall of the RPV lower head causing damage. The jet continues to flow to the RPV lower head to form a molten oxidic pool similar to the first configuration. A unique characteristic of this configuration is that heat transfer is dominated by forced convection instead of natural convection, due to the molten pool being agitated by the molten jet. The increased heat flux from forced convection is another concern in addition to the concern of RPV shell damage from jet impingement.

Configuration 3 - molten corium before the metallic and oxidic materials relocate. This configuration contains a large oxidic pool (approximately 50 percent of the core inventory) with a small metallic component (unoxidized zircaloy and stainless steel). This configuration may be "quasi-steady"; as such, it is similar to Configuration 1 except for the quantity of core debris and the bounding decay power at a specific time.

Configuration 4 - additional relocation. This configuration considers that, after development of Configuration 3, an additional approximately 35 percent of the core materials relocate to form a second molten pool. The metallic layer from the first relocation is heated from below by the molten pool, and above by the overlying pool and crust.

Configuration 5-metallic layer below oxidic pool. This configuration represents the situation in which sufficient uranium dissolves into unoxidized zirconium to form a heavier metallic layer that sinks below the oxidic pool. If this configuration forms, it presents a unique challenge to vessel integrity because heat sources within the lower metallic layer are focused toward the bottom of the vessel.

Configuration 1 and Configuration 3 are sufficiently similar to be considered as a single configuration. Based on the literature review, and considering the physical characteristics of the small core, Configuration 1 is selected as the most appropriate core debris configuration, based on the conservative assumption of full core relocation and the following considerations.

- Configuration 2 is judged not appropriate for a small core because holding a significant molten pool of fuel materials in the core region requires a sizable crucible crust and blockage. In such a circumstance, the molten pool in the core region could supply a continuous molten jet into the molten pool in the RPV lower plenum to allow the forced convection condition to last for a reasonably long time and potentially threaten the integrity of the RPV lower head. Given the small amount of fuel materials in comparison to a large reactor, a molten jet is judged not to be a concern for lower RPV head integrity, especially considering the thick heavy reflector. Further, the small core indicates that the lower support plate temperature is closely tied to the core temperature. As a result, the lower core support plate would be expected to fail structurally before the core melts significantly.
- Configuration 4 is judged not to be appropriate for a small core. Larger cores would allow molten pool formation in the RPV lower plenum in multiple phases. However, core debris relocation in a small core is likely to occur in a contiguous manner.
- Configuration 5 involves a layer of metallic U-Zr liquid sinking to the bottom of the relocated core debris. MELCOR calculations indicate that the unoxidized (metallic) Zr mass in the relocated debris is significantly less than the oxidized Zr mass. Thus, it is unlikely that a sizable pool of unoxidized Zr forms to allow dissolution of significant uranium from UO2. Even if a shallow layer of metallic U-Zr forms at the bottom of the core debris, the heat flux near the center of the RPV lower head is lower than that near the edge of the pool due to convective effects. Given the CHF profile as a function of the surface orientation, Configuration 5 would be less challenging than a solid configuration and thus is not used in the in-vessel retention-RPV analysis.

An additional consideration in evaluating the effect of the core configuration on retaining the core debris in the RPV is the "focusing" effect. The focusing effect reflects the postulate that a molten metallic layer, composed primarily of steels and unoxidized zirconium that are lighter than the oxidic debris, may form above the oxidic debris. Although this layer does not generate heat, it may thermally challenge the section of the RPV wall it is in contact with. This is because the convective forces and high thermal conductivity of the molten metallic layer can focus the heat flow from the top of the oxidic debris onto a relatively small area along the RPV wall; the focusing effect increases as the area in contact with the RPV decreases.

Basis for Evaluating Core Debris Retention in RPV

The outside surface of the RPV lower head is cooled by the water in the CNV. Heat transfer from the external surface of the RPV lower head is most effective if conditions remain in the nucleate boiling regime. In this regime, there is a high heat flux at relatively low excess temperature of the RPV wall above the temperature of the water in the CNV. In the nucleate boiling regime, the heat flux and excess temperature of the RPV wall increase at a roughly proportional rate until the CHF is approached. At this heat flux, generated steam has difficulty departing from the surface at a sufficient rate for the surface to remain wetted. If the external heat flux is increased marginally beyond the CHF, the heat transfer regime transitions to film boiling and the excess temperature of the RPV wall increases dramatically. If instead the excess surface temperature is increased marginally beyond the corresponding temperature at the CHF, the heat transfer regime enters transition boiling and the local external heat flux decreases. The latter condition applies for geometries with significant thermal heat capacity and the ability to effectively conduct heat away from localized regions of degraded heat transfer. Remaining in the nucleate boiling regime, however, ensures that the excess temperature of the RPV wall remains small and the integrity of the RPV is assured.

Experimental studies related to in-vessel retention (IVR) were reviewed for applicability to the NuScale design. The studies relevant to NuScale capability to retain a damaged core in the RPV are those for the downward-facing, heated surface with curvature, as provided by NUREG/CR-6507 (Reference 19.2-9), Guo and El-Genk (Reference 19.2-10) and Theofanous (Reference 19.2-11, Reference 19.2-12). The studies demonstrate the CHF value is primarily controlled by the effectiveness of generated steam in escaping from underneath the RPV surface (a flat plate is not as efficient in venting steam as a curved surface) and the amount of subcooling in the surrounding water pool. The studies provide insights for the underside of the RPV head as well as the vertical portion of the RPV wall. The studies provide a range of CHF values for the bottom center of a hemispherical surface like the RPV lower head and larger CHF values for vertical surfaces like the vertical portion of the RPV wall. The CHF results were strongly sensitive to the ability of a surface to vent steam from the region in which it is generated, showing a strong correlation to the inclination angle of the geometry.

The Subscale Boundary Layer Boiling (SBLB) experiment described in NUREG/CR-6507 is the most relevant to an in-vessel retention-RPV analysis in which the RPV lower head is a clean hemisphere (or a shape close to a hemisphere) and the water pool is saturated or subcooled. The study indicates that, at saturated atmospheric conditions, a CHF of 400 kW/m^2 is appropriate for the bottom of a hemispherical surface and 1 MW/m^2 for vertical surfaces. Although the lower head design of the NPM diverges from a clean hemisphere due to the seismic retention pin, the results of the SBLB tests remain applicable for the curved portion of the lower head because the NPM design does not include features that hinder the upward movement of steam. The vertical portion of the retention pin as well as the transition fillet region are necessarily more vertically oriented than the bottom of the hemispherical surface and can thus be conservatively assessed against the 400 kW/m^2 CHF estimate. The results of the Guo and El Genk experiments are judged to be applicable to the flat bottom surface of the retention pin; the experiments support a minimum CHF of 200 kW/m^2 for saturated atmospheric conditions.

Although the in-vessel retention-RPV analysis employs CHF estimates that were derived for saturated fluid at atmospheric pressure, the coolant in the CNV during an in-vessel relocation event will be significantly subcooled and pressurized due to the presence of noncondensible hydrogen in the containment. Subcooling enhances CHF due to the sensible heat required to initiate the boiling process and due to interfacial condensation of generated steam, which reduces overall steam voiding. Increased pressure enhances CHF due to increased vapor density, resulting in smaller bubbles and a more easily wetted surface. Considering the degree of subcooling and pressurization observed following core relocation for the NPM, the CHF would increase in comparison to the saturated atmospheric condition as quantified by the analytical model presented in NUREG/CR-6507. As such, CHF estimates for saturated atmospheric conditions are conservative relative to expected conditions within the NPM.

To evaluate the structural capability of the RPV to retain a core debris bed, the concept of heat flux limited wall thickness is introduced. From Theofanous (Reference 19.2-7), steel maintains its full strength when its temperature does not exceed 900 degrees K (627 degrees C). If the RPV lower head is in steady-state contact with core debris on the interior wall and cold water on the exterior, a linear temperature profile is established across the RPV lower head wall thickness. The temperature at a certain depth in the wall equals 900 degrees K, given that the interior surface temperature exceeds 900 degrees K due to contact with core debris. Conversely, the distance from the cold wall surface to the 900-degree K point defines the thickness of the RPV that can be relied upon to support the lower head and its contents. This distance is termed the "heat flux limited wall thickness". The RPV can retain adequate wall thickness only if the outside wall surface remains below 900 degrees K, which is guaranteed if the heat removal mechanism on the outside wall surface remains in the nucleate boiling regime, i.e., the CHF is not exceeded. Conservative interpretation of minimum wall thickness from Theofanous (Reference 19.2-7) concludes that a wall thickness of 1.1 cm that remains below 900 degrees K is sufficient to support the weight of the lower head and its contents during severe accident conditions.

Success Criteria for Retention of Core Debris in the Reactor Pressure Vessel

An evaluation of thermal attack from oxidic debris on the RPV lower head is performed using a three-dimensional ANSYS conduction model (Reference 19.2-6) and conservative hand calculations. The approach is to:

- evaluate the maximum heat flux from the relocated core debris to the RPV wall over the entire RPV wall inner surface

- identify susceptible locations where RPV failure is more likely to occur due to either a melt-through or a loss of structural strength

The intent is to evaluate the potential for melt-through or loss of strength at susceptible locations. Thus, a thermal success criterion and structural success criterion were considered, consistent with Theofanous (Reference 19.2-7) and Rempe.

Thermal success criterion: The heat flux at all locations on the outside of the RPV lower head from the relocated core debris must be smaller than the CHF for those locations. Two potential RPV failure locations are of particular interest.

- The retaining pin and the immediately surrounding, nearly-horizontal region of the RPV lower head is a concern for thermal failure because the CHF at this location is the minimum according to relevant experimental studies. Thus, the heat flux on the outside surface of the lower head is compared to the CHF to evaluate the thermal success criterion.
- The heat flux from a possible molten metal layer on top of the relocated core debris pool to the internal surface of the side wall of the RPV lower head was compared to the CHF for the same location on the outside of the RPV wall. The heat flux from the metal layer is likely to be higher than the maximum heat flux to the internal surface of the RPV lower head from the relocated core debris. However, the location where the metal layer is in contact with the RPV wall is expected to be where the RPV wall surface is nearly vertical and CHF is near its maximum.

Structural success criterion: The heat flux limited wall thickness (i.e., the thickness of the RPV wall that is sufficiently strong to support the lower head and its contents) for those locations must be also adequate to support the actual loads from the lower head (including its contents and the RPV to CNV pressure difference).

Evaluation of Retention of Core Debris in the Reactor Pressure Vessel

Two bounding assessments are considered to evaluate the success of retention of core debris in the RPV:

1) The first assessment assumes that there is no metallic layer formed above the oxidic debris and that the entirety of the heat generated in the core debris is directed onto the RPV lower head (i.e., no heat loss from the top of the debris). This evaluation uses the ANSYS code to calculate the temperature profile in the RPV lower head shell and the heat flux distribution over the outer surface of the RPV lower head.

2) The second assessment assumes that the downward-facing heat transfer from the core debris to the lower head is minimized and that the remaining decay heat is focused onto the edge of the metallic layer formed above the oxidic debris. This assessment is performed primarily with conservative hand calculations.

The general heat balance for the assumed relocated core configuration is illustrated in Figure 19.2-2 and illustrates the basis for the assessments. It is postulated that under severe accident conditions, large quantities of core debris relocate to the lower plenum of the RPV. Heat transfer from the fallen debris evaporates any remaining water in the lower plenum and begins heating up the vessel structures. The heat source in the system is the radioactive decay of the oxidic materials. A portion of the decay heat is transferred across the vessel wall (the portion of the RPV wall in contact with the debris) to the water in the containment (Q_{down}). The remaining decay heat is transferred to the metallic layer, if present, on top of the debris (Q_{up}), which in turn rejects the heat through the side vessel wall (the portion of the RPV wall in contact with the metal layer) to the water in the containment (Q_{side}) and by radiation to the structures above it (Q_{rad}). Excess heat generated increases the temperature of the oxidic materials. An increase in the core debris temperature enhances the heat transfer out of the core debris, and eventually the system reaches steady state.

Key modeling assumptions for the ANSYS simulation include:

- The decay heat load on the RPV lower head is selected based on a combination of complete core relocation, which is conservative based on MELCOR results, and a rapid time to core relocation.
- A conservative model of the core configuration after a severe accident was assumed. Specifically the debris field is assumed to consist solely of UO_2 which conservatively maximizes the volumetric heat generation rate.
- Conservative modeling of heat load to the RPV lower head was assumed, e.g., heat loss by radiation from the top of the debris was not credited.
- Conservative values of CHF were assumed as the thermal success criterion
- Conservative value of required RPV wall thickness as the structural success criterion was assumed.

Key parameters of the simulation are provided in Table 19.2-1. The ANSYS simulation considers all relocated debris as a solid volume.

The results of the simulation are illustrated in Figure 19.2-3. The figure illustrates that the portion of the RPV lower head shell thickness kept below 900 degrees K (627 degrees C) is much greater than 1.1 cm. This implies that the RPV lower head does not fail structurally under the thermal attack from the relocated core debris.

The RPV bottom head, the transition region to the alignment feature, and the surfaces of the alignment feature were also evaluated in terms of CHF. The intent of the evaluation was to ensure that the maximum heat flux at any point on the outer surface of the RPV lower head is less than the local CHF. Figure 19.2-4 and Figure 19.2-5 illustrate the heat flux on the RPV lower head, vertical portion of the alignment pin and transition fillet. The figures illustrate that the maximum heat flux at the RPV to alignment pin transition is 333 kW/m^2. As stated earlier, experimental studies for hemispherical surfaces suggest that the CHF for this geometry is at least 400 kW/m^2. Figure 19.2-6 illustrates the heat flux on the retention pin bottom surface. This figure indicates that the maximum heat flux on the bottom of the alignment pin is 43 kW/m^2. Experimental studies demonstrate the CHF for this geometry is at least 200 kW/m^2. Thus, the ANSYS simulation results demonstrate that thermal attack from oxidic debris does not result in a challenge to lower head or alignment pin integrity.

The second evaluation considered a focusing effect associated with a potential metallic layer floating above oxidic materials. This evaluation assumes the oxidic core debris is not porous because porosity would prevent the formation of a distinct metallic layer. The height of the metallic layer was calculated based on limiting oxide and metallic mass ratios in the RPV lower plenum calculated by MELCOR. The heat flux is inversely proportional to thickness; theoretically the flux could be maximized with an infinitely thin layer. However, practically, the heat flux from a very thin layer becomes limited because of constraints on the convective and conductive heat transfer radially across the layer. Additionally, when the thickness of the metallic layer is significantly less than the thickness of the vessel wall, conduction in the shell is expected to dissipate the heat axially such that the peak heat flux on the outside surface of the RPV is drastically reduced. The CHF hand-calculated at the location on the RPV vessel of the potential metallic layer is 928 kW/m^2. Conservative calculations, neglecting radiation from the top of the layer, determined the peak heat flux from the side of the layer to be 618.3 kW/m^2, or about 30 percent lower than the CHF. The peak heat flux for a best-estimate calculation with radiation included is only 175.5 kW/m^2. Thus, the focusing effect from a potential metallic layer above oxidic debris does not result in a challenge to RPV integrity.

Summary of Retention of Core Debris in the Reactor Pressure Vessel

An evaluation of the capability of the RPV to retain core debris after a severe accident has been performed using conservative ANSYS modeling and hand calculations. The evaluation considers potential core configurations in the lower RPV head after a severe accident and heat removal characteristics of the RPV, which is immersed in the water retained by the CNV. Boundary conditions for a severe accident are obtained from MELCOR simulations. The analysis demonstrates that the thermal and structural integrity of the lower head is maintained in the event of in-vessel core relocation.

The conservatisms employed in the IVR analysis include:

- bounding decay heat load. Entire core relocates at the earliest onset of relocation.
- no credit for heat removal from the top surface of debris.
- maximized heat transfer to metallic layer for evaluation of the focusing effect.
- zero heat transfer to metallic layer for evaluation of thermal attack from oxidic debris.
- solid debris configuration assumed for maximum heat flux to bottom of lower head (region most susceptible to reach CHF).

- no credit for CHF enhancement from subcooling or pressurization of the containment pool.
- use of CHF exceedence as a criterion for vessel failure (i.e., not accounting for localized transition boiling).

The design characteristics of the NPM that improve the in-vessel retention-RPV capability compared to traditional large light water reactors are:

- retention of water in the CNV allowing passive heat transfer. Loss of RCS inventory and core uncovery is associated with core damage events. Only the potential accident sequences in which containment is isolated are relevant to consideration of in-vessel retention in the RPV. In this situation, the amount of water released to the CNV floods the outside RPV wall to a level that provides efficient cooling of any core debris in the RPV lower head.
- low core power density. The relocated core debris in the RPV lower head has lower volumetric heat generation rate than typical currently operating plants. This is because the NPM has much lower power density and takes a relatively long time to reach core relocation in a severe accident, allowing a significant decrease of decay power.
- small amount of fuel materials. The amount of fuel materials is relatively small so that the core debris has a larger surface area to volume ratio than typical currently operating plants. Thus, the core debris has a large heat transfer surface relative to volume.

In summary, in a core damage event, the NuScale design ensures retention of the damaged core inside the RPV. If containment isolation is successful, there is sufficient water retained in the CNV to provide a continuous, passive heat conduction and convection path from the damaged core to the UHS. Because analysis indicates that failure to retain core debris in the RPV after a core damage accident involving an intact containment does not occur, failure of the RPV is not included in the containment event tree.

19.2.3.2.2 Core Damage Progression with Retention in the Containment Vessel

The NuScale design of a vessel (i.e., RPV) within a vessel (i.e., CNV), combined with the relatively small core size and low power density, indicate that a damaged core would be retained in the RPV for severe accident sequences in which the CNV is intact. As stated in Section 19.2.3.2.1, if the containment barrier is intact such that RCS water lost in a severe accident is retained in the CNV, there is a continuous, passive heat conduction and convection path to remove heat from the damaged core and transfer it to the reactor pool. Thus, retention of core debris within the RPV after a severe accident is ensured. However, for the benefit of demonstrating defense-in-depth with respect to the severe accident mitigating capabilities of the NuScale design, a discussion of the IVR capability of the CNV lower head is provided.

Drawing on similarities with the evaluation of core relocation in the RPV, evaluating the possibility of arresting core damage progression in the CNV is based on an analysis approach similar to that used for RPV retention. In both situations, as illustrated in Figure 19.2-7, core debris relocates to the lower head of a concave vessel with the potential to thermally challenge the lower head.

Evaluation of Core Debris Configuration in the Containment Vessel

As was the situation with the core debris configuration in the RPV, core debris that is hypothetically relocated to the CNV is a self-heating body assumed to be shaped by the geometry of the CNV lower plenum. The average heat flux from the core debris is maximized when the core debris consists only of fuel materials; i.e., the greater the amount of non-heat generating materials that are in the core debris, the smaller the average heat flux over the debris surface.

As illustrated in Figure 19.2-7, the core debris is submerged in water for severe accident sequences involving an intact containment. The water pool overlying the core debris precludes the possibility of the focusing effect on the CNV side wall as a highly conductive molten metallic layer on top of the oxidic debris is not possible given effective upward boiling heat removal. Even in the postulated scenario that a stable insulating vapor blanket forms over the debris and allows for a molten metallic layer, the heat removal from the top of the layer by radiation alone would mitigate a potential focusing effect. As such, the focusing effect is judged not to be a challenge to IVR in the CNV.

Basis for Evaluating Core Debris Retention in the Containment Vessel

Similar to the analysis of IVR in the RPV, the empirical CHF estimates derived from the SBLB tests are judged appropriate for the CNV lower head. While the region underneath the CNV lower head confined by the support skirt and the reactor pool floor differs from the open pool of the SBLB experiments, these geometric differences are judged not to have a significant effect on the CHF because the space underneath the CNV lower head is sufficient to accommodate the open pool boiling two-phase boundary layer. By extension, the open pool boiling CHF estimates derived from the SBLB tests are judged to remain appropriate for the CNV bottom head.

As previously discussed, the core debris in the CNV lower head is submerged in water, so heat removal from the top surface of relocated core debris in the CNV is greater than in the RPV situation. Additionally, the same debris mass has a greater surface area and thinner body in the CNV due to the lesser curvature of the CNV lower head (i.e., larger radius). These factors reduce the steady-state heat flux imposed on the CNV lower head and improve the core debris coolability in comparison to the RPV configuration. Because the CHF was not exceeded in the RPV analysis, it is also not exceeded for the CNV in a location that is in contact with the pool water.

Evaluate Potential Containment Vessel Failure

The CNV lower head has two parts, the curved cap of the vessel and an exterior, structural cylindrical skirt as illustrated in Figure 19.2-8. The space directly under the cap enclosed by the skirt is referred to as the "skirted region." To allow for exchange of coolant flow between the skirted region and the UHS residing outside the skirt, there are numerous large slots evenly spaced just below the joint where the skirt and the cap meet, and numerous small slots also evenly spaced just above the bottom of the skirt. If core debris is in the CNV lower plenum, water in the skirted region is heated and steam is generated. The slots provide pathways for steam generated inside the skirt to escape and for the water outside to flow in. The joint where the skirt and cap meet is designed with a small fillet region directly above the larger skirt slots, which is expected to accumulate a small amount of vapor that cannot be vented by the slots. Because the steam layer blankets a small region of the CNV lower head compared to the thickness of the vessel wall, the local heat transfer degradation is not expected to cause significant local heatup as heat conducts to the well cooled proximities.

The CNV lower head integrity remains coolable as long as the slots provide a sufficient pathway for vapor escape, such that the small vapor region in the fillet does not grow and cause the lower head to exhibit significant dryout conditions and local overheating. Thus, the CNV lower head integrity is challenged only if the holes on the skirt fail to provide sufficient pathways for the steam generated in the skirted region to escape freely.

Summary of Analysis Results

The analysis is based on hand calculations to estimate the volume of steam generated inside the skirted region under the CNV lower head, with the boundary conditions obtained from MELCOR simulations. In the simple analytical model, with a given steam generation rate and a conservative loss coefficient through the slots, the height of the steam layer in the skirted region relative to the top of the upper slots is calculated. Assumptions for the conservative sensitivity case were applied as follows:

- The decay heat load on the CNV lower head is selected based on a combination of 92 percent UO_2 relocation with no relocation of metallic materials and conservatively rapid time to core relocation.
- Energy required to bring the subcooled reactor pool water to the saturated condition is ignored.
- Heat loss through the skirt is ignored.
- Heat flux from the top of the core debris is eliminated (representing no coolant in the CNV), resulting in the highest possible heat flux to the CNV lower head.

