NUSCALE™
Power for all humankind

NuScale US460 Plant
Standard Design Approval Application

Chapter Nineteen

Probabilistic Risk Assessment and Severe Accident Evaluation

Final Safety Analysis Report

Revision 1

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF TABLES

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES

CHAPTER 19 PROBABILISTIC RISK ASSESSMENT AND SEVERE ACCIDENT EVALUATION

19.1 Probabilistic Risk Assessment

The PRA is performed consistent with the requirements of 10 CFR 52.137(a)(25). It assesses the risk for a single NuScale Power Module (NPM) and includes Level 1 and Level 2 evaluations. The PRA follows the guidance in interim staff guidance (ISG) DC/COL-ISG-028 (Reference 19.1-3). This ISG applies to a standard design as an acceptable approach to conforming with American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS) RA-S-2008 (Reference 19.1-1) and addenda ASME/ANS RA-Sa-2009 (Reference 19.1-2), as endorsed by Regulatory Guide (RG) 1.200, Revision 3. The PRA supporting the standard design does not include a Level 3 evaluation (although NuScale performed a limited offsite consequence assessment to support the evaluation of potential design improvements in Section 19.2.6).

When addressing general concepts, the term "PRA" refers collectively to the Level 1 and Level 2 risk metric evaluation as well as the phenomenological evaluation of severe accident response. Because of a small radionuclide inventory in a single module compared to typical, currently operating plants, risk metrics associated with small modular reactors have different implications for public health and safety. To reflect this perspective, and to clarify that the calculated risk metric values are based on a PRA for a single module, this chapter uses the terms core damage frequency (CDF) and large release frequency (LRF) to present results for CDF and large release frequency calculations for a single module. When referring to multi-module (MM) risk metrics, the chapter uses terms "multi-module core damage frequency" (MM-CDF) and “multi-module large release frequency” (MM-LRF). The conditional containment failure probability (CCFP) refers to the risk metric associated with failure of a containment vessel (CNV), which houses a reactor pressure vessel (RPV). Together, the CNV and RPV comprise the NPM.

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 (IEs) that can be addressed at the standard design stage. NuScale assesses the risk associated with multi-module operation using a systematic approach that includes both a qualitative evaluation of the potential impact of shared systems and a quantitative assessment based on the single-module, full-power, internal-events PRA to identify potential multi-module risk contributors.

This section summarizes key aspects of the PRA and associated insights. Supporting documentation including 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 standard design, combined license (COL) (or other applications), 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 US460 standard design. As such, the PRA identifies dominant severe accident sequences, risk-significant structures, systems, and components (SSC) and key operator actions. The PRA evaluates insights from currently operating plants and conformance with NRC safety goals and design alternatives for significance to the NuScale design. Table 19.1-1 summarizes specific uses of the PRA.

19.1.1.2 Combined License Application Phase

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

19.1.1.2.1 Use of Probabilistic Risk Assessment in Support of Programs

COL Item 19.1-1: An applicant that references the NuScale Power Plant US460 standard design 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: An applicant that references the NuScale Power Plant US460 standard design will identify and describe specific risk-informed applications being implemented during the COL application phase.

19.1.1.3 Construction Phase

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

19.1.1.3.1 Use of Probabilistic Risk Assessment in Support of Programs

COL Item 19.1-3: An applicant that references the NuScale Power Plant US460 standard design 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: An applicant that references the NuScale Power Plant US460 standard design 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 following section describes use of the PRA in the operational phase (from initial fuel loading through commercial operation).

19.1.1.4.1 Use of Probabilistic Risk Assessment in Support of Programs

COL Item 19.1-5: An applicant that references the NuScale Power Plant US460 standard design 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: An applicant that references the NuScale Power Plant US460 standard design 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 standard design rather than an as-built, as-operated 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 is applicable to the technical adequacy of the PRA for a standard design.

The PRA has sufficient detail to meet 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, bounding but realistic assumptions are made to ensure that an appropriate safety margin exists for risk-informed information provided by the PRA.