In this conservative sensitivity case, the height of the steam-trapped fillet region under the skirt is increased from 1 inch to 1.496 inches, and using more realistic relocated mass and heat transfer from the top of the debris, the height increases to 1.233 inches. This is a minimal increase, especially compared to the CNV vessel thickness of 3 inches. As a result of the configuration of the slots in the skirt, a natural circulation flow will develop with liquid flow entering the skirt from the bottom slots and a two-phase liquid and steam flow exiting through the top slots. Because of the stable two-phase flow out of the top slots, the free flow of steam from the skirted region is unimpeded by recirculating or counter-current flows.

The analysis concludes that the minimal steam accumulation in the skirted region does not lead to significant dryout of the CNV lower head, therefore melt-through or structural failure is not predicted by analysis. Thus, the CNV would retain core debris in the event of RPV failure.

Analyses and simulations of core damage scenarios predict no CNV failure. Although the IVR analysis explicitly incorporated a number of uncertainties by conservative selection of analysis parameters, other phenomenological uncertainties may remain (e.g., critical heat flux, focusing effect, intermetallic reactions). However, even if the CNV were postulated to fail, resulting in fuel on the floor of the reactor pool, the reactor pool water would effectively scrub radionuclides and prevent a large release to the environment.

19.2.3.3 Severe Accident Mitigation Features

Features that mitigate a potential severe accident are summarized in this section. The potential for cooling the RPV from the outside is facilitated by the containment design as discussed in Section 19.2.3.3.1. Section 19.2.3.3.2 through Section 19.2.3.3.6 address the capability of the NuScale design with respect to potential containment challenges if core debris is not retained in the active core region of the RPV in a severe accident. Section 19.2.3.3.7 deals with other potential mitigation features and Section 19.2.3.3.8 addresses equipment survivability in the CNV during a potential severe accident. Because of unique characteristics of the NuScale design, analysis indicates that the only mechanism for failure of the containment function is containment bypass or failure of containment isolation.

19.2.3.3.1 External Reactor Vessel Cooling

In the event of a severe accident with associated core damage, external reactor vessel cooling refers to the capability of cooling a core debris bed retained in the RPV by means of heat conducted through the RPV wall. The NuScale design with its small core, low power density and large surface-to-volume ratio facilitates external RPV cooling. Additionally for all intact containment accidents, coolant is retained in the CNV, surrounding the RPV vessel. The result of these features of the NuScale design is that retaining core material in the RPV is demonstrated for sequences with core damage and intact containment, as discussed in Section 19.2.3.2.1.

19.2.3.3.2 Hydrogen Generation and Control

Hydrogen is a highly flammable gas which is highly diffusive and buoyant. Deflagration and detonation are two different combustion processes that require separate consideration. In a deflagration, the combustion wave propagates at a velocity less than the speed of sound. In detonation, the combustion wave propagates at a velocity greater than the speed of sound, which creates a high-pressure shock wave that can cause significant damage on the structure it contacts. Key properties of hydrogen relevant to and as informed by Reference 19.2-24 through Reference 19.2-29, include:

- Hydrogen is flammable over a wide range of concentrations. Changes in pressure or temperature cause the upper flammability limit to change. When steam concentrations exceed about 55 volume percent, the system is no longer flammable. Under the conditions of the CNV during a severe accident, volume percent and molar percent can be taken as equivalent.

- Hydrogen forms a flammable mixture with air at ambient conditions and its ignition energy is also low (about one-tenth of that required for gasoline vapors).
- Air concentrations must be greater than 20 volume percent in order to allow hydrogen deflagration (air is about 21 volume percent oxygen, so the minimum oxygen concentration that allows hydrogen deflagration is about 4 percent by volume).

The potential for hydrogen combustion is minimized in the NuScale design based on the following considerations with respect to initial conditions and severe accident conditions:

Initial Conditions

- As stated in Section 6.2, during normal operation, a near vacuum is maintained in the CNV by the containment evacuation system (CES). Thus, the initial containment pressure with respect to the containment design pressure is very low.
- Due to the very low initial containment pressure and small free volume of the containment, the amount of oxygen initially present in the containment is very small.
- The initial hydrogen concentration in containment is negligible because the amount of air in the containment is very low and the fraction of hydrogen in air is very small. While there is some hydrogen in the RPV during steady-state operation (for water chemistry purposes), this would not transport to the containment until after a potential accident had initiated.
- The CNV is not compartmentalized, thus significant differences in localized gas concentrations are not a concern, consistent with the requirement of 10 CFR 50.44(c)(1).

Severe Accident Conditions

The only source of oxygen generation during severe accidents with an intact containment is the radiolysis of water, which is relatively slow because of the relatively low decay power in the NPM. In terms of concentration (by mole or volume), the oxygen concentration is 21 percent initially as the gases in the containment are only air. However, because the total oxygen molar inventory is minimal, the initial 21 percent concentration of oxygen decreases to well below 4 percent as soon as any vapor or gases from the RPV are released into containment. Initially, steam is the dominant gaseous species, causing a steam-inert environment. After the core becomes uncovered, cladding oxidation results in the large production of hydrogen that drives the oxygen concentration well below combustion limits. In the long-term, the amount of oxygen increases slowly as both oxygen and hydrogen are generated in a stoichiometric ratio by radiolysis of coolant, potentially reaching combustible limits after several weeks.

Containment leakage has a negligible effect. Technical specifications include a requirement that containment pressure be maintained at a near vacuum. For an intact containment, the containment leak rate is small, as defined in Section 6.2; thus, oxygen that leaks out of the CNV is not subtracted from the oxygen generated by radiolysis when calculating concentration. Further, leakage is indiscriminate among the gases, so the flammability limits are not significantly affected by leakage.

In general, for a light water reactor severe accident evaluation, potential sources of hydrogen during a severe reactor accident are:

- steam-zirconium oxidation reaction
- steam-steel oxidation reaction
- radiolysis of water
- core-concrete interaction
- corrosion of zinc-based paint and galvanized steel
- corrosion of aluminum

The steam-zirconium and steam-steel reactions are the most important hydrogen sources. Core-concrete interaction is not applicable as concrete is not used in the CNV. Hydrogen from zinc, galvanized steel, or aluminum is small in comparison to the zirconium and radiolysis sources which produce enough hydrogen to burn all available oxygen.

The selection of severe accidents for assessing the potential for hydrogen combustion is based on a review of applicable phenomena with the objective of identifying those severe accident scenarios that represent the limiting challenge to containment integrity and the bounding potential source term. Based on this evaluation, the most important parameters for hydrogen production are the timing of core damage events, the presence of steam in the RPV and the flow rate of steam through the RPV. The CDF for specific severe accident sequences was not considered as a primary factor in the bounding accident selection because all sequences have a very low calculated CDF.

For significant amounts of hydrogen to be produced in a severe accident sequence, the core must be uncovered, and remain uncovered for multiple hours. In the NuScale design, a pipe break or valve failure followed by multiple mitigation system failures can result in a loss of RCS inventory and core uncovery. Examples of such events are a CVCS LOCA, an RSV failing open, and a spurious ECCS valve actuation. Because the timing of core degradation is important with respect to hydrogen generation, the accidents selected for evaluation include severe accident sequences with:

- the largest combined flow area resulting from a pipe break and open ECCS valves (Simulation LCC-05T-01: CVCS LOCA with RVVs opening upon actuation signal; RRVs fail to open).
- largest flow area through open ECCS valves (Simulation LEC-06T-00: spurious RVV actuation with all RVVs opening upon actuation signal; RRVs fail to open).

- largest flow area resulting from a single pipe break (Simulation LCC-05T-02: CVCS LOCA with no ECCS valves opening).
- smallest flow area through an open RCS valve (Simulation TRN-07T-01: RSV failed open with no ECCS valves opening).
- very small flow area from an incomplete pipe break (Simulation LCC-05T-03: 20 percent full flow area CVCS LOCA with no ECCS valves opening).

This wide range of flow areas considered for RCS coolant loss produces significant variation in the timing of key events such as core uncovery, onset of core damage, and core relocation. Consideration of multiple locations, flow areas, and ECCS failure modes results in significant variation among the flow paths and flow rates of steam through the RPV. The simulations that were evaluated for potential hydrogen combustion are listed in Table 19.2-2.

Figure 19.2-9 shows the hydrogen mass versus time for the evaluated severe accident cases. The figure illustrates that hydrogen generation is significant for all cases, with the maximum production from Case TRN-07T-01. There is a definitive trend that slower core damage results in greater hydrogen production as the active fuel region is hotter for a prolonged period prior to partial relocation to the lower plenum. The range of total hydrogen produced from the five intact containment severe accidents is 122.1 lbm (27,500 moles) to 222.9 lbm (50,200 moles) which includes oxidation of cladding and supporting steel. A fuel-clad coolant reaction of 100 percent is calculated to produce 46,671 moles of hydrogen; thus, the maximum from the severe accident cases bounds 100 percent fuel-clad coolant reaction.

Figure 19.2-10 illustrates the oxygen concentration (mole fraction) in the highest elevation control volume modeling the CNV versus time for the evaluated severe accident cases. This location is representative of the entire CNV atmosphere space. The figure shows the initial concentration of 21 percent for natural air, dropping to less than 1 percent due to steaming as RCS fluid flashes to steam, an increase to a maximum of 3.2 percent as steam condenses, and then a second decrease as hydrogen is generated due to cladding oxidation and thus the mole fractions of oxygen and other gases are decreased. The oxygen concentration remains below one percent as hydrogen generation ceases.

Deflagration-to-Detonation Transition

Deflagration-to-detonation transition is a potential mode to initiate a detonation through flame acceleration from a deflagration. The margin to design stress limits for a deflagration-to-detonation transition load is presented in Section 6.2.5.3 and is not covered further in this section.

Adiabatic Isochoric Complete Combustion

From Section 6.2.5.3, the containment can withstand the structural effects of a global deflagration, reflected detonation load, and deflagration-to-detonation transition load within 72 hours. To provide additional insight into the potential challenge to containment should a long-term hydrogen deflagration occur after

72 hours, an evaluation of adiabatic isochoric complete combustion was performed using the MELCOR code. A simple model of the CNV was created with initial conditions taken from engineering calculations and limiting results of the severe accident simulations specified in Section 19.2.3.2. The evaluation produces conservative values of pressure and temperature because:

- the combustion is assumed to be adiabatic, so that heat loss to the heat structure is ignored.
- the combustion is assumed to be complete, burning 100 percent of the limiting reactant gas species (oxygen).
- the combustion is assumed to take place in a constant containment volume without allowance for pressure relief by the available RPV volume (i.e., isochoric).

As discussed earlier, the conditions for combustion are disallowed by excess steam or hydrogen after a severe accident. Therefore, after a severe accident, combustion is only possible following an extended period of radiolysis causing the oxygen concentration to increase to the minimum combustible limits. The base case adiabatic isochoric complete combustion analysis uses a radiolysis limit of 30 days, which is judged to be a reasonable time for actions to mitigate a beyond design basis, severe accident challenge. The total moles of oxygen are determined from the 30 day radiolysis production combined with initial oxygen due to air in containment. It is conservatively assumed that all oxygen produced by radiolysis remains in the CNV. The moles of hydrogen are calculated so that oxygen will be just above a 4 percent concentration, the lowest combustion limit. The number of moles of hydrogen calculated by this method is greater than that produced by 100-percent fuel clad-coolant reaction. The resulting maximum containment pressure from adiabatic isochoric complete combustion after 30 days of radiolysis is calculated to be approximately 860 psia, below the CNV design pressure. Therefore, the conservative adiabatic isochoric complete combustion analysis with several weeks of oxygen production demonstrates that hydrogen combustion does not pose a credible risk to the NuScale CNV.

Adiabatic Isochoric Complete Combustion Sensitivity Study

An additional adiabatic isochoric complete combustion calculation was performed to analyze a combustion event based on the maximum hydrogen production from the severe accident simulations specified in Section 19.2.3.2. It is conservatively assumed that all produced hydrogen is in the CNV at the time of combustion. Oxygen and hydrogen are produced by radiolysis until oxygen exceeds a 5 percent concentration, which is the MELCOR default lower limit and is more challenging for this sensitivity as it increases the total available moles of oxygen for combustion. It is estimated that radiolysis would have to proceed uninhibited for 45 days to produce such an oxygen concentration. The adiabatic isochoric complete combustion calculation results show that the post-deflagration pressure for the sensitivity case is approximately 920 psia, which remains below the containment design pressure.

In summary, over-pressurizing the NuScale CNV due to hydrogen combustion is physically unrealistic due to the very limited oxygen concentration before and after postulated severe accidents. The post-deflagration pressures from conservative adiabatic isochoric complete combustion calculations are below the CNV design pressure. Based on these results, containment structural integrity is maintained for a severe accident that releases more hydrogen than would be generated from 100 percent fuel clad-coolant reaction accompanied by hydrogen burning as required by10 CFR 50.44 (c)(5). In these calculations, oxygen, not hydrogen, is the limiting reactant for combustion.

19.2.3.3.3 Core Debris Coolability

As discussed in Section 19.2.3.2.1 and Section 19.2.3.2.2, core debris coolability is ensured in both the RPV and CNV lower heads. The NuScale design does not include concrete inside the CNV. Thus, molten core-concrete interaction is not applicable to the NuScale design.

19.2.3.3.4 High-Pressure Melt Ejection

High-pressure melt ejection (HPME) refers to the phenomenon of RPV failure at high pressure with the result that core debris is ejected and dispersed throughout the containment. A concern of HPME is the threat to the containment integrity due to direct containment heating causing a rapid heating of the containment atmosphere. Another potential threat to containment is associated with direct contact of the dispersed debris with the metal containment itself. Literature sources indicate that a significant pressure differential between the RPV and containment is required to cause HPME from the RPV. While there is not a commonly accepted value for the necessary pressure differential to support HPME, literature sources (Reference 19.2-21, Reference 19.2-22, and Reference 19.2-23) indicate that a pressure differential greater than 100 psid is required. As indicated below, HPME cannot occur in the NuScale design because a significant pressure differential between the RPV and CNV cannot exist at the time of core relocation.

In the NuScale Power Plant design, the passive DHRS and ECCS are designed to provide efficient primary system heat removal and to effectively depressurize the RPV in response to an initiating event. If the RPV is not depressurized by these safety systems, depressurization occurs due to a loss of RCS inventory resulting from the initiating event (e.g., a LOCA or inadvertent valve opening). The inventory lost from the RCS is retained in the CNV and provides a heat transfer medium between the RPV and CNV, and then to the UHS. As a result of this heat transfer, pressures in the RPV and CNV equalize; therefore, there is no driving pressure for HPME to occur.

The severe accident simulations presented in Section 19.2.3.2 were reviewed to evaluate the potential for high pressure melt ejection. Because every simulation results in the relocation of at least nine fuel assemblies to the RPV lower plenum, all have the potential for HPME.

Figure 19.2-11 illustrates that after the time of core relocation to the RPV lower head (as presented for each sequence in Section 19.2.3.2) the pressure differential between the RPV and CNV in every simulation is less than 75 psid. Further, the RPV and CNV reach pressure equilibrium well before the RPV lower head temperature increases to the point at which RPV failure could be postulated. In this equilibrium configuration, the pressure in the lower volume of the CNV exceeds that in the RPV due to the hydrostatic head of water in the CNV, indicating that there is no driving force for HPME, if RPV failure were postulated. Therefore, an HPME and the associated potential threat to containment integrity does not occur, regardless of break location or size.

19.2.3.3.5 Fuel-Coolant Interaction

The potential for an adverse interaction of molten fuel and coolant during a severe accident, either in the RPV ("in-vessel") or external to the RPV if molten fuel is not retained ("ex-vessel"), was evaluated. Fuel-coolant interaction can result in an energetic and rapid phase transition from liquid water to steam, referred to as a "steam explosion." During the transition, expanding fluids perform work, thereby challenging the integrity of the RPV or CNV. While traditional evaluations of steam explosions and empirical data suggest molten fuel is a requirement for a fuel-coolant interaction, molten fuel is not expected based on severe accident MELCOR modeling. Regardless, an evaluation was performed based on the consideration of certain fundamental characteristics of energetic steam explosions, such as:

- a significant amount of molten corium above a water pool is required so that sufficient thermal energy exists to produce a steam explosion.
- a significant water pool is required so that sufficient inventory exists for an explosive transition from liquid water to steam.
- a larger fall height of debris into a deep water pool facilitates the breakup of debris. This initial breakup is a precursor to debris fragmentation, which is needed for rapid heat transfer associated with an energetic steam explosion.
- a large void (steam) fraction can prevent spontaneous occurrence of a steam explosion because a large steam fraction (large film thickness) makes debris-liquid contact difficult. Thus, explosions in saturated water are more difficult to trigger than in subcooled water.
- the presence of non-condensable gases in the mixture (e.g., hydrogen production due to corium oxidation by the steam as would occur in a severe accident) has a cushioning effect that hinders film collapse during the triggering stage of fuel-coolant interaction. The resistance to film collapse impedes fuel-coolant interaction.
- a steam explosion is more difficult to trigger spontaneously when the system pressure is high because the stability of the vapor film increases with pressure. Additional energy relative to lower pressure situations is required to collapse this vapor film.
- a "melt pour" type of interaction (i.e., corium poured into a water pool) bounds the energetics associated with a "stratified" type of interaction (i.e., water flooding a corium debris bed).

The potential for in-vessel and ex-vessel steam explosions are discussed in more detail below.

In-Vessel Steam Explosion

The "alpha mode" of containment failure is considered with regard to its potential in the NuScale design. In the alpha mode, the concern is that a steam explosion inside the RPV could induce a water slug which could impact the uppermost structures of the RPV or induce significant dynamic loading challenging the integrity of the RPV. If such an event were to occur, a sudden increase in energy within the RPV could challenge RPV section and bolted interfaces, potentially compromising vessel integrity. If this were to happen, it could cause failure of the upper head, potentially resulting in containment failure. The issue is described in NUREG-1524, NUREG/CR-5030, and Corradini et al (Reference 19.2-19, Reference 19.2-31, Reference 19.2-32, respectively).

For an in-vessel steam explosion, the body of molten corium is in the core region above the core support plate, while the water pool is below the plate. The potential for an in-vessel steam explosion in the NuScale design is minimized based on the size of the NuScale core, physical dimensions of the RPV, and thermal-hydraulic conditions within the RPV, including:

- The amount of melt available for steam explosion is small. The thermal-hydraulic analyses, as described in Section 19.2.3.2, conclude that the core support structure is expected to fail prior to significant core melting. Thus, there is limited potential for interaction between a significant amount of suspended molten corium mass and a water pool within the RPV.
- Fuel materials are predominantly solid, rather than molten. As such, debris fragmentation following a core relocation event is unlikely. Without a breakup of core materials, rapid thermal-energy transfer between fuel and coolant is difficult.
- Water volume and associated water mass in the RPV lower plenum is small. Small dimensions limit the potential for corium fragmentation and inhibit energy transfer to existing coolant.

To provide additional insight into the potential for a steam explosion to damage the RPV (and subsequently to induce an “alpha-mode” containment failure), an analysis is performed postulating the occurrence of an in-vessel steam explosion. To understand the release of energy as a result of the process, the Hicks-Menzies thermodynamic model of a steam explosion is used (NUREG-1524). The Hicks-Menzies model represents a thermodynamic maximum of the work potential of an expanding fluid. As such, calculated core debris energy and coolant expansion work is inherently conservative. The model assumes fuel and coolant achieve thermodynamic equilibrium in an adiabatic and isochoric process. Energy is then released as a result of fluid expansion during an isentropic process. During expansion, coolant internal energy decreases as work is performed on the RPV. To demonstrate RPV integrity following a steam explosion, the energy associated with coolant expansion is compared to, and must be less than, the energy of a pressurized fluid within the RPV at the ultimate failure pressure of the vessel. This comparison serves as the basis to describe the capacity of the RPV against in-vessel FCI expansion work.

To evaluate the thermodynamic model of this phenomenon, parameter values were selected for corium mass, corium temperature, initial RPV system pressure, and coolant mass so that the conversion of thermal energy in the fuel to mechanical work by the expanding coolant is maximized.

Severe accident sequences with an intact containment (i.e., break inside containment or break outside containment, but isolated) and core relocation are of interest for the evaluation of an in-vessel steam explosion. Sequences with a breached or bypassed containment already contain a release pathway. As such, the alpha-mode containment failure is not of additional consequence. MELCOR cases satisfying this criterion are provided in Table 19.2-10. Within this table, each case is summarized and key characteristics, parameters, and initial state values relevant to the steam explosion analysis are provided.

From MELCOR results, observations of the NPM design were confirmed, including relocated core material configuration and the available coolant inventory. Because core relocation occurs as a result of support plate failure at temperatures less than the melting temperature of oxidic fuel materials, relocated corium within the RPV is largely a solidified mass, and not molten. Furthermore, limited coolant inventory within the RPV reduces the potential for energetic steam explosions to perform work on the RPV during fluid expansion.

The result of the Hicks-Menzies thermodynamic analysis shows a high conversion ratio of thermal energy in the fuel to mechanical energy as coolant expands to fill the full volume of the RPV. All expansion energy is assumed to transfer to an upward liquid water slug and no energy loss is assumed for dissipation in the upper internals of the RPV. As a result, the energy applied to the upper head of the RPV is conservative. Furthermore, because the NuScale core is small, relocated fuel materials contain a relatively small amount of initial thermal energy. This limits the potential for coolant to perform work on the RPV during the expansion process. Consequently, work performed on the RPV by expanding coolant is insufficient to challenge vessel integrity.

Uncertainty in input parameters is considered by using the results of MELCOR accident simulations to inform the analysis of in-vessel FCI. A probability distribution for each input parameter is created using the minimum and maximum values from the MELCOR accident simulations presented in Table 19.2-10. A uniform distribution is applied between those bounds with a lognormal distribution describing extreme values of each distribution which are beyond the extreme values predicted by MELCOR simulations. Random samples for each input parameter are then acquired via Monte Carlo sampling and used to evaluate the Hicks-Menzies model. No combination of sampled input parameters results in failure of the RPV as a result of an in-vessel FCI.

With a significant amount of solid (versus molten) material in relocated core debris, the potential for an in-vessel steam explosion is highly unlikely. Further, conservative thermodynamic analysis assuming fragmentation and heat transfer corresponding to molten debris (irrespective of debris temperature) found that the energy released from a hypothetical steam explosion is insufficient to challenge RPV integrity. As a result, the alpha-mode of containment failure cannot occur.

Ex-vessel Steam Explosion

As discussed in Section 19.2.3.2.1, analysis demonstrates that failure of the RPV after a core damage accident involving an intact containment does not occur. As a result, a very rapid or instantaneous interaction of fuel materials inside of the RPV and liquid coolant in the CNV does not occur; therefore, a quantitative analysis postulating such conditions was not performed.