The methodology used in the PRA that supports the US460 standard design is the same as that used in the NuScale US600 standard design (Docket No. 52-048), which was subject to an independent review by selected experts. Self-assessments based on the ASME/ANS PRA standard supporting requirements were performed for the PRA. This approach ensures that the PRA is appropriate to provide results and risk insights.

19.1.2.1 Probabilistic Risk Assessment Scope

The PRA addresses internal and external initiating events (or "initiators") and operating modes, which are represented by specific evaluations of “full” or "at-power" conditions and at LPSD conditions. The PRA evaluates 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 six-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 standard design. 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.

NuScale applied conservative, but realistic, assumptions to account for these uncertainties to ensure that 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 design.

19.1.2.3 Probabilistic Risk Assessment Technical Adequacy

The PRA is consistent with the guidance in DC/COL-ISG-028, which supplements RG 1.200 as an acceptable approach to demonstrate that the PRA used in the standard design has a sufficient level of technical adequacy. Conformance with this regulatory guidance ensures that the PRA is technically adequate to provide confidence in the results and risk insights.

The PRA meets the DC/COL-ISG-028 guidance 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 (Reference 19.1-1).

The NuScale Power Plant US460 standard design can incorporate up to six modules. Evaluation of the risk of multiple-module operation is based on the single-module, full-power, internal-events PRA. The PRA uses a systematic process 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 standard design.
- 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.

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.

19.1.3.1 Design and Operational Features for Preventing Core Damage

The 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. This design feature reduces the 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 reactor coolant pumps, which eliminates the potential for reactor coolant pump seal failure events.
  - There are no RPV or CNV penetrations below the top of the reactor core.
- The response to a loss of reactor coolant system (RCS) inventory inside containment is simplified because inventory makeup from external sources is not required to prevent core uncovery; only recirculation of RCS inventory from the CNV to the RPV through the emergency core cooling system (ECCS) valves is needed.
- 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.

- The evacuated steel CNV allows elimination of RPV insulation, which eliminates potential sump blockage concerns.
- Containment volume is sized so that the core does not uncover for initiating events associated with loss of RCS inventory inside containment or isolated pipe breaks outside the CNV.
- 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 design includes features that arrest progression of a postulated core damage event and prevent releases from containment, including:

- The containment system (CNTS) employs valves that fail-safe to their accident-response position on loss of power.
- The evacuated CNV 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 the CNV are partially 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 design includes features intended to terminate containment releases and minimize offsite consequences:

- A reactor core has a relatively small amount of radioactive material available for release during a postulated accident.
- The CNV is partially immersed in an underground, stainless steel-lined, concrete pool (i.e., the UHS) that is sized to accommodate the heat load from operating modules and spent fuel for more than 30 days.
- In the event of a CNV breach below the reactor pool water level, the pool acts to filter radionuclides before they reach the environment.

19.1.3.4 Uses of Probabilistic Risk Assessment in the Design Process

The design was developed in consideration of issues associated with typical currently operating plants. Thus, there are several design features inherent to the design that address characteristics of currently operating plants related to operational risk. Table 19.1-2 summarizes these features, which contribute to a low 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 potential design improvements, as described in Section 19.2.6, is supported by PRA analyses.

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

This section discusses the internal events PRA for a single NPM operating at full power.

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 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 NPM. The full-power PRA addresses the risk associated with operation in Technical Specification Mode 1 (Operations).

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

NuScale constructed the PRA by first developing a representative spectrum of potential internal initiating events as discussed in Section 19.1.4.1.1.2. For each initiating event, a "Level 1" event tree illustrates 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, presented in Section 19.1.4.1.1.4, include safety-related and nonsafety-related mitigating systems.

The top events of the event trees are modeled using fault trees. Fault trees 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. Section 19.1.4.1.1.3 discusses success criteria.

Table 19.1-4 summarizes systems included in the PRA model. Table 19.1-5 is the system dependency matrix that illustrates interrelationship among the frontline systems, as indicated in the horizontal axis, and their supporting systems, on the vertical axis. Frontline systems are defined as those capable of performing an accident mitigating function and included as top events on an event tree. A matrix cell with an "X" indicates a dependency between a frontline system and a support system. For example, the containment flooding and drain system (CFDS) includes a dependency on the augmented DC power system (EDAS) to open the containment isolation valves (CIVs) to support injection. An "X^5" identifies that the dependency among systems is not required for accident mitigation because the design is fail-safe. For example, the ECCS is dependent on power to maintain valves closed as indicated by the relationship with the module protection system (MPS) that 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). 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.

For each initiating event and accident sequence represented by a Level 1 event tree, the outcome for a sequence is assigned an end state based on whether the NPM response to the initiating event is successful in terms of preventing core damage and containment failure. Sequences with successful mitigation that prevents core damage are indicated by "OK." Sequences that are not successfully mitigated are evaluated using a "Level 2" event tree as indicated by "LEVEL2-ET" and discussed in Section 19.1.4.2.1.

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 identify potential initiating events for the unique NuScale design from 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 as well as PRA studies from operating plants and advanced reactor designs. Key industry sources include:

- NUREG/CR-5750 (1999), "Rates of Initiating Events at US Nuclear Power Plants: 1987-1995."
- NUREG/CR-6890 (2005), "Reevaluation of Station Blackout Risk at Nuclear Power Plants, Analysis of Loss of Offsite Power Events: 1986-2004."
- EPRI NP-2230, "ATWS: A Reappraisal. Part 3. Frequency of Anticipated Transients" (Reference 19.1-11).
- NUREG/CR-6928 (2007), "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants."
- INL/EXT-21-65055, “Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants: 2020 Update,” (Reference 19.1-13).
- NUREG-1829 (2008), "Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process."
- "Advanced Light Water Reactor Utility Requirements Document" (Reference 19.1-16).

Failure modes and effects analyses are performed on systems whose failures are judged to have the potential for inducing an upset condition (i.e., initiating event), or negatively affect the NPM’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 IE 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 pressurized water reactors (PWRs).

The third technique for identifying 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 provides confirmation of the completeness of the initiating event spectrum identified by the other methods.

The potential initiating events that are identified by the three techniques are reviewed for applicability to the design and, if appropriate, screened from further consideration. For example, screening eliminates initiators associated with reactor coolant pump faults because reactor coolant pumps are not part of the 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 categories are established, as shown in the first column of Table 19.1-7:

- pipe breaks and LOCAs
- 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 NPM 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 “Pipe Breaks and Loss of Coolant Accidents" 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 in the "Initiator" and “Label” columns, respectively, of Table 19.1-7. 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.

19.1.4.1.1.3 Success Criteria

Per the ASME/ANS PRA Standard (Reference 19.1-1), 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 method 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 end in a stable or improving NPM configuration using the following definitions:

- Mission time is the period of time that a system or component is required to operate successfully to perform its function. Mission times are specified for components that are required to operate following an initiating event. Mission times take into account the time needed to reach a safe, stable, long-term condition, and time needed to establish long-term recovery actions. The PRA mission time is 72 hours.
- Core damage is defined as occurring when:
  - the collapsed level in the reactor has decreased such that active fuel in the core has been uncovered for a sustained period, and
  - a fuel peak cladding temperature (PCT) of 2200 degrees Fahrenheit or higher is reached as defined by the thermal-hydraulic calculation.

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. 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 the 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 following ECCS success.

- 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. In sequences where makeup inventory via CVCS is credited, operators initiate makeup with suction from the boron addition system (BAS), which can be used to support reactivity control. In addition, in sequences with success of ECCS, the ECCS supplemental boron function assures shutdown under cold conditions.
- 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 CNTS isolation valves to close. Containment isolation supports the system success criteria for avoiding core damage by

- achieving DHRS passive core cooling by closing the main steam isolation valves (MSIVs) and the feedwater isolation valves (FWIVs).
- limiting the loss of primary coolant following a pipe break outside containment.
- ensuring ECCS passive core cooling by retaining primary coolant inside the CNV, which facilitates the transfer of heat from the fuel to the reactor pool.
- limiting the transfer of mass and energy from the primary side to the secondary side following an SGTF.