However, from the perspective of demonstrating defense-in-depth, several aspects of the NuScale design minimize the possibility of an ex-vessel FCI:

- Considering a situation with an intact containment, the RCS water relocated to the CNV, and a failed RPV lower head, the distance between the bottom of the lower head of the RPV and the CNV is small and MELCOR accident sequences with an intact containment predict this space to be occupied by a water pool. An energetic FCI requires space between molten fuel materials, if present, and a water pool to promote material breakup. Breakup helps create a larger total surface area for contact with liquid coolant, thereby increasing rapid heat transfer. Because accident sequences with an intact containment contain a significant amount of liquid coolant in the annular region between the RPV and CNV, there is no available space between a failed RPV lower head and the water pool beneath to foster material breakup needed to promote an energetic transfer of heat to the water pool in the CNV.
- The CNV is not large enough to allow for a relocation of all core materials from the RPV to the CNV. Because of the limited space between the RPV and the CNV, a significant portion of the fuel material will remain backfilled within the RPV above a fuel mass in the CNV. This prevents fuel material from interacting with a water pool in containment. Coupled with the small size of the NuScale core, a relocation of fuel materials from the RPV to the CNV will involve less material than a similar FCI within the RPV, further limiting the potential energy transference necessary for an energetic ex-vessel steam explosion.
- Because of the large water pool predicted to reside in the containment annulus, the resultant conversion ratio for an ex-vessel FCI will be significantly less than the predicted ratio using the Hicks-Menzies thermodynamic model of an in-vessel FCI (which was shown to not challenge RPV integrity), thereby limiting the potential for work to be performed on the CNV by expanding coolant.

For these reasons, the potential for efficient transfer of thermal energy between fine fuel materials and coolant (which is required for an energetic ex-vessel FCI) is minimized.

Summary of Results

Analysis results and assessment of design features demonstrate that the potential for an energetic in-vessel or ex-vessel FCI is minimized. Additionally an analysis of in-vessel FCI demonstrated that there would not be sufficient energy to fail the RPV. Therefore, FCI is not predicted to threaten containment integrity. However, in consideration of phenomenological uncertainties (e.g., corium temperature, vessel failure energy), a postulated FCI that fails the CNV was evaluated. MELCOR simulations documented in Section 19.2.3.2 show that at the earliest possible time of FCI, the airborne fraction of volatile fission product aerosols is less than NuScale's calculated threshold for a large release, as determined in Section 19.1.4.2.1.4. Therefore, the evaluation demonstrates that an instantaneous release of the entire airborne aerosol inventory at the time of a postulated FCI would not constitute a large release.

19.2.3.3.6 Containment Bypass

A containment bypass is a flow path that allows an unintended release of radioactive material directly to the Reactor Building, bypassing containment. Core damage sequences that include containment bypass or failure of containment isolation are assumed to result in a large release as defined in Section 19.1.4.2.1.4. No distinction is made between "early" or "late" releases. Containment bypass could occur through (i) failure of containment isolation or (ii) steam generator tube failure (SGTF) concurrent with failure of secondary-side isolation on the failed steam generator (SG). Containment bypass is represented by top event CNTS-T01 as discussed in Section 19.1.4.2.1.3.

Containment Isolation Failure

As stated in Section 6.2.4, the containment system design provides for isolation of systems that penetrate the CNV. The design is reflected in a containment isolation and bypass model as summarized in Section 19.1.4.2.1.3.

Thermally-Induced Steam Generator Tube Failure

In the NuScale design, the SG bundles are integrated within the RPV; they form part of the RPV reactor coolant pressure boundary. In contrast with conventional pressurized water reactors, the primary reactor coolant circulates over the outside of the SG tubes, with the steam-formation occurring in the secondary coolant on the inside of the SG tubes. As such, the NuScale SG tubes operate with the higher primary pressure on the outside of the tubes and lower secondary pressure on the inside of the tubes. The result is that there are predominately compressive stresses on the tubes versus the typical tensile stresses. Because the mechanism for fatigue crack propagation is tensile stress, the NuScale SG pressure conditions are expected to prevent crack propagation.

Due to the lack of data on thermal-induced SGTFs for the NuScale design, an evaluation of creep rupture was performed based on historical data for conventional SG tube flaws and time-history temperature and pressure conditions representative of NuScale severe accident sequences.

The SG tubes under severe accident conditions typically have a much higher probability of failure because of the higher temperatures during a severe accident. The probability of an SGTF is calculated using the tube failure /creep rupture model presented in NUREG-1570 (Reference 19.2-33). Although the formulations employed for predicting creep rupture are based on internally pressurized tubes, the NuScale steam generator tubes are externally pressurized. As a result, the calculated probability of a thermally induced SGTF is judged to be overestimated because creep progresses more vigorously under tension than under compression. The nominal temperature and stress conditions that the tubes are exposed to are derived from a representative MELCOR severe accident simulation. Uncertainty is accounted for by imposing a distribution about the nominal values for temperature, pressure, and the Larson-Miller parameter. The probability of such a failure is incorporated into the Level 2 PRA as described in Section 19.1.4.2. In the Level 2 PRA, if a core damage event causes a thermally-induced SGTF with concurrent failure of the secondary-side isolation valves on the damaged SG, a containment bypass accident has occurred and a large release is assumed. A thermally induced SGTF does not pose a unique severe accident phenomena risk that would threaten the CNV, and is not analyzed deterministically.

19.2.3.3.7 Other Severe Accident Mitigation Features

The NuScale design includes additional features that are relevant to mitigation of severe accidents. In addition to the capabilities summarized in the prior sections, the design includes unique features that are not explicitly credited in the PRA.

- Partial immersion of the CNV in the reactor pool provides radionuclide scrubbing in the event of CNV lower head failure.
- For severe accidents with CNV bypass or containment isolation failure, the release would potentially be further reduced by the Seismic Category I Reactor Building.

19.2.3.3.8 Equipment Survivability

Consistent with SECY-90-016, SECY-93-087, and SECY-94-302 (Reference 19.2-15), equipment required to mitigate severe accidents is evaluated to perform its intended severe accident functions. As stated in the references, the evaluation is intended to demonstrate that there is reasonable assurance that equipment needed for severe accident mitigation and post-accident monitoring (including the capability to monitor combustible gases as required by 10 CFR 50.44(c)(4)) will survive in the severe accident environment over the time span for which it is needed. Severe accident environmental conditions may produce extremes in pressure, temperature, radiation, and humidity.

Following a severe accident in which core damage has occurred, the two functions that must be maintained are containment integrity and post-accident monitoring (including the capability to monitor combustible gases). Post-accident monitoring is not relied upon for mitigating severe accidents, but is intended only to provide information on severe accident conditions as required by 10 CFR 50.34(f)(2)(xix).

The time span over which survivability is reasonably assured is specific to the equipment and its function. All equipment that is necessary to maintain containment integrity is reasonably assured to survive for at least 24 hours after core damage. Equipment used for post-accident monitoring, except for combustible gas monitoring, is reasonably assured to survive for a duration based on the variable monitored and what operators would do with that information, with a maximum duration of 24 hours after core damage. Equipment that is necessary for continuous monitoring of combustible gases is reasonably assured to survive for at least 72 hours.

Equipment is qualified to 100-percent humidity. In terms of post-accident dose, the NuScale design has used a methodology for assuring equipment survivability based, in part, on environments predicted for severe accidents as modeled in the NuScale PRA. This approach provides confidence that the equipment needed for severe accident mitigation and monitoring survives over the time span in which it is needed. Equipment survivability in a radiation environment is first evaluated by comparing the severe accident dose to the environmental qualification design-basis dose. The severe accident dose is based on the core damage source term described in Section 15.10. For cases in which the environmental qualification dose is larger, survivability is assured. For cases in which the severe accident dose is larger, qualitative assessments, testing, or additional analyses are performed to assure survivability.

Post-accident temperature and pressure conditions are discussed with regard to containment integrity and post-accident monitoring capabilities as follows.

<u>Containment Integrity</u>

Containment integrity is the only safety function relied upon for severe accident mitigation. The function is ensured through successful closure of the containment isolation valves and ensuring that the CNV, including penetrations and seals, remains intact. Given how early a containment isolation signal is generated following postulated PRA initiating events, containment isolation valves are expected to reach the desired position well before core damage occurs.

Simulation results confirm the NPM remains below CNV temperature and pressure limits for all accident sequences considered in the PRA. The two most challenging transients with respect to CNV temperature and pressure loads are the CNV response to an ultimate failure of the RPV due to overpressurization and the CNV response to an adiabatic complete combustion of the hydrogen conditions described in Section 19.2.3.3.2. Thermal-hydraulic results show that even if the RPV were to fail due to overpressurization, the CNV ultimate failure pressure would not be exceeded and any RPV-CNV pressure differential would subside well before core damage. A conservative thermodynamic analysis of a complete combustion of the hydrogen/oxygen inventory described in Section 19.2.3.3.2 imparting all energy adiabatically and directly into the exposed CNV steel (exposed on the inside-surface) confirms that the steel temperature would rise less than 75F, remaining well below the CNV design temperature.

NuScale's unique and robust design has reduced or eliminated many of the traditional failure mechanisms that challenge containment integrity once it is successfully isolated. Section 19.2.3.3 further discusses a module's response to such challenges.

Post-Accident Monitoring

In the NuScale design, no post-accident monitoring variables are required to mitigate a severe accident. Each Type B, C, and D post-accident monitoring variable is included in the equipment survivability assessment. Additionally, the containment evacuation system containment isolation valves, containment flooding and drain system containment isolation valves, containment isolation valve hydraulic skids, containment gas sample pump, and combustible gas monitors are included for the monitoring of combustible gases. The pump and monitors provide the capability to continuously monitor, whereas the containment isolation valves and skids are only needed to start monitoring.

Following a severe accident, there is reasonable assurance that monitoring capability is maintained if the conditions experienced during the accident progression are not significantly harsher than the conditions for which the equipment is qualified.

The instrumentation in and directly around the core may be subject to more extreme conditions during core damage, but the utility of such monitoring variables diminishes greatly after core damage has occurred.

As shown in Figure 19.2-12, the simulation results from the severe accident cases in Section 19.2.3.2 exhibit RPV shell temperatures that do not increase above the RPV design temperature, even after core damage and relocation. Figure 19.2-12 does not include the temperature of the RPV lower head because the NuScale RPV lower head is not designed with instrumentation for post-accident monitoring. Severe accident module pressures are also not of significant risk, as discussed in Section 19.2.3.3.4. The relatively benign severe accident conditions are attributed to the effective passive heat removal through the CNV to the UHS, further enhanced by the retention of primary coolant in the CNV.

In a post-accident environment, the RPV shell temperature provides an upper bound of the temperatures experienced inside the CNV. Considering that severe accident simulations show that the RPV shell temperature does not exceed the equipment qualification temperature for instruments inside the CNV, there is reasonable assurance that post-accident monitoring will be maintained during a severe accident.

The remainder of instrumentation for post-accident monitoring is exterior to the CNV, such as containment isolation valve position indication, which experience conditions much less severe than those on the RPV and are reasonably assured to survive severe accident temperature and pressure conditions. Combustible gas monitoring is part of the NuScale design and does not require equipment inside the CNV.

19.2.4 Containment Performance Capability

As discussed in SECY 90-016, SECY 93-087 and associated staff requirements memoranda (Reference 19.2-4, Reference 19.2-5, Reference 19.2-13, and Reference 19.2-14), containment performance with regard to severe accidents is evaluated using deterministic and probabilistic approaches.

Deterministic Evaluation of Ultimate Pressure Capacity

An evaluation of the ultimate pressure capacity of the CNV is provided in Section 3.8. The evaluation demonstrates that the ultimate pressure capacity significantly exceeds the design pressure. The results of severe accident MELCOR simulations, as presented in Section 19.2.3.2 confirm that the CNV withstands the pressures associated with severe accidents, which are less than both the design pressure and the ultimate failure pressure, including the pressure associated with potential hydrogen generation, consistent with requirements in 10 CFR 50.34(f)(3)(v)(A)(1) and 10 CFR 50.44. The design of the UHS prevents the CNV pressure from increasing significantly after 24 hours, thereby ensuring the CNV continues to provide a barrier against the uncontrolled release of fission products. Further, the CNV is shown to maintain structural integrity from potential hydrogen combustion, eliminating the need to manage combustible gases in order to maintain control of the containment boundary in the event of a severe accident. Finally, NuScale has no safety-related low-pressure injection that requires venting to atmosphere. Thus, a containment vent is unnecessary in the NuScale design.

Probabilistic Evaluation of Containment Performance

Using a probabilistic approach, the conditional containment failure probability (CCFP) should not exceed 0.1. This criterion has been applied to the NuScale module in the following manner.

- The criterion is applied to internal and external event scenarios when a module is operating at power. During low power and shut down operation, the containment may not be credited in some plant operating states; thus, the criterion is not a useful indicator of containment performance.
- The CCFP is defined as the ratio of the large release frequency over the core damage frequency. As discussed in earlier sections, the only mode of containment failure evaluated probabilistically is bypass or failure of containment isolation; analysis indicates that other severe accident containment challenges do not occur.

The composite CCFP for a module is calculated to be less than 0.1, which meets the safety goal, as discussed in Section 19.1.

Combustible Gas Control

Containment performance is ensured also by achieving combustible gas control. During normal plant operation, combustible gas control is achieved by maintaining a near vacuum in the CNV by the CES. As discussed in Section 19.2.3.3.2, during severe accident conditions combustible gas control is provided initially by the steam-inert environment and later by the large production of hydrogen that reduces oxygen concentration below combustible limits. Additionally, an adiabatic isochoric complete combustion analysis was performed to evaluate the ability of the CNV to cope with combustible gases generated by radiolysis occurring for weeks after a severe accident. The analysis showed the resulting containment pressure was calculated to be below the CNV design pressure which demonstrates that hydrogen combustion does not pose a credible risk to the NuScale CNV. A listing of SSC that are required to remain functional following a hydrogen combustion event to support containment integrity and core cooling is provided in Section 3.3.5 of TR-0716-50424, Revision 0, "Combustible Gas Control" Technical Report (Reference 6.2-3).

Summary of Containment Performance

Consistent with SECY-93-087, deterministic and probabilistic evaluations of containment capability have been performed. The deterministic evaluation of containment capability in comparison to potential severe accident challenges confirms that the CNV is a leak-tight barrier for a period of at least 24 hours following the onset of core damage for the most-likely severe accident sequences. The probabilistic evaluation demonstrates that the reliability of containment isolation in response to severe accident meets the safety goal, as confirmed by the composite CCFP.

19.2.5 Accident Management

Accident management refers to the actions taken during the course of a beyond design basis accident by the plant operating and technical staff to:

- prevent core damage
- terminate the progress of core damage if it begins and retain the core within the RPV
- maintain containment integrity as long as possible
- minimize offsite releases

The inherent design characteristics (e.g., fail-safe equipment position and design simplicity) and thermal-hydraulic characteristics (e.g., passive cooling) of the NuScale design are such that there are no operator actions required to place an NPM in a safe configuration for postulated design basis accidents. That is, operator actions during postulated accidents are associated with monitoring the module or providing backup in the event of multiple component failures. Section 19.2.5.1 summarizes the capability of the NuScale design with respect to the different stages of a postulated accident. Section 19.2.5.2 summarizes the programmatic structure for accident management.

19.2.5.1 Accident Management Design Capability

The capability to manage the course of a severe accident at each stage is summarized below.

Prevention of Core Damage

The Level 1 PRA discussed in Section 19.1 demonstrates the very low CDF is dominated by beyond design basis accidents involving incomplete actuation of the ECCS. In such sequences, inventory makeup to the RPV is required to prevent core damage. Potential actions to provide the necessary makeup, depending on the particular failures involved in the event, include

- manual action to open ECCS valves to allow ECCS flow between the RPV and the CNV, which allows decay heat removal to the UHS (reactor pool).
- manual initiation of makeup to the RPV through the CVCS injection line using the CVCS makeup pumps.
- manual initiation of makeup to the RPV through the pressurizer spray line using the CVCS makeup pumps.
- manual initiation of the CFDS to add water to the CNV to remove heat from the RPV through passive conduction and convection, preventing RPV over-pressurization, or when the CFDS is credited in conjunction with successful ECCS, the makeup coolant mitigates an unisolated outside-containment LOCA.

Terminate Core Damage Progression and Retain the Core within the RPV

The actions identified for prevention of core damage are also taken to arrest the progression of core damage once begun and retain the core within the RPV.

Maintaining Containment Integrity

The analyses supporting the Level 2 PRA discussed in Section 19.1 demonstrate that challenges to containment are due to failure of containment isolation or containment bypass. Potential actions to maintain containment integrity, depending on the particular failures involved in the event, include

- manual action to restore containment isolation.
- isolation of an SGTF to preserve the reactor coolant pressure boundary.

Minimize Offsite Releases

The small size of an NPM core results in a correspondingly small radionuclide source term. Although not credited in the PRA, potential releases would be further minimized because

- most of the CNV is below water, thus radionuclide release due to CNV failure of the lower head would be minimized due to the scrubbing effect of the reactor pool.
- for severe accidents with CNV bypass or containment isolation failure, there is potential deposition in the bypass piping and the release would potentially be further reduced by the Seismic Category I Reactor Building.

19.2.5.2 Accident Management Programmatic Structure

The programmatic structure of management of severe accidents occurring in an NPM reflects lessons learned from industry experience and recent developments in severe accident response. Programmatic elements of severe accident management are:

- Accident mitigation focuses on the containment of fission products. When an accident can no longer be mitigated by emergency operating procedures (EOPs), activities transition to severe accident management guidelines (SAMGs) or other administrative controls. The EOPs and other operating procedures are addressed in Section 13.5.

- The response to an ATWS defined by 10 CFR 50.62 is addressed in SAMGs or other administrative controls. The module capability to accommodate an ATWS event is summarized in Section 19.2.2.1.
- The response to an SBO defined by 10 CFR 50.63 is addressed in SAMGs or other administrative controls. The module capability to accommodate an SBO and related events is summarized in Section 19.2.2.3.
- The response to a loss of large area defined in 10 CFR 50.54(hh)(2) is addressed in SAMGs or other administrative controls. The module capability to accommodate a loss of large area event is summarized Section 20.2.
- The response to an aircraft impact event defined in 10 CFR 50.150 is explicitly addressed in SAMGs or other administrative controls. The key design features associated with the NuScale design capability to survive an aircraft impact are discussed in Section 19.5.
- Mitigating strategies for beyond design basis external events defined by 10 CFR 50.155 are discussed in Section 20.1.

COL Item 19.2-1: A COL applicant that references the NuScale Power Plant design certification will develop severe accident management guidelines and other administrative controls to define the response to beyond-design-basis events.

19.2.6 Consideration of Potential Design Improvements Under 10 CFR 50.34(f)

As described in prior sections, a design-specific PRA has been performed consistent with the requirement in 10 CFR 50.34(f)(1)(i) to identify improvements in the reliability of core and containment heat removal systems that are significant and practical. The potential improvements that are considered are identified as severe accident management design alternative(s) (SAMDAs). The following sections summarize the method for identifying and evaluating these design alternatives and the conclusions of the SAMDA evaluation. The evaluation is provided in the Environmental Report (Reference 19.2-16).

COL Item 19.2-2: A COL applicant that references the NuScale Power Plant design certification will use the site-specific probabilistic risk assessment to evaluate and identify improvements in the reliability of core and containment heat removal systems as specified by 10 CFR 50.34(f)(1)(i).

19.2.6.1 Introduction

The SAMDA analysis is a cost-benefit analysis wherein the cost of modifying the nuclear power plant design is weighed against the monetized estimation of risk associated with the consequences stemming from a possible severe accident. The Environmental Report documents the SAMDA analysis as the basis for supporting the Nuclear Regulatory Commission environmental assessment of the NuScale design per 10 CFR 51.30(d) to ensure compliance with Section 102(2)(c) of the National Environmental Policy Act of 1969.

19.2.6.2 Estimate of Risk for Design

The estimate of the risk that provides the basis for the SAMDA evaluation is developed from the PRA performed for the design certification and an estimate of the characteristics of a potential site. Key points of the evaluation are

- the PRA for the design certification provided Level 1 and Level 2 information for all modes of operation. In addition to full power, low power, and shutdown internal events, the design certification PRA addressed internal flood, internal fire, high winds, external flooding, and seismic hazard.
- site characteristics are based on the Surry Nuclear Power Station with 2017 economic information and 2060 population estimates, which are considered representative for the purposes of the SAMDA evaluation for standard design.
- to determine the off-site dose and economic consequences required for the calculation of the cost of maximum benefit, the two release categories identified in the Level 2 PRA are redefined into eight release categories to more realistically estimate the off-site consequences of severe accidents. Radionuclide source terms corresponding to each release category are determined with MELCOR severe accident simulations.
- the MACCS code (Reference 19.2-20) is used to evaluate the population dose and off-site economic consequences.
- on-site operational dose estimates and cleanup and decontamination cost estimates are used from NUREG/BR-0184 (Reference 19.2-18).
- multiple-module events are addressed by applying multipliers (corresponding to the maximum number of modules that could be involved in an accident corresponding to each release category) to the severe accident effects when evaluating the maximum benefit of a design alternative.

The maximum benefit associated with eliminating all risk in the NuScale design (which can be viewed as an estimate of the severe accident risk for the NuScale design) is conservatively calculated to be $136,000 for a 12-NPM NuScale Power Plant. This maximum benefit is bounding for a NuScale plant with a smaller number of NPMs.

19.2.6.3 Identification of Potential Design Improvements

The SAMDA evaluation is performed using the guidance provided in NEI 05-01 (Reference 19.2-17) and NUREG/BR-0184. Design alternatives that are considered included those typically considered for currently operating plants and those that may be beneficial to the unique NuScale design. Design alternatives specific to the NuScale design are identified to improve the reliability of the structures, systems and components (SSC) that are determined to be risk significant; in some cases a generic SAMDA is applicable to the risk significant component, but in most cases, a design-specific SAMDA is identified and evaluated. A total of 199 SAMDA candidates are developed and evaluated, and 46 of those SAMDAs are specific to the NuScale design.

NuScale design-specific SAMDA candidates for plants with 1 to 12 NPMs are postulated for a variety of plant systems. SAMDAs are postulated to reduce the impacts of severe accident risk for the following systems:

- chemical and volume control system
- containment flooding and drain system
- containment system
- control rod drive system
- decay heat removal system
- emergency core cooling system
- highly reliable DC power system
- module protection system
- Reactor Building crane system
- reactor coolant system
- reactor trip system

19.2.6.4 Risk-Reduction Potential of Design Improvements

The candidate SAMDAs identified are qualitatively screened into one of seven initial screening categories. The intent of the screening is to identify the candidates with the potential for risk reduction in the NuScale design that warrant a detailed cost-benefit evaluation. These categories and the screening process itself are based on the "Phase I" analysis screening criteria described in NEI 05-01. These seven categories include "not applicable," "already implemented," "combined," "excessive implementation cost," "very low benefit," "not required for design certification," and "considered for further evaluation." These categories are described in greater detail below.