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 19.1-6 describes the success criteria associated with the top events of the event trees.

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 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. An up branch indicates success of a function on the event tree 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 provides the results, or "end state," of the Level 1 evaluation. The representative thermal-hydraulic case is identified in the "comments" for each accident sequence; thermal-hydraulic evaluation is discussed in Section 19.2. Potential Level 1 event tree end states are:

- Success - 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.
- Core damage - 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.
- Transfer - Sequences that progress to the point that module response is the same as modeled by another initiating event may result in transfer to another event tree for remaining evaluation (e.g., TGS---TRAN--NPC).

A brief summary of each event tree follows.

CVCS--BREAK-IOC: CVCS Injection Line Pipe Break Outside Containment

The CVCS--BREAK-IOC 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 in the CVCS piping in the injection line or the pressurizer (PZR) spray line. The distinguishing characteristic of this initiator is that CVCS makeup cannot be credited to provide RCS inventory because of the break location.

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, actuation of the DHRS, and operator confirmation of shutdown margin with bypass of the 8-hour ECCS timer. As a result, 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 the DHRS are unavailable, then heat-up of primary coolant and pressurization of the RPV occurs to the point of RSV demand. If one RSV successfully opens, the RCS depressurizes and the ECCS is demanded. Successful ECCS actuation removes heat through containment into the reactor pool by passive convection and conduction to cool the module to a safe, stable configuration (Sequence 4). If RSV fails to open, ECCS functioning remains a success path.

For sequences where isolation of the injection line break fails, core damage is avoided if all ECCS valves and a single train of DHRS functions. Core damage is also avoided if a single reactor vent valve (RVV), a single reactor recirculation valve (RRV), and CFDS function.

The event tree consists of 19 accident sequences. Fourteen 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. Successful response to an ATWS requires isolation of the CVCS line break followed by successful ECCS valve functioning (Sequences 15 and 17).

CVCS--BREAK-DOC: CVCS Discharge Line Pipe Break Outside Containment

The CVCS--BREAK-DOC 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--BREAK-DOC initiator is similar to that described for a CVCS--BREAK-IOC except that the CVCS discharge line is where the break occurs.

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, actuation of the DHRS, and operator confirmation of shutdown margin with bypass of the 8-hour ECCS timer. As a result, 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 the DHRS, reactor safety valve, ECCS, and CFDS functions.

The event tree consists of 19 accident sequences. Fourteen sequences involve successful actuation of the RTS. The remaining sequences involve failure of the RTS and depict the module response to an ATWS. Successful response to an ATWS requires isolation of the CVCS line break followed by successful ECCS valve functioning (Sequences 15 and 17). 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 CFDS does not guarantee success.

CVCS--ALOCA-IIC: CVCS Injection Line LOCA Inside Containment

The CVCS-ALOCA-IIC event tree, provided in Figure 19.1-4, illustrates the accident sequence logic for an IE that is a pipe break in the RCS injection line or pressurizer spray line (between the CIV and the line's penetration into the RPV) or a break in the ECCS reset line. 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. Discharge of reactor coolant into the CNV would continue because the flow cannot be isolated. As a result, the RPV pressure and water level decrease and equalize pressure between the RPV and the CNV, nullifying the reactor recirculation valve IAB. The low riser level signals an ECCS actuation. 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 top event CVCS-T04 models potential compensatory measures carried out by operators to inject makeup water to the RPV. The operator action requires re-opening CIVs, aligning a flowpath from BAS, activating a makeup pump, and aligning the CVCS to provide cooling through either the injection line or pressurizer spray line, as appropriate. An unsuccessful CVCS injection leads to core uncovery and evaluation in the Level 2 analysis (Sequence 3).

The event tree consists of six accident sequences. Four sequences involve successful actuation of the RTS. In the event of an ATWS, successful ECCS operation would prevent core damage (Sequence 5).