- Not applicable: SAMDA candidates that are not considered applicable to the NuScale design are those with specific pressurized water reactor equipment that is not in the NuScale design.
- Already implemented: Candidate SAMDAs that are already included in the NuScale design or whose intent is already fulfilled by a different NuScale design feature are considered "already implemented" in the NuScale design. If a particular SAMDA has already been implemented in the NuScale design, it is not retained for further analysis.
- Combined: The SAMDA candidates that are similar to one another are combined and evaluated in conjunction with each other. This combination of SAMDA candidates leads to a more comprehensive or plant-specific SAMDA candidate set. The combined SAMDA would then be assessed against the remaining six screening categories.
- Excessive implementation cost: If a SAMDA requires extensive changes that exceed the maximum benefit of $136,000 even without an implementation cost estimate, it is not retained for further analysis.

- Very low benefit: If a proposed SAMDA is related to a system for which improved reliability would have a negligible impact on overall plant risk, it is considered to have a very low benefit for implementation and is not retained for further analysis. The Level 1 and Level 2 PRA importance lists from all NuScale PRAs are used to determine the risk-significance of systems and components in the NuScale design for the SAMDA screening process. If a component is not considered risk-significant to the NuScale design, then implementing a SAMDA related to that component is very low benefit.
- Not required for design certification: SAMDA candidates related to potential procedural enhancements, surveillance action enhancements, multiple plant sites, or design elements that are to be finalized in a later stage of the design process are outside of the scope of this report and are categorized as "not required for design certification."

COL Item 19.2-3: A COL applicant that references the NuScale Power Plant design certification will evaluate severe accident mitigation design alternatives screened as “not required for design certification application.”

- Considered for further evaluation: Any SAMDA candidate that did not screen into any of the previous six screening categories is subject to a more in-depth cost-benefit analysis.

<u>Result of Phase I Screening</u>

A total of 199 SAMDA candidates developed from industry and NuScale documents were evaluated in this phase of the analysis. The screening of each SAMDA and the basis for the screening is shown in the Environmental Report.

- 45 SAMDA candidates are not applicable to the NuScale design.
- 18 SAMDA candidates are already implemented into the NuScale design either as suggested in the SAMDA or as an equivalent replacement that fulfilled the intent of the SAMDA.
- 13 SAMDA candidates are combined with another SAMDA because they have the same intent.
- 37 SAMDA candidates are not required for design certification because the candidates are related to a procedural or surveillance action, are related to a multiple plant site, or are related to design elements to be finalized at a later stage in the design process that is outside the scope of the design certification.
- 34 SAMDA candidates are of very low benefit to reducing risk in the NuScale design.
- 1 SAMDA candidate is categorized as having an excessive implementation cost.
- 51 SAMDA candidates are considered for further evaluation.

19.2.6.5 Cost Impacts of Candidate Design Improvements

A total of 52 SAMDAs are screened into the "excessive implementation cost" or "considered for further evaluation" categories. Of the 52 SAMDAs, one is screened in

Phase I as exceeding the maximum benefit of $136,000 for the NuScale design. The remaining 51 are considered to be potentially cost beneficial in Phase I screening, and are considered for further evaluation in the Phase II cost-benefit comparison.

19.2.6.6 Cost-Benefit Comparison

Any SAMDA screened into the "considered for further evaluation" category undergoes a more rigorous cost-benefit analysis. All 51 SAMDA candidates that are not screened in Phase I are estimated to have a bounding benefit of $1,160, much less than the estimated cost of implementation of greater than $100,000 for each SAMDA candidate. Therefore, none of the candidates are considered to be potentially cost beneficial in the Phase II screening.

Sensitivity analyses are performed with more conservative estimates for the maximum benefit. For example, a different site is analyzed or different off-site consequence modeling assumptions are considered. The Environmental Report provides more information on sensitivity analyses.

19.2.6.7 Conclusions of SAMDA Evaluation

Design alternatives that are considered in the SAMDA evaluation include those typically considered for currently operating plants and those that may be beneficial to the unique NuScale design. There are no design alternatives determined to be cost-beneficial for severe accident mitigation.

19.2.7 References

19.2-1 American Society of Mechanical Engineers/American Nuclear Society, "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), New York, NY.

19.2-2 U.S. Nuclear Regulatory Commission, "PRA Procedures Guide," NUREG/CR-2300, Volume 1, Chapter 7, January 1983.

19.2-3 U.S. Nuclear Regulatory Commission, "An Approach for Estimating the Frequencies of Various Containment Failure Modes and Bypass Events," NUREG/CR-6595 Rev. 1, October 2004.

19.2-4 U.S. Nuclear Regulatory Commission, "Evolutionary Light-Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements," Commission Paper SECY-90-016, January 12, 1990.

19.2-5 U.S. Nuclear Regulatory Commission, "Evolutionary Light Water Reactor (LWR) Certification Issues and their Relationships to Current Regulatory Requirements," Staff Requirements Memorandum for Commission Paper SECY-90-16, June 26, 1990.

19.2-6 ANSYS (Release 16.0) [Computer Program]. (2015). Canonsburg, PA: ANSYS Incorporated.

19.2-7 Theofanous, T.G., et al., "In-vessel Coolability and Retention of a Core Melt," DOE/ID-10460, Vols. I and II, October 1996.

19.2-8 Rempe, J.L., "Potential for AP600 In-Vessel Retention through Ex-Vessel Flooding," INEEL/EXT-97-00779, December 1997.

19.2-9 U.S. Nuclear Regulatory Commission, "Critical heat flux (CHF) Phenomenon on a Downward Facing Curved Surface," NUREG/CR-6507, June 1997.

19.2-10 Z. Guo and M.S. El-Genk, "An experimental study of saturated pool boiling from downward facing and inclined surfaces," *International Journal of Heat Mass Transfer*, (1992): 35: 9, 1992.

19.2-11 Theofanous, T.G. and S. Syri, "The coolability limit of a reactor pressure vessel lower head," *Nuclear Engineering and Design*, (1997): 169: 1-3:59-76.

19.2-12 Theofanous, T.G., et al., "Critical heat flux through curved, downward facing, thick walls," *Nuclear Engineering and Design*, (1994): 151: 1:247-258.

19.2-13 U.S. Nuclear Regulatory Commission, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," Commission Paper SECY-93-087, April 2, 1993.

19.2-14 U.S. Nuclear Regulatory Commission, "Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," Staff Requirements Memorandum for Commission Paper SECY-93-087, July 21, 1993.

19.2-15 U.S. Nuclear Regulatory Commission, "Source Term-Related Technical and Licensing Issues Pertaining To Evolutionary And Passive Light-Water-Reactor Designs," Commission Paper SECY-94-302, December 19, 1994.

19.2-16 NuScale Power, LLC, Design Certification Application, Part 3, “Applicant's Environmental Report - Standard Design Certification,” Portland, OR, December 2016.

19.2-17 Nuclear Energy Institute, "Severe Accident Mitigation Alternatives (SAMA) Analysis Guidance Document," NEI 05-01, Rev. A, Washington, DC, November 2005.

19.2-18 U.S. Nuclear Regulatory Commission, "Regulatory Analysis Technical Evaluation Handbook," NUREG/BR-0184, January 1997.

19.2-19 U.S. Nuclear Regulatory Commission, "A Reassessment of the Potential for an Alpha-Mode Containment Failure and a Review of the Current Understanding of Broader Fuel-Coolant Interaction Issues," NUREG-1524, July 1996.

19.2-20 U.S. Nuclear Regulatory Commission "Code Manual for MACCS2: Volume 1, User's Guide," NUREG/CR-6613 (SAND97-0594), May 1998.

19.2-21 U.S. Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, December 1990.

19.2-22 Fauske & Associates, Inc., and Sandia National Laboratories, "High Pressure Melt Ejection (HPME) and Direct Containment Heating (DCH), State-of-the-Art Report," NEA/CSNI/R(96)25, Paris, France, December 1996.

19.2-23 Meyer, L., et al.,"Direct containment heating integral effects tests in geometries of European nuclear power plants," *Nuclear Engineering and Design*, (2009): 239: 2070-2084.

19.2-24 Los Alamos National Laboratory, "Engineering Standards Manual ISD 341-2," Rev. 1, October 2006.

19.2-25 U.S. Department of the Interior, Limits of Flammability of Gases and Vapors, Bulletin 503, Bureau of Mines, 1952.

19.2-26 U.S. Department of the Interior, Investigation of Fire and Explosion Accidents in the Chemical, Mining, and Fuel-Related Industries - A Manual, Bulletin 680, Bureau of Mines, 1985.

19.2-27 U.S. Department of the Interior, Flammability characteristics of combustible gases and vapors, Bulletin No. 627, Bureau of Mines, 1965.

19.2-28 Shapiro, Z.M. and T.R. Moffette, "Hydrogen Flammability Data and Application to PWR Loss-of-Coolant Accident," Report WAPD-SC-545, 13th edition, Bettis Plant, 1957.

19.2-29 U.S. Nuclear Regulatory Commission, "Hydrogen: Air: Steam Flammability Limits and Combustion Characteristics in the FITS Vessel," NUREG/CR-3468, Rev. 3, December 1986.

19.2-30 Not Used.

19.2-31 U.S. Nuclear Regulatory Commission, "An Assessment of Steam-Explosion-Induced Containment Failure," NUREG/CR-5030, February 1989.

19.2-32 Corradini, et al., "Evaluation of Dynamic Pressures from Steam Explosions Applied to Advanced Light Water Reactors," Nuclear Science and Engineering, (2011): 168, 185-196.

19.2-33 NUREG-1570, "Risk Assessment of Severe Accident-Induced Steam Generator Tube Rupture," March 1998.

Table 19.2-1: Key Parameters for ANSYS Simulation of Retention of Core Debris in the Reactor Pressure Vessel

Parameter	Value
Mass of UO_2 in the oxidic debris	10,730 kg
Mass of ZrO_2 in the oxidic debris	0
Temperature of water in the containment	380 °F
Temperature of water in the reactor pool	100 °F
Total decay power in the UO_2	1 MW
Heat loss from the top of oxidic debris by radiation	0

Table 19.2-2: Core Damage Simulations for Severe Accident Evaluation

Simulation ID	Initiating Event	DHRS	RSV	PCS	ECCS	CVCS	CFDS	Comment
LCC-05T-01	CVCS LOCA Inside CNV	NA	ND	NA	PA	NA	NA	RPV IVR, H2, HPME, FCI, ES
LCC-05T-02	CVCS LOCA Inside CNV	NA	ND	NA	NA	NA	NA	RPV IVR, H2, HPME, FCI, ES
LCC-05T-03	CVCS LOCA Inside CNV	NA	ND	NA	NA	NA	NA	RPV IVR, H2, HPME, FCI, ES
LEC-06T-00	RVV LOCA	NA	ND	NA	PA	NA	NA	RPV IVR, H2, HPME, FCI, ES
TRN-07T-01	General Transient	NA	SO	NA	NA	NA	NA	RPV IVR, H2, HPME, FCI, ES
LCU-03T-01	CVCS LOCA Outside CNV	NA	ND	NA	NA	NA	NA	CNV IVR, HPME, ES
LCU-01T-01	CVCS LOCA Outside CNV	NA	ND	NA	NA	NA	Available	RPV IVR, HPME, ES

Notes:

The simulations that are used to support the evaluation of severe accident phenomena are summarized in this table. The Comments column identifies the phenomena that are of interest; the Comments column does not indicate that the phenomenon is predicted by the simulation.

Abbreviations:

NA: Not applicable (system not credited)

ND: Not demanded (system not demanded)

PA: Partial actuation (RVVs open, RRVs fail closed)

SO: Stuck open

IVR: In-vessel (RPV, CNV) retention

H2: Hydrogen combustion

HPME: High pressure melt ejection

FCI: Fuel-coolant interaction

ES: Equipment survivability

Table 19.2-3: Sequence LCC-05T-01 Key Events

Time (seconds)	Event
0	CVCS injection line LOCA inside CNV
3	High CNV pressure - signal for CNV isolation (successful), SCRAM (successful)
40	Pressurizer heater isolation
90	Low low pressurizer level
681	ECCS actuation signal on high containment level - partial actuation
700	Maximum CNV pressure (747 psia) measured at the top of the CNV
7860 (2.2 hr)	RPV collapsed level below top of active fuel (TAF)
14625 (4.1 hr)	High core outlet temperature
16440 (4.6 hr)	Onset of cladding oxidation
16593 (4.6 hr)	First gap release (group 1)
17190 (4.8 hr)	Core damage (> 2200 °F)
21120 (5.9 hr)	Maximum cladding temperature (3829 °F)
33963 (9.4 hr)	Failure of core support plates in rings 1 & 2 - begins debris relocation to RPV lower plenum
150000 (41.7 hr)	End of cladding oxidation (timing approximate)
259200 (72 hr)	Simulation terminates

Table 19.2-4: Sequence LCC-05T-02 Key Events

Time (seconds)	Event
0	CVCS injection line LOCA inside CNV
3	High CNV pressure - signal for CNV isolation (successful), SCRAM (successful)
40	Low pressurizer level - signal for pressurizer heater isolation
90	Low low pressurizer level
681	ECCS actuation signal on high containment level - fails completely (i.e., all five valves fail to open)
1500	Maximum CNV pressure (305.5 psia) measured at the top of the CNV
3661 (1.0 hr)	RPV collapsed level below TAF
5650 (1.6 hr)	High core outlet temperature
8340 (2.3 hr)	Onset of cladding oxidation
8522 (2.4 hr)	First gap release (group 2)
9212 (2.6 hr)	Core damage (> 2200 °F)
11160 (3.1 hr)	Maximum cladding temperature (3838 °F)
24390 (6.8 hr)	Failure of core support plates in rings 1 & 2 - begins debris relocation to RPV lower plenum
131400 (36.5 hr)	End of cladding oxidation
259200 (72 hr)	Simulation terminates

Table 19.2-5: Sequence LCC-05T-03 Key Events

Time (seconds)	Event
0	CVCS injection line LOCA inside CNV
16	High CNV pressure - signal for CNV isolation (successful), SCRAM (successful)
166	Low pressurizer level
379	Low low pressurizer level
3453	ECCS actuation signal on high containment level - fails completely (i.e., all five valves fail to open)
26039 (7.2 hr)	RPV collapsed level below TAF
50154 (13.9 hr)	High core outlet temperature
89700 (24.9 hr)	Onset of cladding oxidation
90284 (25.1 hr)	First gap release (group 2)
91633 (25.4 hr)	Core damage (> 2200 °F)
94200 (26.2 hr)	Maximum cladding temperature (3757 °F)
128066 (35.6 hr)	Failure of core support plates in rings 1 & 2 - begins debris relocation to RPV lower plenum
138300 (38.3 hr)	Maximum CNV pressure (179 psia) measured at the top of the CNV
152700 (42.4 hr)	End of cladding oxidation
259200 (72 hr)	Simulation terminates

Table 19.2-6: Sequence LEC-06T-00 Key Events

Time (seconds)	Event
0	RVV #1 LOCA
0	High CNV pressure - CNV isolation signal
2	Signal for SCRAM (successful)
40	Maximum CNV pressure (630.9 psia) measured at the top of the CNV
1010	ECCS actuation signal on high containment level - partial actuation
1432	Pressurizer heater isolation
2319	Low low pressurizer level
16200 (4.5 hr)	RPV collapsed level below TAF (timing approximate)
21973 (6.1 hr)	High core outlet temperature
24360 (6.8 hr)	Onset of cladding oxidation
24539 (6.8 hr)	First gap release (group 1)
25223 (7.0 hr)	Core damage (> 2200 °F)
29640 (8.2 hr)	Maximum cladding temperature (3838 °F)
41785 (11.6 hr)	Failure of core support plates in rings 1 & 2 - begins debris relocation to RPV lower plenum
95400 (26.5 hr)	End of cladding oxidation (timing approximate)
259200 (72 hr)	Simulation terminates

Table 19.2-7: Sequence TRN-07T-01 Key Events

Time (seconds)	Event
0	General transient: SCRAM and containment isolation
571	High pressurizer pressure
953	RSV #1 first demand (sticks open)
958	High CNV pressure
2200	Pressurizer heater isolation
2542	Low low pressurizer level
6801	ECCS actuation signal on high containment level - ECCS failed
50400 (14 hr)	RPV collapsed level below TAF (timing approximate)
63435 (17.6 hr)	High core outlet temperature
72720 (20.2 hr)	Onset of cladding oxidation (timing approximate)
73069 (20.3 hr)	First gap release (group 2)
74183 (20.6 hr)	Core damage (> 2200 °F)
79200 (22.0 hr)	Maximum cladding temperature (3800 °F)
112987 (31.4 hr)	Failure of core support plates in rings 1, 2, & 3 - begins debris relocation to RPV lower plenum
127440 (35.4 hr)	End of cladding oxidation (timing approximate)
131700 (36.6 hr)	Maximum CNV pressure (198.3 psia) measured at the top of the CNV
259200 (72 hr)	Simulation terminates

Table 19.2-8: Sequence LCU-03T-01 Key Events

Time (seconds)	Event
0	CVCS injection line pipe break outside CNV
69	Low pressurizer level - signal for SCRAM (successful) and pressurizer heater isolation (successful)
87	Low pressurizer pressure - signal for CNV isolation (main steam and feed isolated, CVCS not isolated)
92	Low low pressurizer level
4572 (1.3 hr)	RPV collapsed level below TAF
6121 (1.7 hr)	High core outlet temperature
8760 (2.4 hr)	Onset of cladding oxidation
8942 (2.5 hr)	First gap release (group 1)
9493 (2.6 hr)	Core damage (> 2200 °F)
11640 (3.2 hr)	Maximum cladding temperature (3928 °F)
18110 (5.0 hr)	Failure of core support plates in rings 1 & 2 by yielding - begins debris relocation to RPV lower plenum
19800 (5.5 hr)	High secondary pressure lifts relief valve and introduces coolant into the CNV (timing approximate)
21715 (6.0 hr)	High containment pressure signal
29961 (8.3 hr)	Failure of core support plate in ring 3 by creep rupture
34991 (9.7 hr)	Failure of core support plate in ring 4 by creep rupture
42220 (11.7 hr)	Failure of the RPV lower head by thru-wall yielding
51240 (14.2 hr)	Maximum CNV pressure (19.4 psia) measured at the top of the CNV
63480 (17.6 hr)	End of cladding oxidation (timing approximate)
259200 (72 hr)	Simulation terminates

Table 19.2-9: Sequence LCU-01T-01 Key Events

Time (seconds)	Event
0	CVCS injection line pipe break outside CNV
69	Low pressurizer level - signal for SCRAM (successful) and pressurizer heater isolation (successful)
87	Low pressurizer pressure - signal for CNV isolation (main steam and feed isolated, CVCS not isolated)
92	Low low pressurizer level
2000	Start of containment flooding
4831 (1.3 hr)	RPV collapsed level below TAF
5128 (1.4 hr)	ECCS actuation signal on high containment level -- actuation failed, no valves open
7447 (2.1 hr)	High core outlet temperature
8220 (2.3 hr)	Maximum CNV pressure (6.6 psia) measured at the top of the CNV
11160 (3.1 hr)	Onset of cladding oxidation
14333 (4.0 hr)	First gap release (group 1)
15447 (4.3 hr)	Core damage (> 2200 °F)
16800 (4.7 hr)	Maximum cladding temperature (3800 °F)
36430 (10.1 hr)	Failure of core support plates in rings 1 & 2 by yielding - begins debris relocation to RPV lower plenum
53760 (14.9 hr)	End of cladding oxidation (taken as within 0.1% of the 72 hour value)
54621 (15.2 hr)	Failure of core support plate in ring 3 by creep rupture
60734 (16.9 hr)	Failure of core support plate in ring 4 by creep rupture
259200 (72 hr)	Simulation terminates

Table 19.2-10: MELCOR Cases for Fuel-Coolant Interaction (Steam Explosion)

MELCOR Case ID	Initiating Event	Corium Mass (lbm)	Corium Temperature (F)	RPV Pressure (psia)	Coolant Liquid Volume (ft^3)
TRN-07T	General reactor trip	12,300	2318	232.8	49.3
LEC-06T	Spurious opening of a single RVV	9,620	2822	136.9	50.9
LCC-05T-01	CVCS injection line LOCA inside containment	9,078	2782	143.5	52.8
LCC-05T-02	CVCS injection line LOCA inside containment	9,063	3133	187.8	48.5
LCC-05T-03	CVCS injection line LOCA inside containment	9,456	2770	205.6	51.1

Notes:

1. Three sensitivities involving the LCC-05T MELCOR case were used to define bounding input parameters for FCI analysis.
2. Parameters were taken at a time equal to or after core relocation for each MELCOR case to produce a bounding result.

Figure 19.2-1: Illustration of Reactor Pressure Vessel In-Vessel Retention

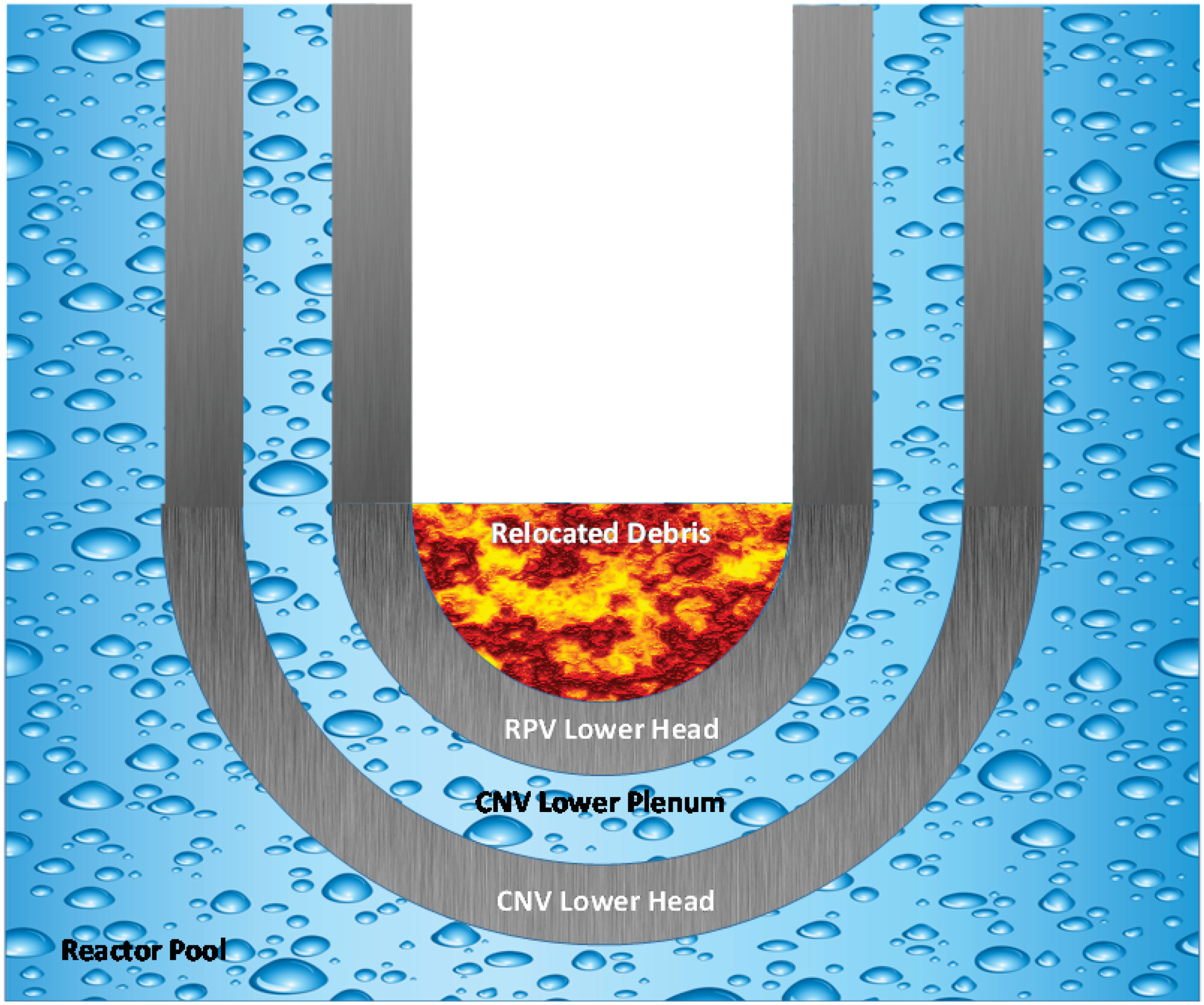


Figure 19.2-2: Heat Transfer Model for Retention of Core Debris in the Reactor Pressure Vessel

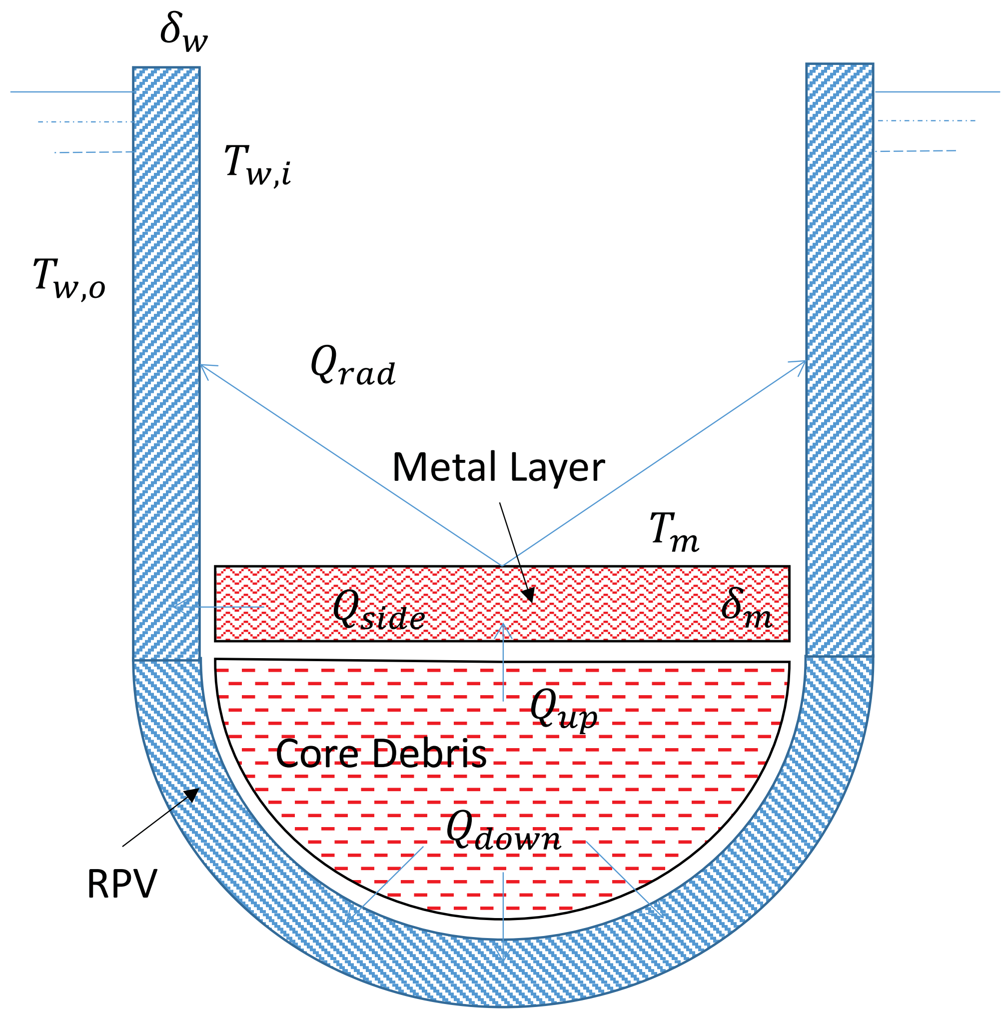


Figure 19.2-3: Expanded Temperature Profile of Reactor Pressure Vessel Lower Head Shell

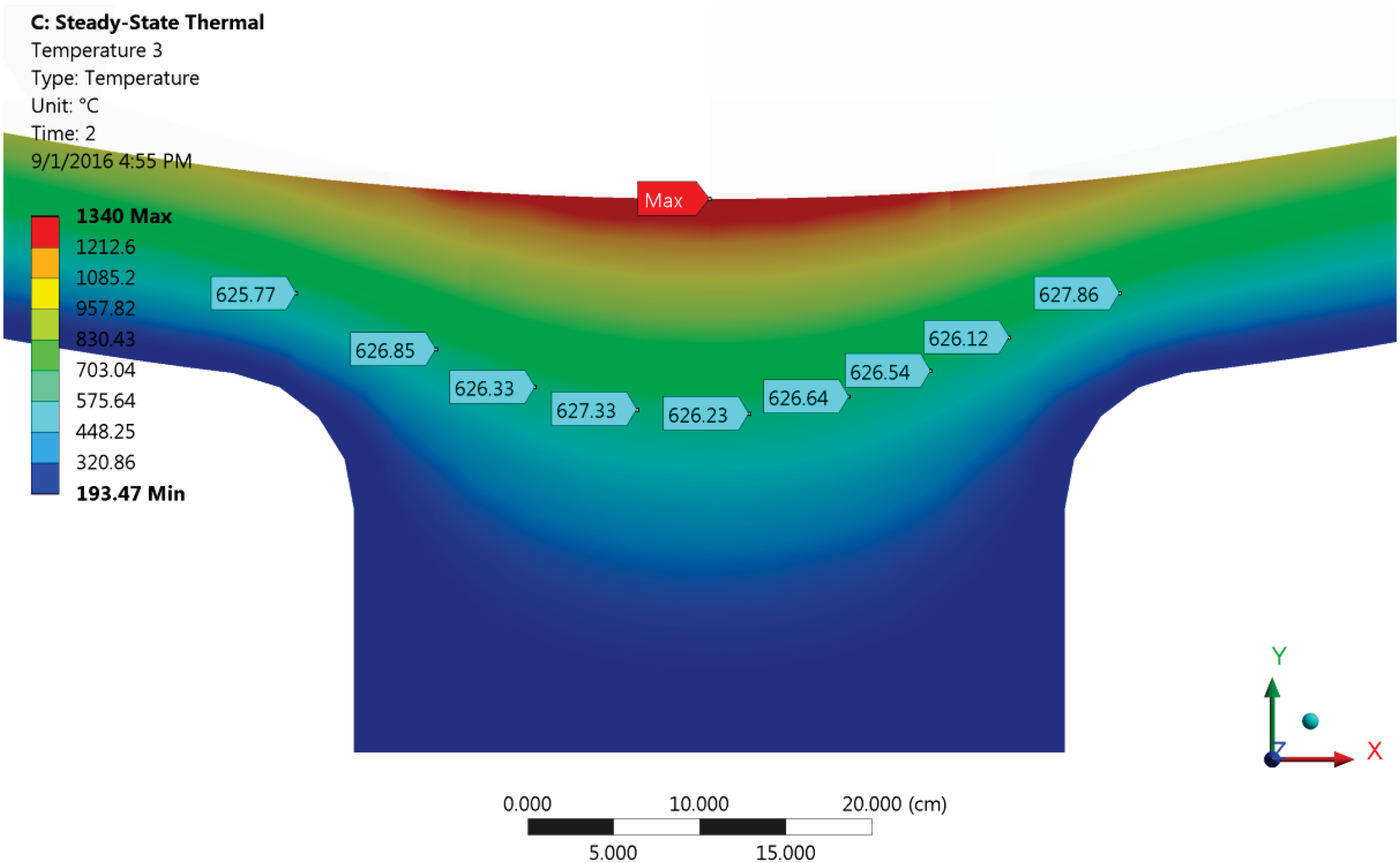


Figure 19.2-4: Heat Flux on Outer Surface of the Reactor Pressure Vessel Lower Head (Bottom-Up View)

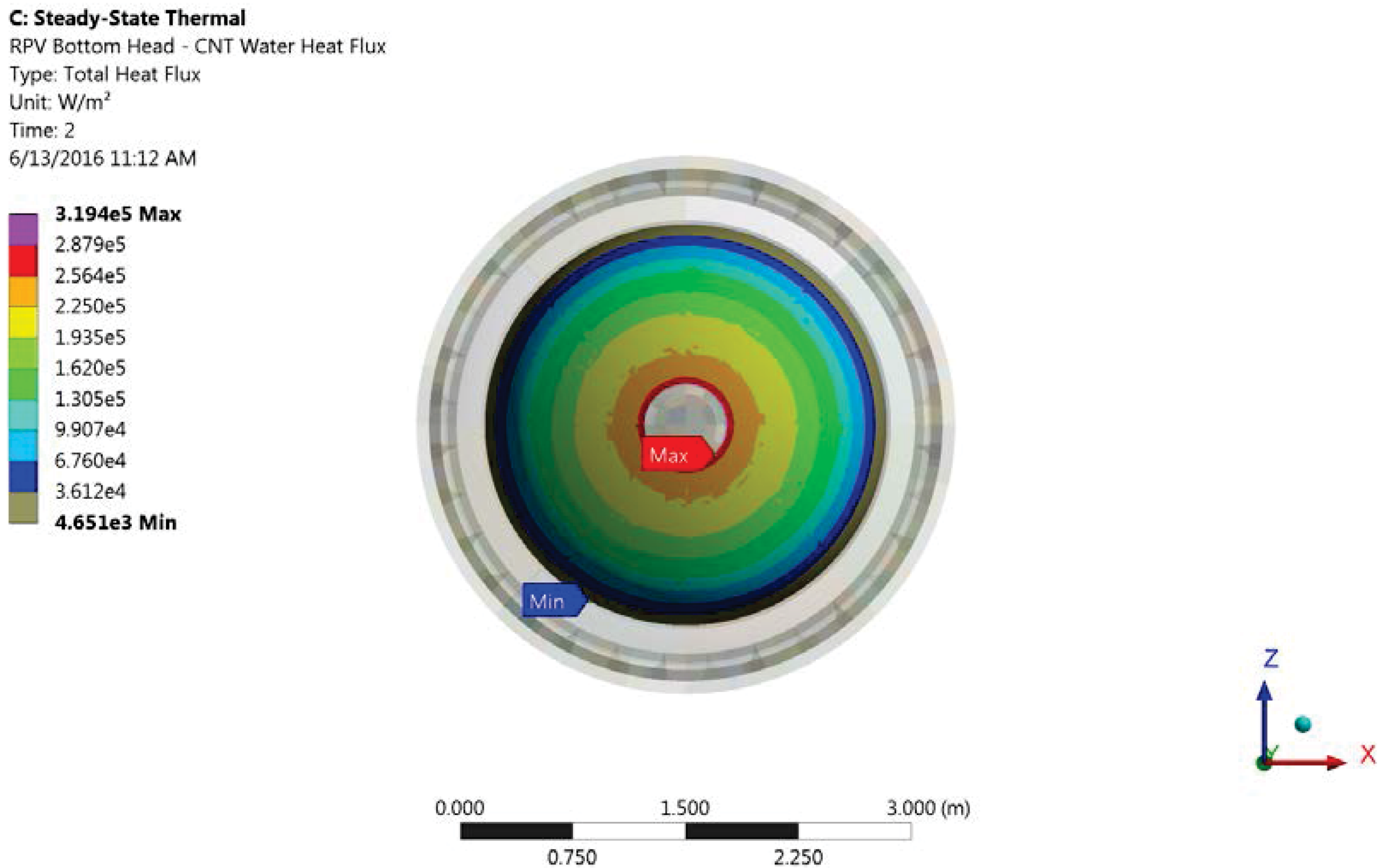


Figure 19.2-5: Heat Flux on the Vertical Surface of the Alignment Pin

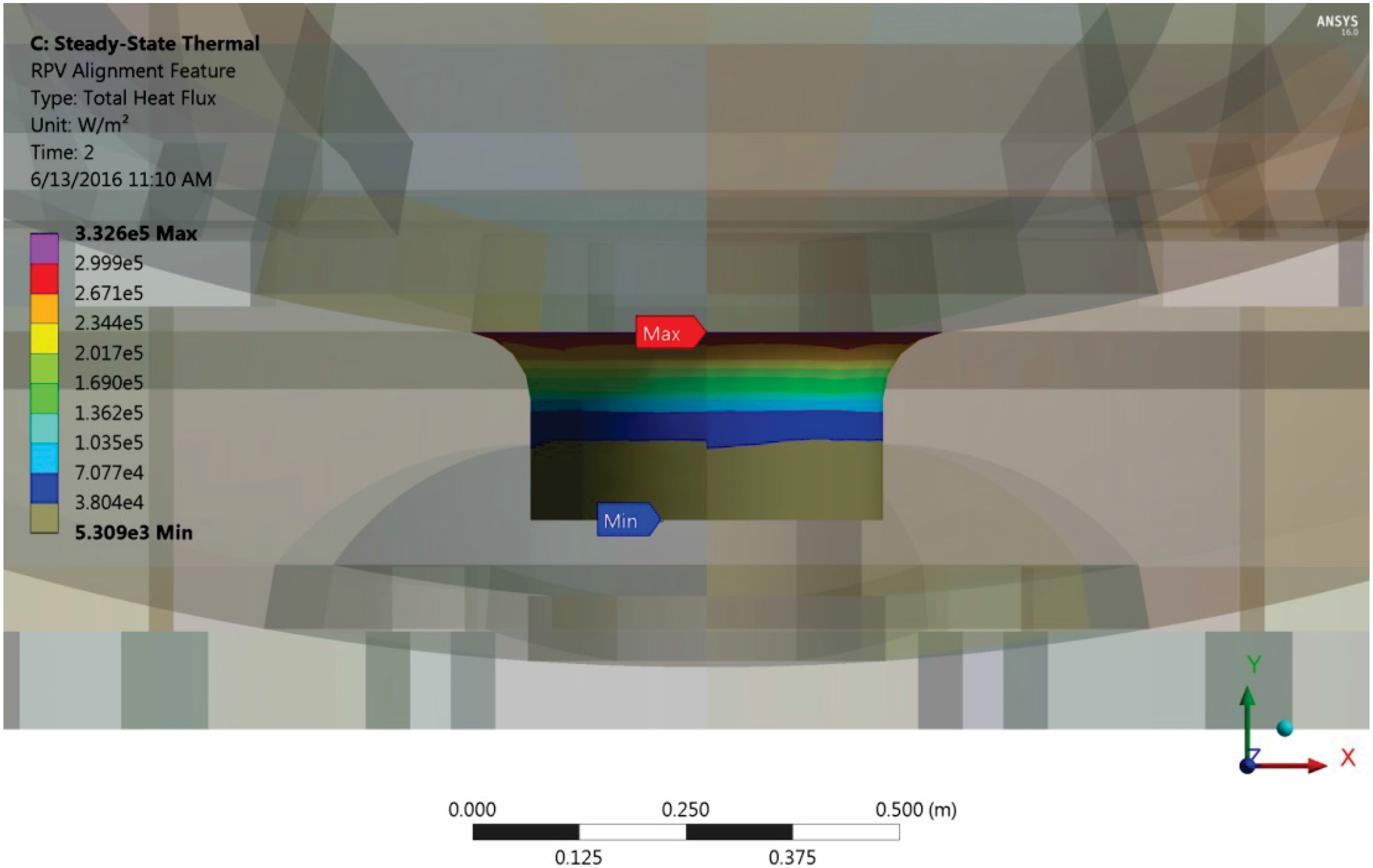


Figure 19.2-6: Heat Flux on the Retention Pin Bottom Surface (Bottom-Up View)

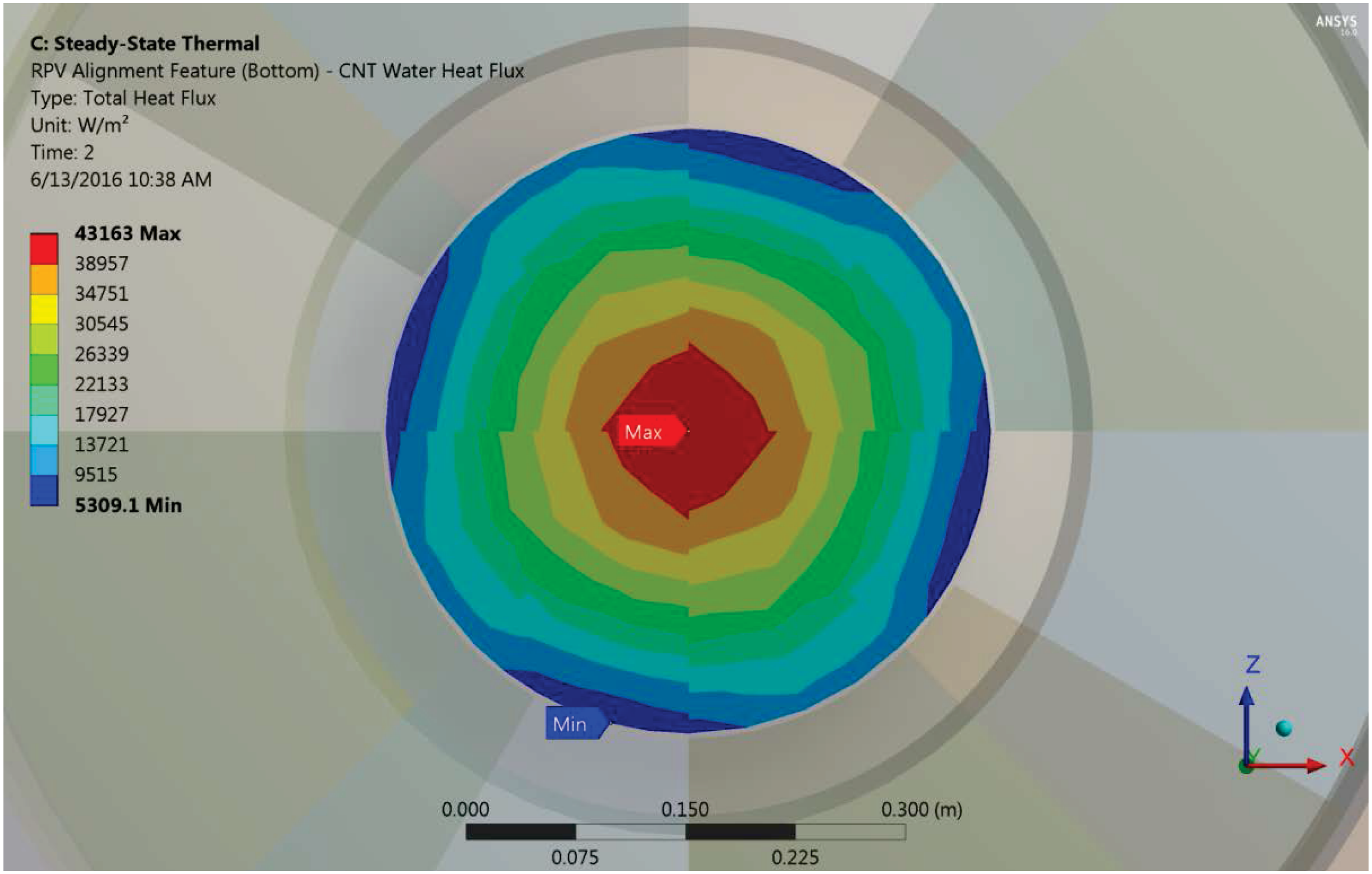


Figure 19.2-7: Illustration of Retention in Reactor Pressure Vessel versus Containment Vessel