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 a pipe break in the RCS discharge line or the RPV high point degasification line (between the CIV and the line's penetration into the RPV), spurious opening of an RSV, or a failure in the pressurizer heater penetration. In this situation, primary coolant inventory inside the RPV discharges into the sub-atmospheric CNV through the break.

The accident progression and expected module response is similar to initiating event CVCS-ALOCA-IIC. The 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 BAS 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 or reactor vent valve (RVV). Opening of either an RRV or RVV results in discharge of RCS fluid into the CNV. This event is 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 RCS---ALOCA-IC 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 (SG) 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 pressurizer level. Containment isolation would close the MSIVs and the FWIVs on both steam generators. The low pressurizer level or high main steam pressure actuates the DHRS. With the reactor tripped, the affected steam generator (indicated as #2 in the event tree) isolated, and a single train of the DHRS (indicated as #1) 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. If one RSV successfully opens, the RCS depressurizes and the ECCS is demanded because of low riser level resulting in a safe, stable configuration (Sequence 5).

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 (Sequence 3). This operator action requires re-opening CIVs, aligning a flow path from the BAS and activating a makeup pump. Given DHRS failure, if both RSVs fail to open, ECCS functioning remains a success path.

If the SGTF were not isolated (Sequences 10 through 12), there is a loss of coolant path and the need for makeup water. Makeup water can be provided by successful ECCS actuation due to low riser level or by operator initiation of the CVCS for injection.

The event tree consists of 19 accident sequences. Twelve sequences involve successful actuation of the RTS. The remaining sequences depict the module response to an ATWS. For ATWS scenarios with the faulted SG isolated the core is maintained in a safe configuration by successful ECCS function (Sequences 13 and 16) or with the CVCS providing inventory addition (Sequence 14). If the faulted SG is not isolated, the CVCS is required to replace lost inventory (Sequence 18).

TGS---FMSLB-UD: Secondary Side Line Break

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 or spurious relief valve opening in feedwater, main steam, or decay heat removal systems. In response to a secondary line break, only one train of the DHRS is available; so DHRS train 1 is considered for mitigation.

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 breaks outside containment, a reactor trip signal is expected on low steam 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). It is possible that the event causes primary pressure to increase to the point of reaching the RSV setpoint. If an RSV is demanded to open following success of DHRS, cycling of the RSV leads to a safe, stable configuration (Sequence 5). If an RSV sticks open, the ECCS functioning prevents core damage (Sequence 9). If the ECCS is unavailable, operator action to add RCS inventory using the CVCS prevents core damage (Sequences 7, 10).

If both trains of the DHRS are unavailable, heat-up of primary coolant and pressurization of the RPV would occur to the point of RSV demand. If one RSV successfully opens, the RCS depressurizes and the ECCS is demanded on low riser level to place the module in a safe, stable configuration (Sequence 12). 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 (Sequence 13).

The event tree consists of 21 accident sequences. Sixteen sequences involve successful actuation of the RTS. Successful response to an ATWS is achieved by either ECCS success (Sequences 17 and 20) or inventory addition using the CVCS (Sequence 18).

EHVS--LOOP: Loss of Offsite Power

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, which causes a disruption in the electrical supply to alternating current (AC) powered loads and a loss of the high voltage AC electrical distribution system (EHVS). Station-wide and module-specific loads such as the feedwater pumps, condensate pumps, and CVCS makeup pumps powered by the low voltage AC electrical distribution system (ELVS) would also be lost. On a loss of AC power, the MPS de-energizes non-ECCS loads, including the RTS, resulting in a reactor trip. 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 a backup diesel generator (BDG). Starting and loading a BDG requires operator action. If AC power is restored, the module response is as a transient; thus, the sequence transfers to the TGS-TRAN-NPC event tree provided as Figure 19.1-11 (Sequence 1).

The remaining sequences 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. Section 19.4 addresses loss of AC as defined by 10 CFR 50.155.) 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 the 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, stable configuration without an ECCS demand, given operator action to bypass the 8-hour ECCS timer (Sequence 2). If AC power is not restored within 24 hours, the ECCS automatically opens to the fail-safe condition and the module is maintained in a safe configuration (Sequence 3).