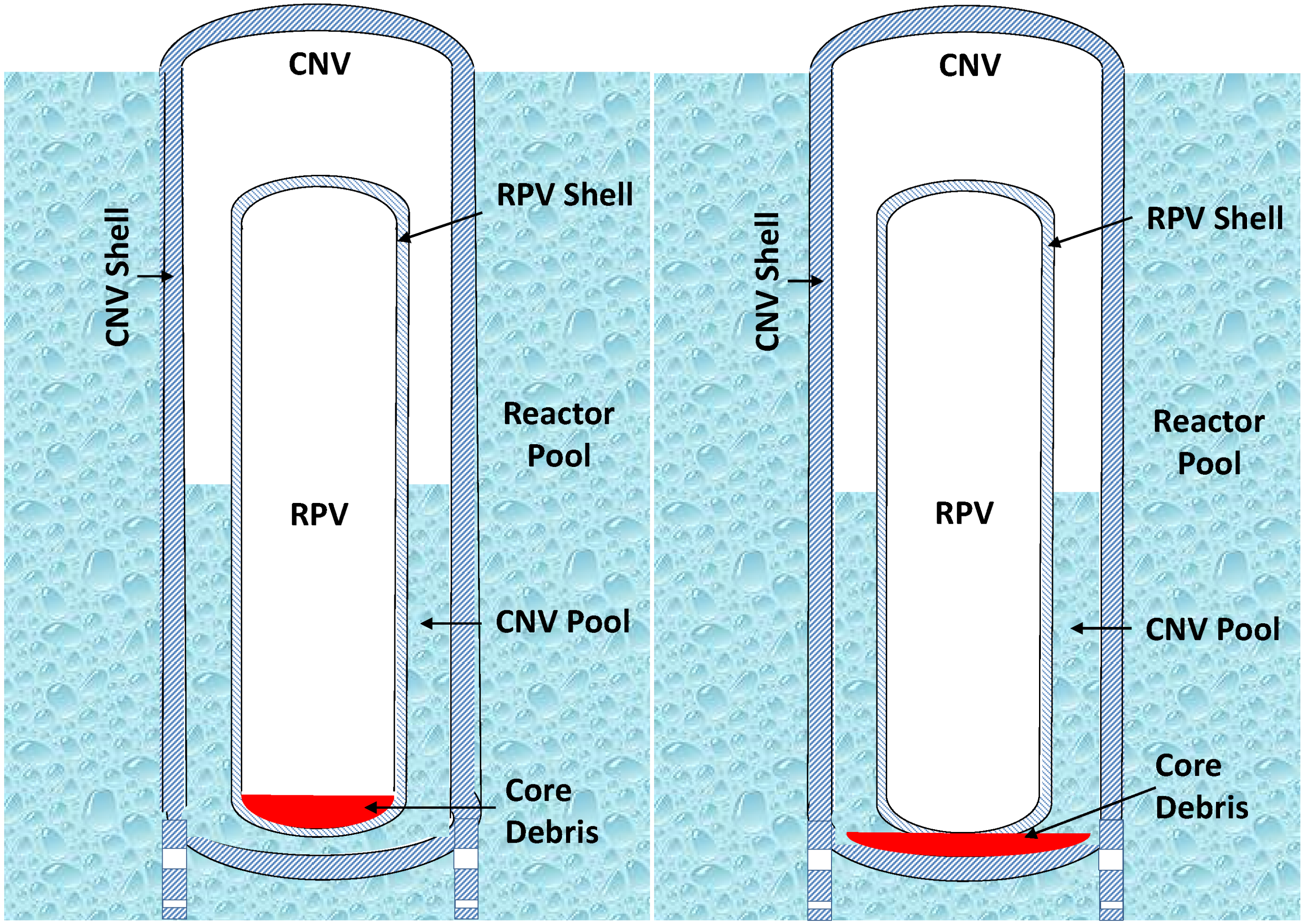


Figure 19.2-8: Front View of the Containment Vessel Support Skirt (Top) and Lower Head Cross-Section (Bottom)

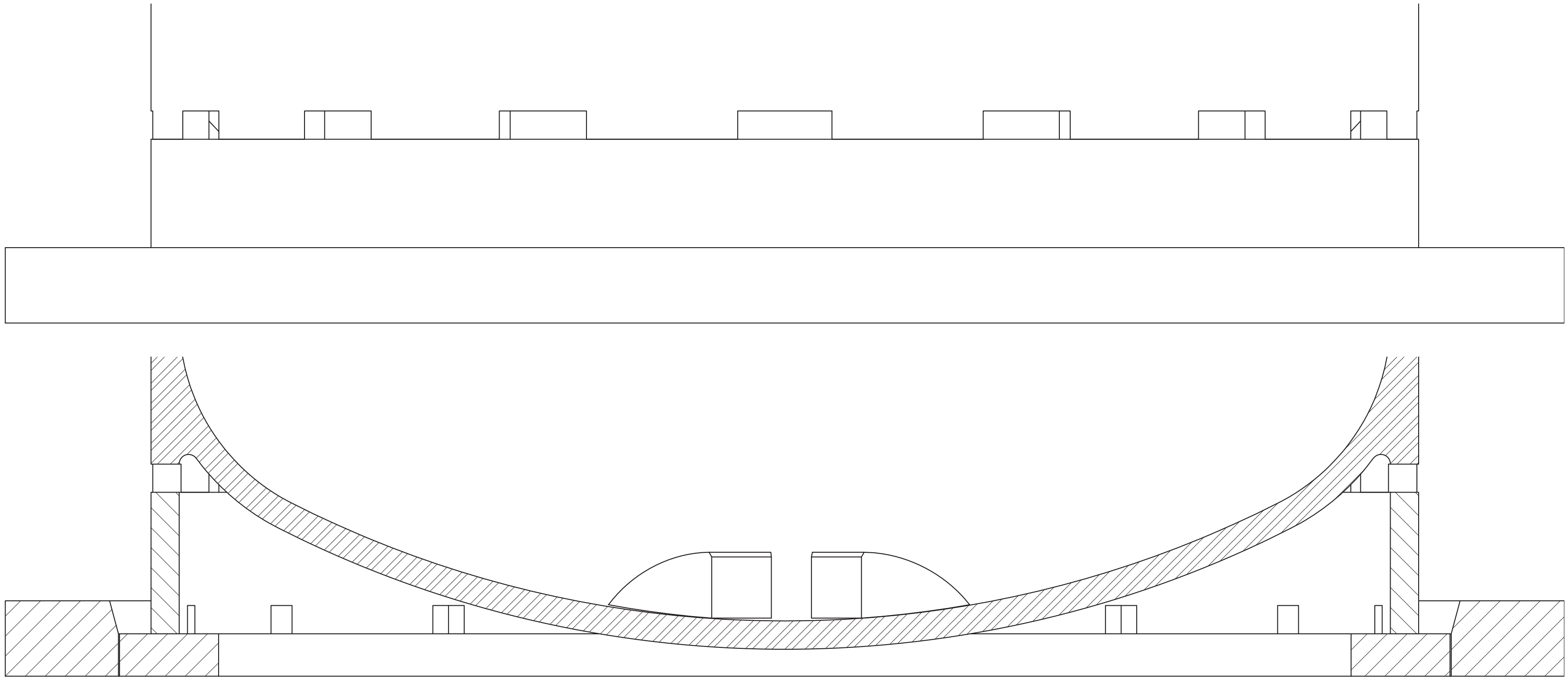


Figure 19.2-9: Hydrogen Generation versus Time

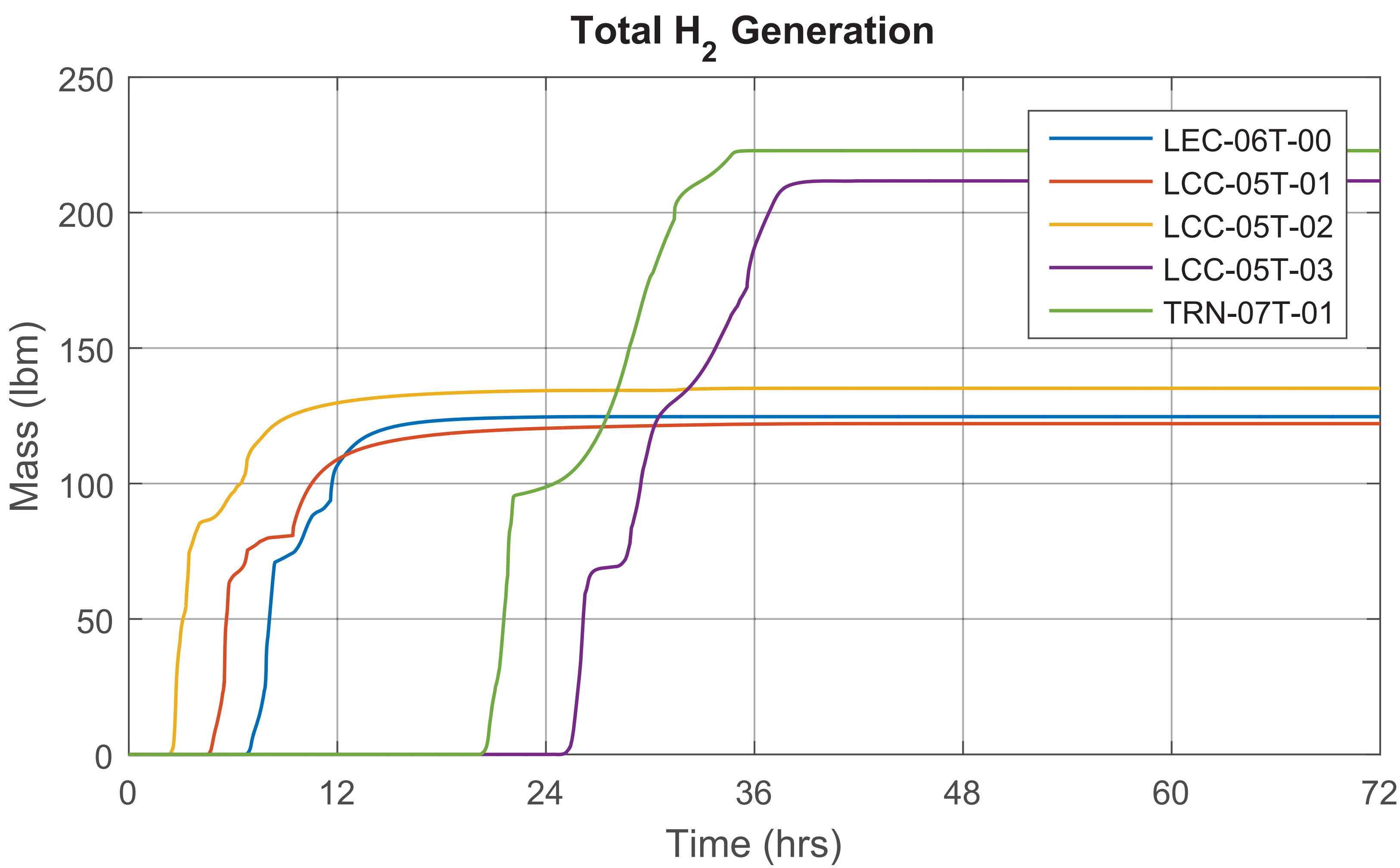


Figure 19.2-10: Oxygen Concentration versus Time

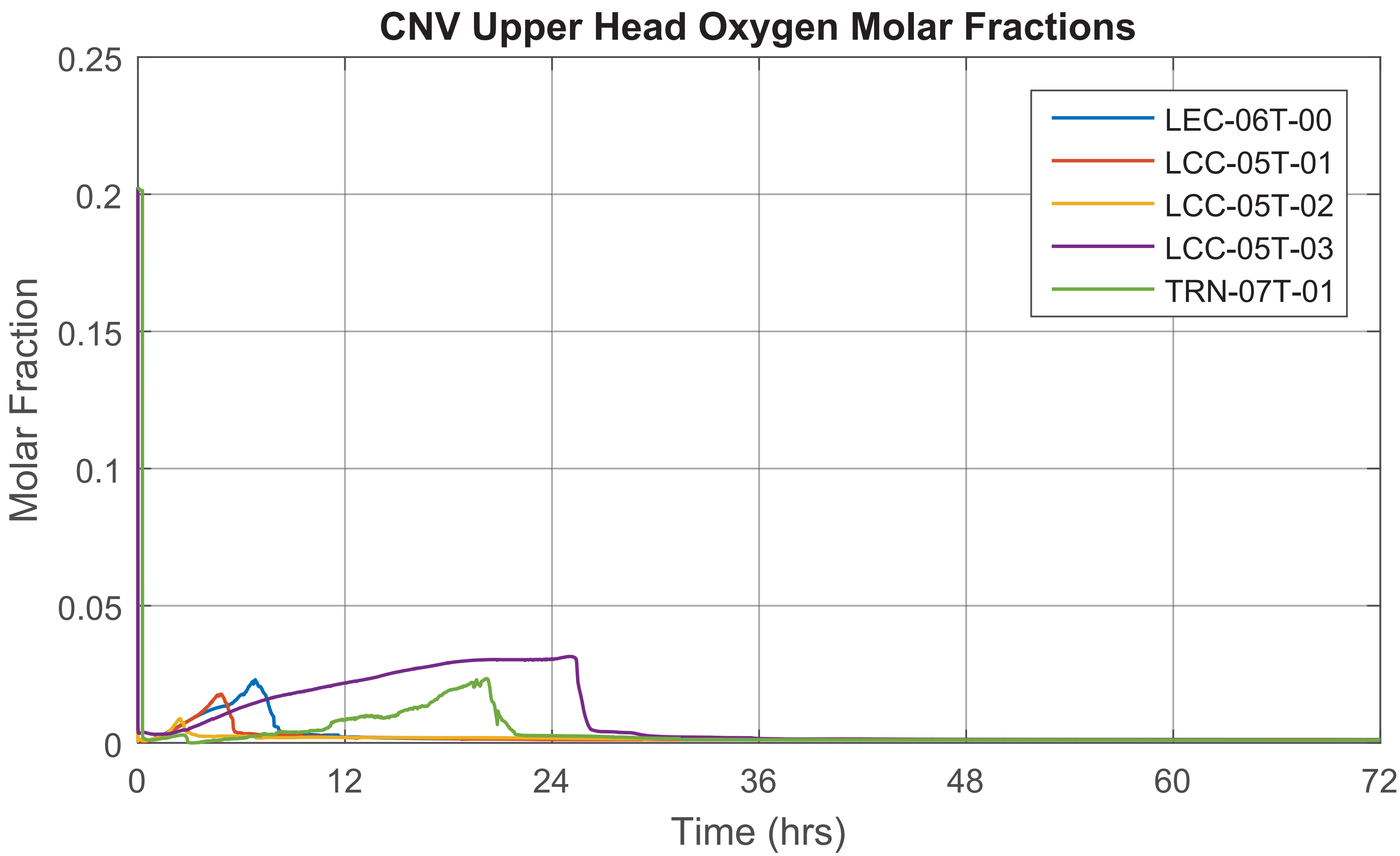


Figure 19.2-11: Pressure Differential between Reactor Pressure Vessel and Containment Vessel

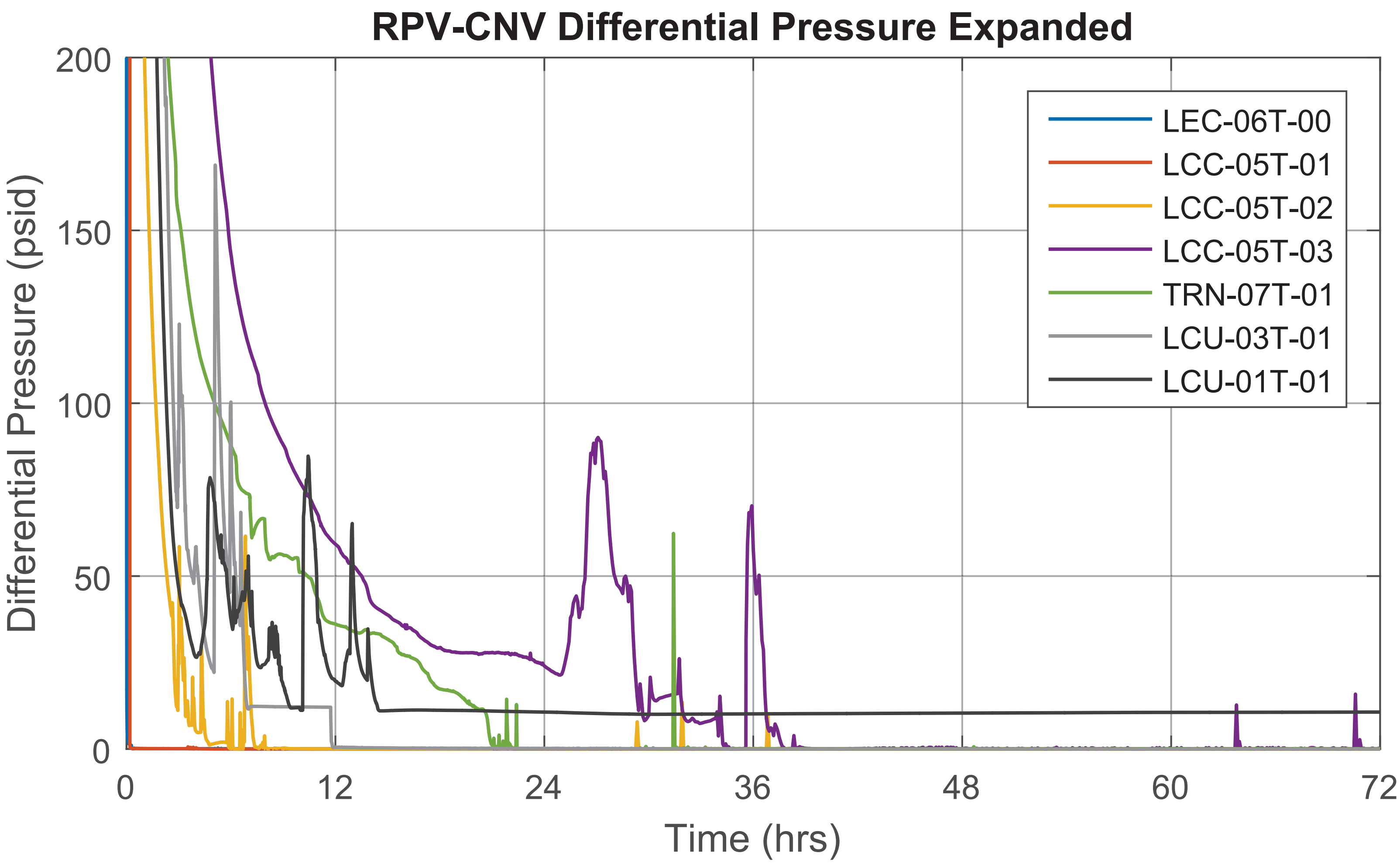
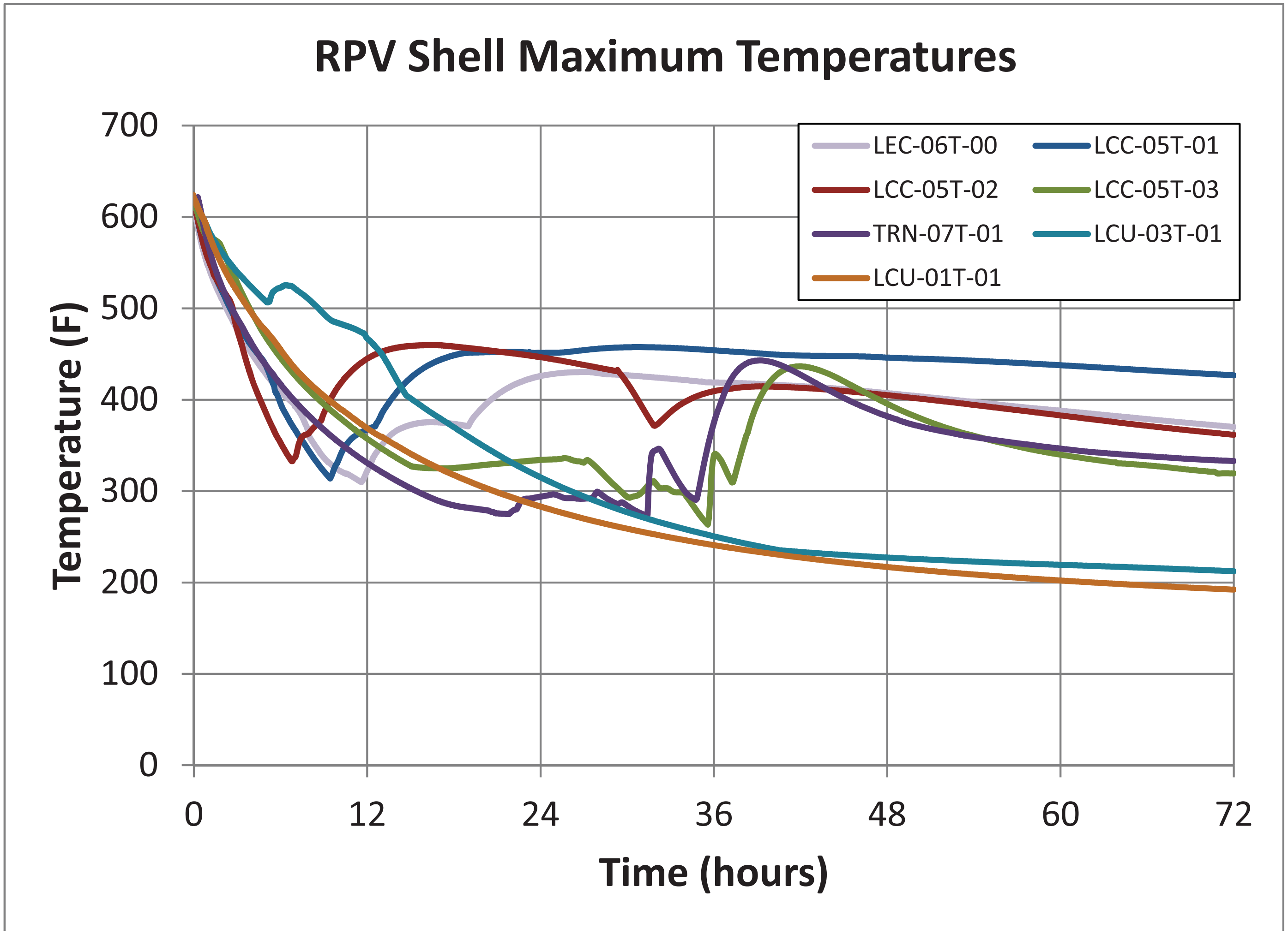


Figure 19.2-12: Maximum Reactor Pressure Vessel Shell Temperatures during Severe Accidents



19.3 Regulatory Treatment of Non-Safety Systems

Regulatory oversight is required for certain nonsafety-related structures, systems, and components (SSC) that perform risk-significant functions, consistent with NRC policy. The regulatory oversight is identified for specific SSC by the regulatory treatment of non-safety systems (RTNSS) process.

The RTNSS process provides assurance that:

- the design of the nonsafety-related, risk-significant SSC satisfies the performance capabilities and reliability/availability (R/A) missions;
- proper design information for the reliability assurance program, including the design information for implementing the Maintenance Rule, is included; and
- proper short-term availability control mechanisms, if required for safety and determined by risk significance, are provided.

This section describes the process for identifying nonsafety-related SSC that perform risk-significant functions in accordance with RTNSS criteria, and for determining the appropriate levels of regulatory treatment required. The RTNSS criteria are provided below. The RTNSS scope, process, and criteria are consistent with the guidance of NUREG-0800 Section 19.3, SECY-94-084, and SECY-95-132.

19.3.1 RTNSS Criteria

The criteria used to determine the functions performed by the nonsafety-related SSC that perform risk-significant functions, and therefore, are candidates for regulatory oversight, are established in NUREG-0800 Section 19.3 as follows:

A. SSC functions relied upon to meet beyond design basis deterministic NRC performance requirements, such as those set forth in 10 CFR 50.62, for mitigating anticipated transients without scram (ATWS) and in 10 CFR 50.63 for station blackout (SBO).

B. SSC functions relied upon to ensure long-term safety (the period beginning 72 hours after a design basis accident and lasting the following 4 days) and to address seismic events.

C. SSC functions relied upon under power-operating and shutdown conditions to meet NRC goals of a core damage frequency (CDF) of less than 1.0E-4 each reactor year and a large release frequency (LRF) of less than 1.0E-6 each reactor year.

D. SSC functions needed to meet the containment performance goal, including containment bypass, during severe accidents.

E. SSC functions relied upon to prevent significant adverse systems interactions between passive safety systems and active non-safety SSC.

The designation of the SSC within the RTNSS program scope reflects the applicable criterion. For example, the SSC which satisfy RTNSS criterion A are designated as RTNSS A SSC.

The identification of RTNSS SSC functions and components is performed as part of design reliability assurance program (D-RAP) described in Section 17.4.

COL Item 19.3-1: A COL applicant that references the NuScale Power Plant design certification will identify site-specific regulatory treatment of nonsafety systems (RTNSS) structures, systems, and components and applicable RTNSS process controls.

As noted in the criteria above, the RTNSS SSC selected for regulatory oversight are nonsafety-related SSC that are necessary to meet NRC regulations, safety goal guidelines, and containment performance goal objectives. The RTNSS systems needed to meet Criteria A, B, and E are based on deterministic considerations (with probabilistic risk assessment (PRA) contributing to determining systems needed to meet Criterion B), and the RTNSS systems needed to meet Criteria C and D are based on probabilistic insights including results from the baseline PRA and a focused PRA sensitivity study. The PRA is described in Section 19.1.

19.3.2 SSC Identification and Designation within RTNSS Program Scope

The scope of the RTNSS program includes those nonsafety-related SSC that satisfy the RTNSS criteria listed in Section 19.3.1 and are therefore subject to additional regulatory treatment. The following sections provide a discussion of the evaluation of the nonsafety-related SSC, and the results of the evaluation.

19.3.2.1 RTNSS A

Nonsafety-related SSC functions identified through the D-RAP process in Section 17.4 were evaluated to determine whether they are relied upon to meet beyond design basis performance requirements for ATWS (10 CFR 50.62) and SBO (10 CFR 50.63).

The regulations in 10 CFR 50.62(b) define ATWS as an anticipated operational occurrence followed by a failure of the reactor trip portion of the protection system. Each pressurized water reactor must have equipment that is diverse from the reactor trip system to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS in accordance with 10 CFR 50.62(c)(1). The NuScale design does not include an auxiliary or emergency feedwater system; therefore, this portion of the rule is not applicable. Additionally, NuScale is seeking an exemption from the requirement for a diverse turbine trip system, as described in Section 7.1.6, based on the design of the module protection system (MPS). The intent of the diverse turbine trip system is met through diversity within the MPS design which addresses the concern of a common cause failure. The MPS is a safety-related system and not subject to RTNSS criteria. The focused PRA was also examined to see if any nonsafety-related SSC are required to mitigate an ATWS. The focused PRA indicates that a module does not require nonsafety-related SSC to meet the ATWS goal of 1.0E-5 per reactor year.

The regulations in 10 CFR 50.63 require, in part, that a light water reactor must be designed to withstand, for a specified duration, and recover from an SBO. The SBO coping analysis for the NuScale Power Plant is described in Section 8.4 and concludes that the design functions adequately during an SBO. However, the normal coping strategy includes reliance on the nonsafety-related DC power supplies, consistent with the regulations in 10 CFR 50.63(a)(2). Although nonsafety-related DC power is utilized during the normal coping strategy, the SBO analysis described in Section 8.4 also demonstrates that core cooling and containment integrity are successfully maintained with only safety-related systems and no reliance on DC power systems. As such, there are no SSC for mitigating SBO that meet RTNSS criteria.

Since the issuance of SECY-95-132 that revised portions of SECY-94-084, the NRC has not identified any additional beyond design basis deterministic requirements within the scope of RTNSS A SSC (in addition to those for ATWS and SBO discussed above).

Based on the consideration of beyond design basis deterministic NRC performance requirements for ATWS and SBO, there are no SSC that meet the RTNSS A criteria.

19.3.2.2 RTNSS B

Nonsafety-related SSC functions identified through the D-RAP process in Section 17.4 are evaluated to determine whether they are relied upon to:

- provide a long term nonsafety-related back-up to passive system functional capability and for a period after 72 hours up to 7 days following an accident.
- meet the acceptance criteria for the seismic margins analysis (SMA).

The safety analyses, PRA insights, and expert panel considerations (discussed in Chapter 15, Section 19.1, and Section 17.4, respectively) did not identify any nonsafety-related SSC relied on to perform a backup to passive safety functions (i.e., ensure long term safety) in the period of 72 hours to 7 days.

The NuScale Power Modules are partially immersed in the reactor pool and protected using safety-related SSC. The reactor pressure vessel is housed in a steel containment vessel (CNV) that transfers sensible and core decay heat through the CNV walls to the ultimate heat sink which provides an effective passive heat sink for both short and long-term heat removal. The functions of core cooling and containment cooling are performed by safety-related SSC that operate automatically without operator action, fail-safe on a loss of power, and are passively maintained for extended periods following an accident. Therefore, nonsafety-related SSC are not relied on to perform a RTNSS B function for a period after 72 hours up to 7 days following an accident to ensure long-term safety.

The RTNSS B evaluation process also considered if any nonsafety-related SSC were candidates for additional regulatory oversight from seismic considerations.

As described in Section 19.1.5.1, both active and passive, nonsafety-related SSC are modeled in the SMA. None of the active, nonsafety-related SSC in the SMA are critical to a success path that averts core damage or a large release. These SSC are in the SMA model, but are modeled with high failure rates so there is limited credit for success following a seismic event. These active, nonsafety-related SSC do not have a substantial impact on the plant risk because failure of active components (such as pumps, compressors, and switches) to perform during or after a seismic event have no effect on the seismic margin due to the high reliability of the passive SSC in the NuScale design. Also, in the NuScale design, the passive mitigating systems fail safe on loss of power.

This results in very few component failures that have the potential to contribute to seismic risk. Random failures of safety-related SSC, such as the emergency core cooling system (ECCS) valves or reactor safety valves (RSVs), would also be required to cause core damage following an earthquake. Because failure of the active, nonsafety-related SSC in the SMA does not affect the seismic margin, they have not been included in the scope of the RTNSS program.

For passive, nonsafety-related SSC, the SMA includes fragility analyses for two nonsafety-related structures: the reactor building crane (RBC) and the bioshields. FSAR Section 19.1.5.1.2 provides the results from the SMA, which show that the plant design meets the regulatory requirement for a high confidence of low probability of failure (HCLPF) value that is greater than 1.67 times the design basis safe shutdown earthquake (SSE). FSAR Table 19.1-35 shows that both the RBC and the bioshields have a HCLPF value above the regulatory expectations. As shown in Table 3.2-1, the RBC is classified as Seismic Category I and the bioshields are classified as Seismic Category II so both meet the design requirements of Regulatory Guide 1.29 to ensure that they have sufficient capacity during and after an SSE. Thus, additional regulatory oversight for these components was not identified under the scope of the RTNSS program.

Therefore, no nonsafety-related SSC meet the RTNSS B criteria.

19.3.2.3 RTNSS C

Nonsafety-related SSC functions were evaluated to determine whether they are relied upon under power operating and shutdown conditions to meet the NRC core damage frequency goal of less than 1.0E-4 each reactor year and large release frequency goal of less than 1.0E-6 each reactor year.

A focused PRA, described in Section 19.1.9.3, evaluated CDF by assuming that only safety-related SSC function and all nonsafety-related SSC fail. The results of the focused PRA determined that the CDF and LRF goals are met by relying on only safety-related SSC (i.e., without crediting nonsafety-related SSC).

Also, nonsafety-related active systems were considered for including in the scope of the RTNSS Program to compensate for the uncertainties in the PRA and in the modeling of severe accident phenomenology. The PRA explicitly assessed the uncertainties in the modeling and performance of passive safety systems including assessing the likelihood that the passive safety systems in a NuScale plant might be operating outside of the conditions in which core heat removal would be effective.

The section titled, Thermal-Hydraulic Uncertainty, in Section 19.1.4.1.1.5 summarizes the comprehensive assessment of the performance of the DHRS and ECCS, which are safety-related passive heat removal systems incorporated in the NuScale design.

The results of the analyses performed for the assessment provide the bases for probabilistic characterizations of the effectiveness and likelihood of failure of these two passive heat removal processes. That is, this assessment explicitly characterizes the uncertainties associated with the operating regimes for each of these two passive processes to be effective. The assessment generated the probabilities that each of these passive processes would fail to operate effectively. Table 19.1-10 provides calculated probabilities for the failure of passive heat transfer for each system. Tables 19.1-11 and 19.1-12 identify the phenomena impacting passive reliability for each system. In addition, Tables 19.1-22 and 19.1-31 include the results of sensitivity studies that increased the failure probability of passive heat removal for each system by an order of magnitude to provide additional insights on modeling uncertainties and establish confidence in the failure rates.

The failure probabilities and associated uncertainty estimates provided in Table 19.1-10 for failure of the two passive heat removal systems to operate effectively are explicitly included in the NuScale PRA model that is used to generate CDF and LRF results. These failure probabilities are likewise explicitly included in the RTNSS evaluation for the RTNSS C acceptance criterion. As described above, the focused PRA demonstrated that reliance on nonsafety-related systems is not needed to achieve this RTNSS C criterion. The assessment of the uncertainty of the effectiveness of the highly reliable passive DHRS and ECCS heat removal systems 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 the Commission 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 RTNSS D

Nonsafety-related SSC functions identified through the D-RAP process in Section 17.4 were evaluated to determine whether they are needed to meet the containment performance goal, including containment bypass, during severe accidents. The severe accident evaluation used to identify these SSC functions is described in Section 19.2.

As discussed in Section 19.1, the containment design meets the containment performance goals. Accordingly, the containment provides a reliable, leak-tight barrier by ensuring that containment stresses do not exceed ASME service level C limits for a minimum period of 24 hours following the onset of core damage. Following this 24-hour period, the containment continues to provide a barrier against the uncontrolled release of fission products.

The containment performance goal is a measure of containment performance and is calculated by dividing the LRF by the CDF. The numeric value of the containment performance goal is 0.1, meaning that containment should fail no more than 10 percent of the times that core damage occurs. The PRA shows that the containment performance goal of 0.1 is met without relying on nonsafety-related SSC. Therefore, no nonsafety- related SSC meet the RTNSS D criteria.

19.3.2.5 RTNSS E

A systematic evaluation of potential significant adverse interactions between passive safety-related systems and active nonsafety-related systems was performed. This was accomplished by analyzing the system functions that were identified through the D-RAP process. The passive safety-related functions were identified first followed by identification of the active nonsafety-related functions that interface with the passive safety-related functions. The interactions between the systems were then analyzed to identify potential adverse interactions that could preclude the passive safety-related functionality from being accomplished. This systematic evaluation did not identify any significant adverse interactions between the active nonsafety-related systems and the passive safety-related systems. Therefore, no nonsafety-related SSC meet the RTNSS E criteria.

19.3.3 Functional Design of RTNSS Structures, Systems, and Components

A reliability/availability (R/A) mission is a set of requirements related to the performance, reliability, and availability of a risk-significant SSC function that adequately ensures the accomplishment of its task, as defined by the focused PRA or deterministic analysis.

No R/A missions are established for the nonsafety-related, risk-significant SSC since, as discussed in previous sections, no SSC are determined to meet the RTNSS criteria, and therefore, no RTNSS SSC are identified.

19.3.4 Focused Probabilistic Risk Assessment

The focused PRA is described in Section 19.1.9.3. The focused PRA is developed from the baseline PRA by removing nonsafety-related functions and their support from the baseline PRA model in order to assess the capability of the safety-related passive systems. The focused PRA demonstrates that credit for availability of nonsafety-related components is not needed to meet the Commission's CDF and LRF safety goals. Because the calculated risk metrics are much lower than the safety goals, risk and availability objectives are not established for nonsafety-related components.

The focused PRA maintains the same scope of initiating events and their frequencies as identified in the baseline PRA. The initiating event frequencies developed in Section 19.1 include consideration of nonsafety-related SSC as event initiators. The full power and shutdown PRA models are reviewed to determine whether nonsafety-related SSC could have a significant effect on the estimated frequency of initiating events using the screening criteria:

a) Does the calculation of the initiating event frequency consider the nonsafety-related SSC?

b) Does the unavailability of the nonsafety-related SSC significantly affect the calculation of the initiating event frequency?

c) Does the initiating event significantly affect the CDF and the LRF?

Based on the NuScale risk significance criteria discussed in Section 19.1.4.1.1.9, internal event initiators that contribute 20 percent or more to risk are evaluated for potential risk significance. Nonsafety-related SSC that contribute to potential initiating events are evaluated as unnecessary for inclusion in the RTNSS program because unavailability of nonsafety-related SSC would either (i) preclude module operation (e.g., CVCS), such that it would no longer contribute to an initiating event frequency or (ii) require that another nonsafety-related SSC (e.g., an AC bus) be aligned to support module operation, which indicates that unavailability has little effect on the initiating event frequency. The initiating event frequencies are generally based on generic industry data as discussed in Section 19.1.4.1.1.5. Additionally, sensitivity studies in Table 19.1-22 indicate that the CDF and LRF for the baseline PRA are not sensitive to initiating event frequencies.

The results of the focused PRA are considered in the development of the technical specification requirements. No nonsafety-related design features or functions are relied on to reduce the CDF or LRF below the Nuclear Regulatory Commission goals.

As discussed earlier, the focused PRA supports the identification of RTNSS C and RTNSS D SSC, while contributing to identifying RTNSS B SSC. No RTNSS B, RTNSS C, or RTNSS D SSC have been identified for the NuScale Power Plant design as a result of insights from the focused PRA.

19.3.5 Augmented Design Standards

Augmented design standards are required for RTNSS B SSC to assure reliable performance in the event of applicable hazards, such as natural phenomena. These natural phenomena hazards include safe shutdown earthquake, hurricane and tornado winds, and floods including internal flooding.

RTNSS B SSC are also required to be designed such that safety functions required in the post 72-hour through 4-day period following an accident can be accomplished with the required onsite equipment and supplies.

Since no RTNSS B SSC are identified for the NuScale Power Plant design, no RTNSS augmented design standards are applied.

19.3.6 Regulatory Treatment of RTNSS SSC

Regulatory oversight of RTNSS SSC may include Maintenance Rule (monitoring the effectiveness of maintenance), and either the Technical Specifications or a licensee controlled Availability Controls Manual.

The Availability Controls Manual is established in a manner similar to Technical Specifications and includes availability control limited conditions of operation (ACLCO) and availability controls surveillance requirements. Availability controls are commensurate with the assumptions in the PRA, and include, at a minimum, RTNSS B SSC. The establishment of ACLCO and surveillance requirements provides assurance that the RTNSS SSC can meet their R/A missions and that the component availability is consistent with its R/A mission.

Since no RTNSS SSC are identified, no additional regulatory oversight is required for any nonsafety-related risk-significant SSC.

19.3.7 Reference

19.3-1 NuScale Power, LLC, “Risk Significance Determination,” TR-0515-13952-A, Rev. 0, July 2015.

19.4 Strategies and Guidance to Address Loss of Large Areas of the Plant due to Explosions and Fires

Loss of large areas due to explosions and fires is addressed in Chapter 20.

19.5 Adequacy of Design Features and Functional Capabilities Identified and Described for Withstanding Aircraft Impacts

19.5.1 Introduction and Background

The plant design accounts for potential effects of a beyond-design-basis impact of a large commercial aircraft in accordance with 10 CFR 50.150(a). A design-specific aircraft impact assessment (AIA) has been performed using realistic analyses to demonstrate that:

1) the reactor core remains cooled or the containment remains intact; and

2) spent fuel cooling or spent fuel pool integrity is maintained

The NuScale Power Plant meets three of the four criteria (i.e., core cooling, containment intact, and spent fuel pool integrity) as discussed in the following sections.

The specific assumptions, including aircraft characteristics for the AIA are based on the guidance provided by Regulatory Guide (RG) 1.217, Revision 0, "Guidance for the Assessment of Beyond-Design-Basis Aircraft Impacts." This guidance endorses NEI 07-13, "Methodology for Performing Aircraft Impact Assessments for New Plant Designs," Revision 8 (Reference 19.5-1). The guidelines provided in NEI 07-13 are followed with no exceptions. The assessments were performed by qualified personnel with experience in applying the approved methodology.

19.5.2 Scope of the Assessment

The following effects of a large commercial aircraft impact are assessed:

1) physical damage resulting from the impact of the aircraft fuselage and wing structure and penetration of hardened aircraft components, such as engine rotor shafts and landing gear

2) shock damage resulting from shock-induced vibration on systems, structures, and components (SSC)

3) fire damage resulting from aviation fuel-fed fire

19.5.3 Assessment Methodology

The methodology provided in NEI 07-13 is used to assess the effects of the aircraft impact on the structural integrity of the Reactor Building (RXB) and to evaluate the physical, vibration, and fire effects on SSC in the RXB to ensure continued core cooling and spent fuel cooling capability.

19.5.3.1 Structures of Concern

Structures of concern are those structures that contain SSC necessary to ensure adequate cooling of the fuel in the reactor cores and spent fuel pool (SFP). All 12 NuScale Power Modules (NPMs), the ultimate heat sink (UHS), and the SFP are located inside the RXB. Containment is integral to each NPM. The 10 CFR 50.150(a) functions are accomplished if the RXB resists the impact loading and prevents wreckage and fire from perforating the exterior walls of the RXB. Therefore, the RXB is a building of concern. The Control Building (CRB) is a building of concern because core cooling is accomplished by operator control actions upon notification of an imminent aircraft impact. The arrangement of core cooling equipment inside the RXB, as shown on Figure 1.2-10 through Figure 1.2-18, is a key design feature.

19.5.3.2 Impact Locations

Below grade portions of the RXB are not susceptible to a direct impact by an aircraft. Elevations or portions of elevations may be screened from aircraft impact if intervening or adjacent structures meet the design requirements of NEI 07-13. The location of the RWB in relation to the RXB is a key design feature that limits potential strike locations to the west end of the RXB. The design of the exterior walls of the RWB, as described in Section 3.5.3.1.1, is a key design feature for crediting the RWB as an intervening structure. The RWB is located 25 feet to the west of the RXB, as described in Section 3.8.4.1.3. The roof of the RWB is approximately 49 feet above grade, as shown on Figure 1.2-33. For the structural analysis, the RWB is credited with protection of a portion of the west wall of the RXB. This credit is applied when determining wall thicknesses and configurations. No credit is taken for the Control Building (CRB) or the Turbine Generator Buildings as intervening structures. All other RXB elevations and faces above grade are vulnerable.

19.5.3.3 Assessment of Effects on Fuel Cooling Equipment

To assess the effects on fuel cooling equipment, physical damage, shock damage, and fire damage footprints are overlaid on the RXB general arrangement drawings. Fuel cooling equipment that is within these damage footprints is assumed to lose the ability to perform its function due to the associated physical, shock, or fire effects. The remaining fuel cooling equipment is evaluated to determine if adequate cooling of fuel in the reactors and SFP is maintained.

19.5.4 Assessment Results

19.5.4.1 Physical Damage

The RXB external walls have been assessed and shown to resist physical damage from postulated aircraft strikes. The design of the RXB as described in Section 3B.2 is a key design feature. The design of the RXB equipment door to the RXB as described in this section is a key design feature for protecting core cooling equipment from impacts through the RWB trolley bay. The RXB equipment door is a large, concrete door that is on a series of rails. It can be moved in place for normal operations and out of place when large equipment is moved into and out of the RXB. The door fits like a plug into the exterior wall of the RXB in that it is tapered along the top and sides and is sealed against the building. The door is five-feet thick with steel plate along the outside, and is filled with 5000 psi reinforced concrete. The steel plates are either 1" or 2" thick (see Figure 19.5-1 through Figure 19.5-3).

The design of the Reactor Building HVAC intake awnings and the design of the pipe shields, shown on Figure 1.2-17 through Figure 1.2-19, and described in this section, are key design features for preventing physical damage and fire from entering the RXB.

The awnings protecting the HVAC intakes and pipe penetrations are constructed of 7000 psi concrete with two #11 bars at 12 inches on center each way, top and bottom. In addition, the awning protection has #5 shear ties at 12 inches on center (see Figure 19.5-4).

Based on NEI 07-13 criteria, physical damage from strikes to external openings in the RXB external walls is shown to be restricted to a single vestibule on the exterior of the RXB. There is no equipment in that location that could impact fuel cooling capability.

The trolley on the Reactor Building crane (RBC) cannot be struck and dislodged, because there is no perforation of the RXB outer wall. The design of the RBC is a key design feature for ensuring that impact loads from an aircraft impact on the exterior wall of the RXB prevent the crane from falling into the reactor pool area and either damaging the NPMs or tearing the reactor pool lining. The design and location of the RBC, as described in Section 9.1.5, is a key design feature for protecting the NPMs and the reactor pool lining.

19.5.4.2 Shock Damage

The impact of a commercial aircraft on the RXB structure causes a short duration, high acceleration, high frequency vibration. Shock damage distances are measured from the center of the initial impact along a structural pathway to the affected equipment.

The shock effect is at its greatest at the 100' elevation, and propagates into the UHS, which consists of the reactor pool, refuel pool, and spent fuel pool. NuScale Power Modules (NPM) are shut down by operator action prior to impact, and core cooling is provided by passive systems (i.e., DHRS). There are no SSC susceptible to shock (sensitive electronics or active components) on the NPMs that would interrupt or prevent successful core cooling once the reactor is tripped, the decay heat removal system is actuated, and the containment is isolated.

There is no impact of concern at or below the 50' elevation, other than for SFP cooling. Affected equipment at the 62', 75', 86', and 125' elevations is not required to maintain core cooling or spent fuel cooling.

19.5.4.3 Fire Damage

The design and location of three-hour fire barriers and three-hour, 5-psid fire barriers, including walls, floors, fire dampers, doors, equipment access door, and penetration seals within the RXB are key design features for the protection of core cooling equipment from the impact of a large commercial aircraft. The assessment credited the design and location of fire barriers, as depicted on Figure 1.2-10 through Figure 1.2-18, to limit the effects of internal fire within the RXB to the access vestibules and stairwells. There is no equipment required to maintain core cooling or spent fuel cooling in the access vestibules and stairwells. In addition, the design and location of 5-psid, fast-acting blast dampers in the Reactor Building HVAC system air intakes and exhaust lines (as described in Section 9.4.2.2.1 and shown on Figure 9.4.2-1) are key design features.

These key design features ensure that necessary core cooling equipment is protected from fire damage for postulated strikes.

19.5.5 Assessment of Acceptance Criteria

19.5.5.1 Containment Intact

The containment system (CNTS) is an integral part of the NPM and provides primary containment for the reactor coolant system (RCS). The CNTS includes the containment vessel (CNV), CNV supports, containment isolation valves (CIVs), passive containment isolation barriers, and containment instruments.

The CNV is an evacuated pressure vessel fabricated from low-alloy steel and austenitic stainless steel, as described in Section 3.1.5, Section 3.8.2, and Section 6.2.1 through Section 6.2.4. The CNV is maintained partially immersed in a below-grade, borated-water-filled, stainless steel-lined, reinforced concrete pool to facilitate heat removal.

The containment remains intact if the ultimate pressure capability of the CNV, as described in Section 3.8.2.4.5, is not reduced as a result of the aircraft impact. As stated in Section 19.5.4.1 and Section 19.5.4.3, there is no physical damage or fire damage to equipment required for fuel cooling in the RXB, including the CNTS. There is far shock that reaches the CNTS, but there are no components necessary for maintaining the containment intact that would be affected. Therefore, the containment remains fully intact.

The design of the CNTS, as described in Section 6.2.1 through Section 6.2.4, and the location of the CNTS, shown on Figure 1.2-5, are key design features for maintaining an intact containment.

19.5.5.2 Core Cooling

The NPM, described in Section 4.1, is a self-contained nuclear steam supply system comprised of a reactor core, a pressurizer, and two steam generators integrated within the reactor pressure vessel (RPV) and housed in a compact, steel containment vessel. The RCS, as described in Section 5.1, is a subsystem of the NPM and is located in the CNV. During normal operation, the RCS transports heat from the reactor core to the steam generators through natural circulation. Heat is removed by the main condensers located in the Turbine Building.

Post reactor trip, there are two independent, safety-related, passive DHRSs, as described in Section 5.4.3, that provide redundant core cooling capability for each NPM without reliance on external power. An impact that ruptures the main steam or feedwater piping in the Turbine Building does not affect DHRS passive cooling capability. The DHRS initiation includes closure of the associated main steam and feedwater isolation valves inside the RXB, thereby preventing a loss of secondary side water through the damaged piping. The DHRS is capable of maintaining core cooling for 72 hours.

Upon notification of an imminent aircraft threat, the operators in the main control room scram the reactors, actuate the DHRS, and isolate containment. Heat from the DHRS is transferred passively to the reactor pool that serves as the UHS, (described in Section 9.2.5 and Section 3B.2), which is located below grade in the RXB.

There are no systems with open-water sources (e.g., circulating water system) located in the RXB physical damage footprint for any strike. As such, internal flooding is not an issue of concern.

Containment penetrations are on the CNV, which is protected from impact by the RXB exterior walls. The location of the CNV penetrations and isolation valves, as described in Section 6.2.4, is a key design feature that ensures containment isolation.

There are no control or protective functions that are necessary after aircraft impact for 72 hours, as described in Section 9.2.5.4.

The NPMs, RCS, CNV, DHRS, containment isolation valves, and UHS are key design features for ensuring core cooling, as described above. The closure of the MSIVs and FWIVs, as described in Section 5.4.3.2 and Section 6.2.4, are key design features for ensuring DHRS operation. The ability to scram the reactors, isolate containment, and actuate the DHRS from the MCR, as described in Section 7.0.4.1.2, Section 7.0.4.1.3, Section 5.4.3.2, and Section 6.2.4, are key design features for ensuring the reactor is tripped, containment is isolated, and the DHRS is actuated prior to aircraft impact. Since there is no physical damage to the core cooling equipment in the RXB, the control rod drive system is undamaged and available to initiate a scram, either manually from the MCR or by manually tripping the reactor trip breakers. The design and location of the control rod drive system, as described in Section 4.6, is a key design feature for ensuring a scram can be initiated after impact if the reactor was not scrammed prior to impact.

19.5.5.3 Spent Fuel Pool Integrity

The east, west, and south SFP walls are constructed as described in Section 3B.2. The north SFP wall is a 6 foot thick interior concrete wall with 4 layers of #11 reinforcing bar spaced 12 inches on center in both the horizontal and vertical direction on both faces of the wall. The foundation of the SFP is constructed as described in Section 3.8.5. The reinforced concrete walls and floor have a stainless steel liner as described in Section 3.8.4. The SFP is integrated into the RXB structure and is located below grade. Because the SFP is completely below grade, an aircraft impact cannot strike the pool or the pool liner. Because there is no damage to the pool structure or liner, there is no loss of water level and SFP integrity is maintained. The location of the SFP, as described in Section 9.1.2 and shown on Figure 1.2-10 through Figure 1.2-16, is a key design feature for maintaining SFP integrity from a direct aircraft impact.

There are three hoist systems inside the RXB that can be operated over the SFP area: the fuel handling machine the new fuel jib crane, and the new fuel elevator. Provisions are in place to prevent the RBC from being moved over the SFP, as described in Section 9.1.5.3 and shown on Figure 9.1.5-1 and Figure 9.1.5-2. There are seismic restraints on the RBC, as shown on Figure 9.1.5-3. Because the exterior wall of the RXB is not perforated, the trolleys cannot be dislodged to fall into the reactor pool.

Additionally, there are seismic restraints on the fuel handling machine, as described in Section 9.1.4.2.2 and shown on Figure 9.1.4-2. The design and location of the fuel handing equipment, as described above, is a key design feature for ensuring the hoists remain intact and cannot fall into the SFP and perforate the SFP liner.

19.5.5.4 Spent Fuel Pool Cooling

Spent fuel pool cooling is not maintained for the postulated strike locations due to shock or to loss of power. However, as described in Section 19.5.5.3, SFP integrity is maintained, and SFP cooling is not required. Although forced cooling is lost, the SFP is part of the UHS, which provides a very large water inventory and ensures an adequate water level is maintained above the spent fuel assemblies for beyond the mission time, even with the loss of forced SFP cooling, as described in Section 9.1.3.3.5.

19.5.5.5 Plant Monitoring and Control

For the postulated aircraft impact event, required operator actions occur prior to the aircraft impact, upon notification of the threat. Operators trip the individual NPMs and initiate containment isolation and decay heat removal systems. Following the aircraft impact event, monitoring functions are expected to remain available. However, in the event that post-AIA monitoring is determined to be unavailable, the mitigating strategies of FSAR Section 20.2 for the LOLA beyond-design-basis event are invoked. The actions taken by the Operators prior to the aircraft impact ensure that the reactor core and spent fuel remains cooled, containment remains intact, and spent fuel pool integrity is maintained.

19.5.6 Conclusion

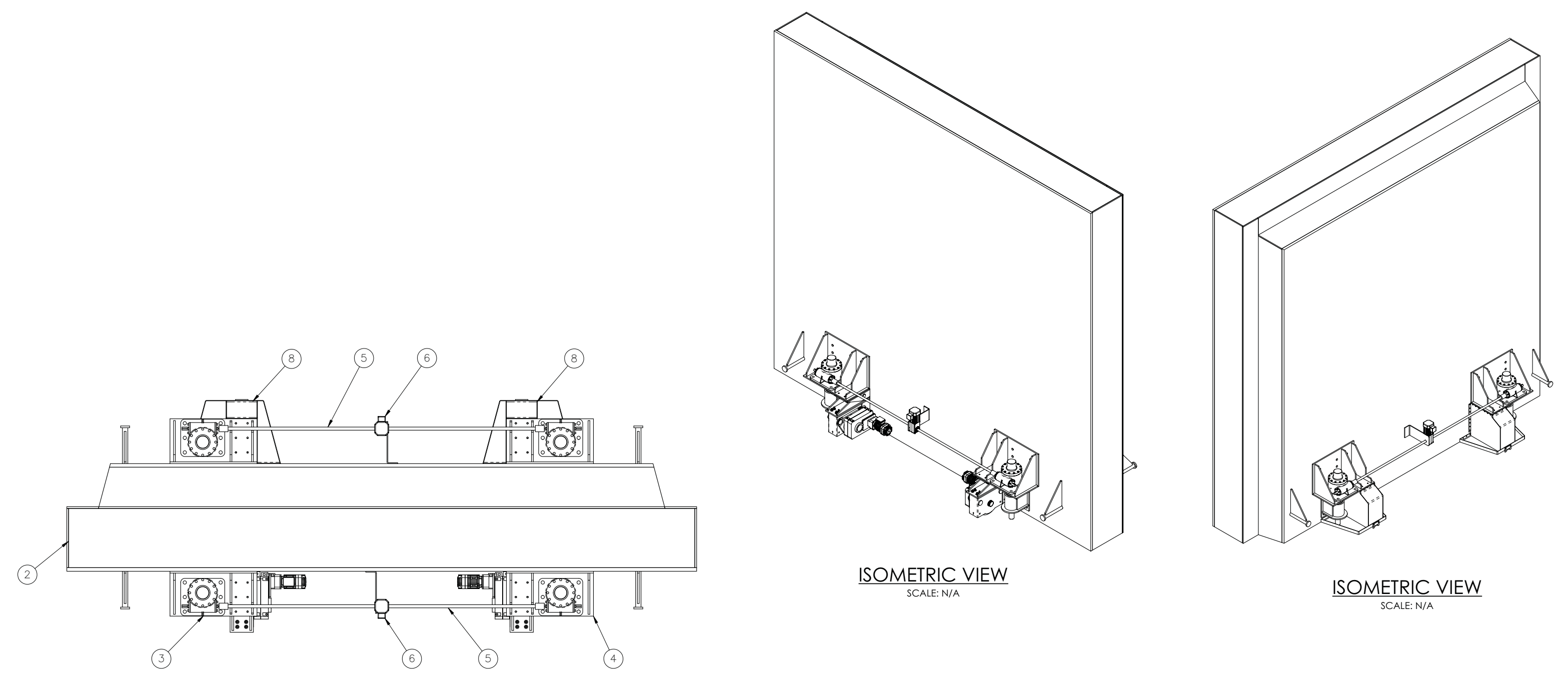
The aircraft impact assessment concludes that the NuScale Power Plant design and functional capabilities provide adequate protection of public health and safety in the event of an impact of the NRC defined large commercial aircraft. Containment intact, core cooling capability, and spent fuel pool integrity are not impaired as a result of the postulated aircraft impacts.

19.5.7 References

19.5-1 Nuclear Energy Institute, "Methodology for Performing Aircraft Impact Assessments for New Plant Designs," NEI 07-13, Rev. 8, Washington, DC, April 2011.

19.5-2 American Society of Mechanical Engineers, ASME NOG-1, “Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder),” ASME-NOG-1, 2004, New York, NY.

Figure 19.5-1: Reactor Building Equipment Door



DESCRIPTION	NO.
RXB EQPT DOOR ASSEMBLY	1
RXB EQPT DOOR WELDMENT	2
NON FLANGED WHEEL DRIVE ASSY (EAST–WEST)	3
FLANGED WHEEL DRIVE ASSY (EAST–WEST)	4
DRIVE SHAFT (LIFT JACKS) W/ COUPLERS	5
MOTOR, THRU BORE (DOOR LOCKING) W/ MOUNT BRACKET	6
DOOR WHEEL SHROUD WELDMENT	8
DOOR WHEEL SHROUD WELDMENT OPP HAND	9
RAIL SWEEP BRUSH (TBD)	10

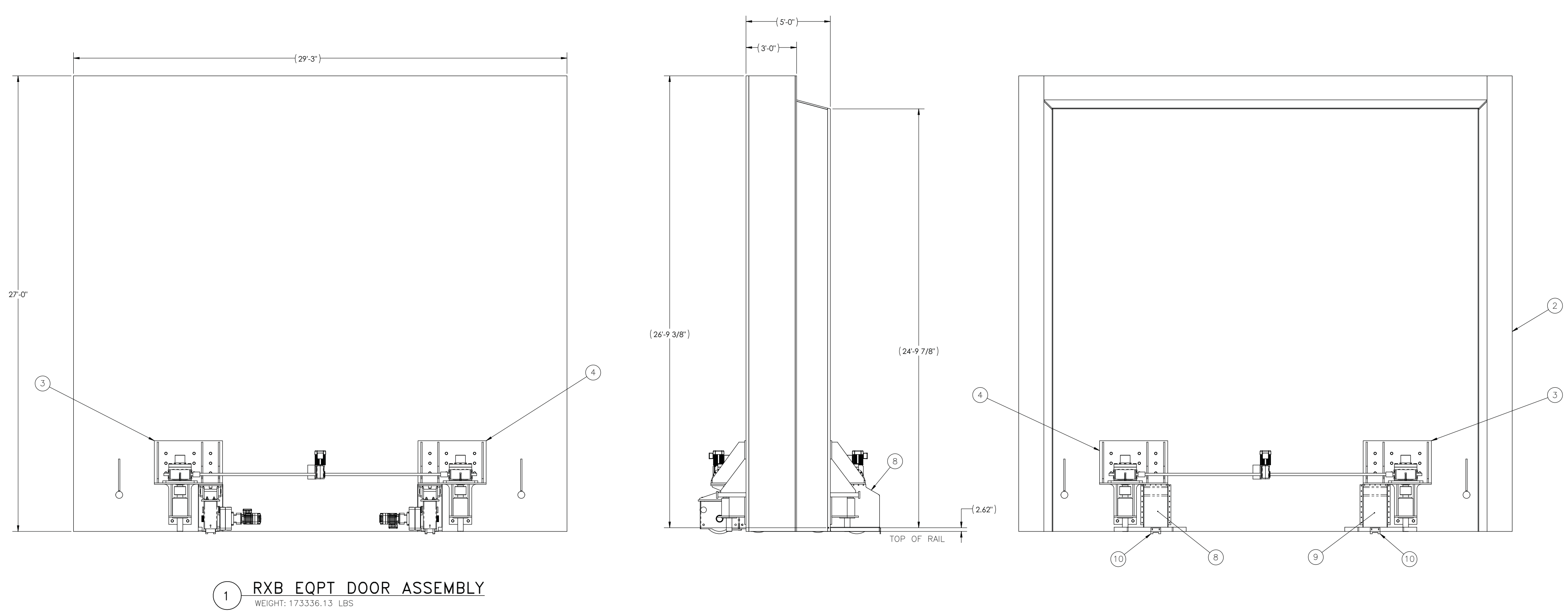
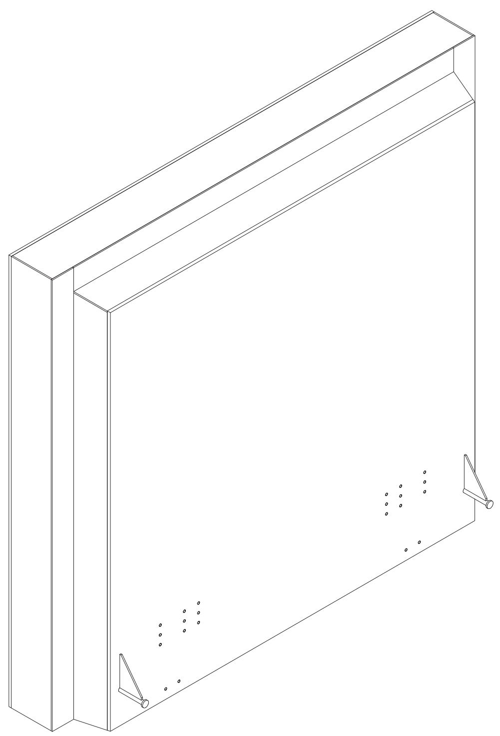


Figure 19.5-2: Reactor Building Equipment Door Weldment



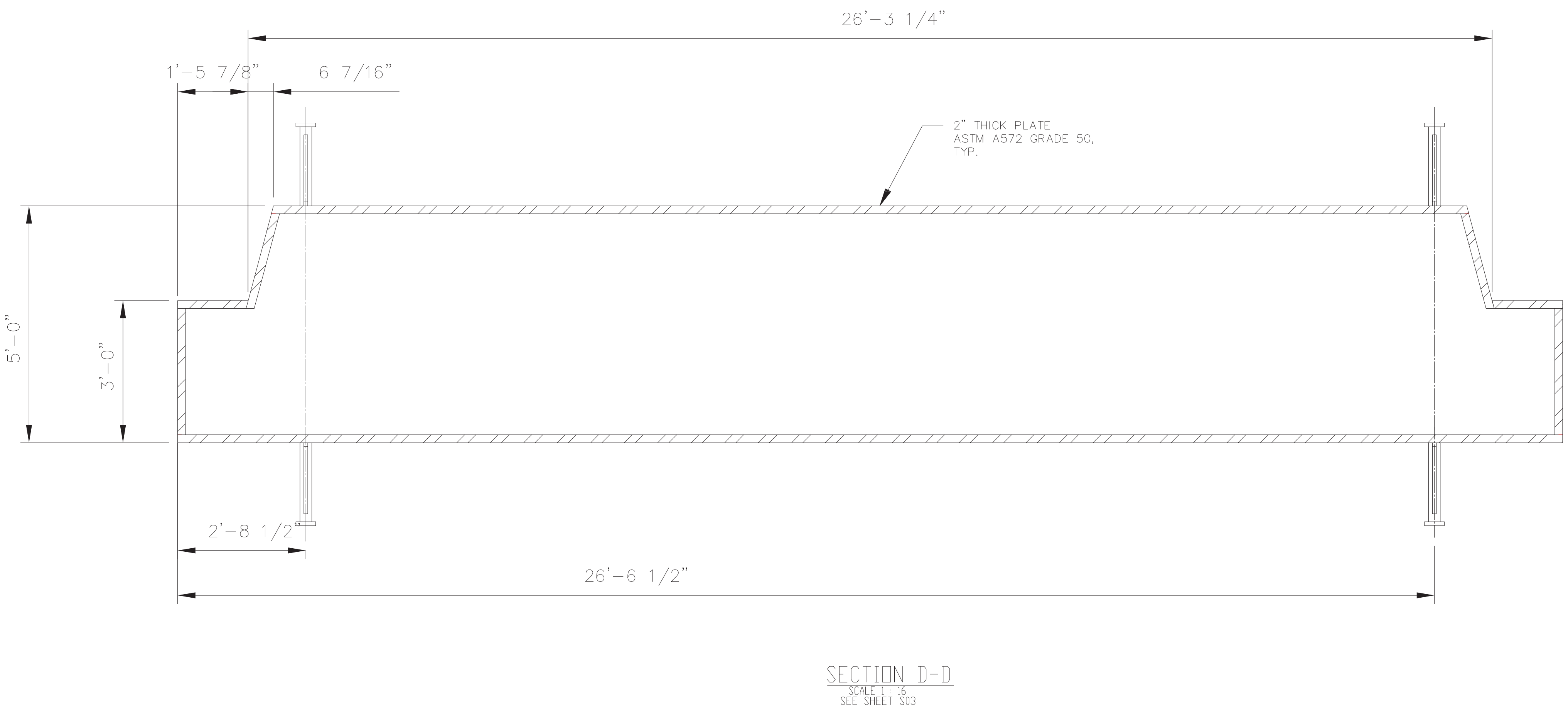


Figure 19.5-3: Reactor Building Equipment Door Assembly – Rebar Detail

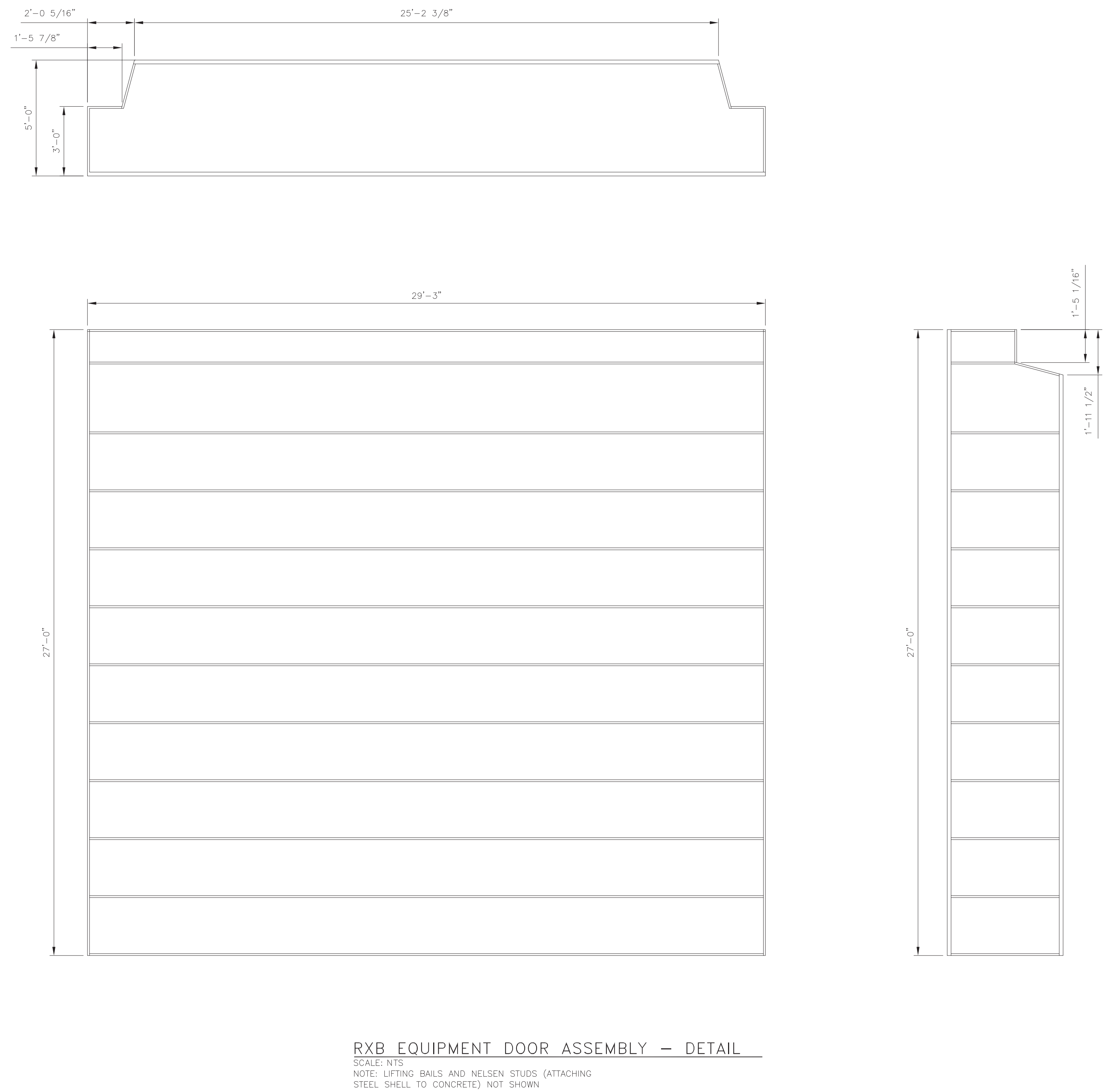


Figure 19.5-4: Reactor Building Structural Concrete