If the event causes the primary pressure to increase to the point of reaching the RSV setpoint, DHRS operation with an RSV cycle (open and closed) controls RPV pressure and, if power is restored within 24 hours, the module is maintained in a safe configuration without further mitigation necessary (Sequence 10). 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 and RCS pressure to the point of triggering a demand for ECCS actuation. Successful ECCS actuation prevents core damage (Sequence 18).

If both trains of the DHRS fail, heat-up of the primary coolant and pressurization of the RPV continues to the point of RSV demand. If one RSV successfully opens, the RCS depressurizes and the ECCS is demanded. Successful ECCS actuation prevents core damage (Sequence 20). Given DHRS failure, if both RSVs fail to open, ECCS functioning remains a success path.

The event tree consists of 27 accident sequences with Sequences 24 through 27 depicting module response to an ATWS. An ATWS is successfully mitigated with ECCS functioning (Sequences 24 and 26).

EDAS--LODC-----ET: Loss of Direct Current Power

The EDAS--LODC event tree, provided as Figure 19.1-10, illustrates the accident sequence logic for an initiating event that involves the loss of direct current (DC) power. The loss of DC power initiating event involves the coincident de-energization of at least two EDAS buses. At least two of the four EDAS buses are required to fail simultaneously in order for the reactor trip signal and engineered safety features to be actuated.

The expected module response to the loss of DC voltage to two or more EDAS buses has the same effect as two safety function modules indicating a trip condition (i.e., a reactor trip signal, containment isolation signal and ECCS actuation signal) because of 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 loss of DC power signals an ECCS actuation. The RVVs open quickly; however, the RRVs open when the differential pressure between the RPV and the CNV is reduced to the IAB release 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.

If both trains of the DHRS fail, heat-up of the primary coolant and pressurization of the RPV continues to the point of RSV demand. If one RSV opens followed by complete ECCS functioning, core damage is prevented (Sequence 4). If ECCS functioning is not successful, operator action to add inventory to the RCS using the CVCS prevents core damage

(Sequence 5). If an RSV fails to open, ECCS functioning remains a successful path to prevent core damage (Sequence 7).

The event tree consists of 12 accident sequences, four of which depict the module response to an ATWS. The expected module response to an ATWS is heat transfer to the reactor pool by successful operation of the ECCS.

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 condenser heat sink, loss of cooling water systems, and a manual trip.

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, DHRS actuation, and bypass of the ECCS-hour timer, which places the module in a safe configuration (Sequence 1). If the 8-hour ECCS timer is not bypassed, either ECCS valve opening or CVCS injection also results in a safe module configuration (Sequences 2, 3, respectively). If an RSV is demanded, the module is placed in a safe configuration with an RSV cycle (open and closed) (Sequence 5). If the ECCS 8-hour timer is not bypassed ECCS actuation (Sequence 6) or CVCS injection (Sequence 7) maintains the module in a safe configuration.

If both trains of the DHRS fail, heat-up of the primary coolant and pressurization of the RPV continues to the point of RSV demand. If one RSV successfully opens, the RCS depressurizes and the ECCS is demanded. Successful ECCS actuation removes heat through containment into the reactor pool by passive convection and conduction to cool the module to a safe, stable configuration (Sequence 12). Failure of ECCS valves to open as designed could be compensated by operator action to inject makeup water to the RPV from the CVCS (Sequence 13). If both RSVs fail to open, ECCS functioning remains a success path (Sequence 15).

The event tree consists of 21 accident sequences, five of which depict the module response to an ATWS. The module remains in a safe configuration after an ATWS with successful ECCS actuation (Sequences 17 and 20) or RCS inventory addition using the CVCS (Sequence 18).

TGS---TRAN--SS: Loss of Support Systems

The TGS---TRAN--SS event tree, provided as Figure 19.1-12, illustrates the response to an initiating event that involves loss of support systems, which results in unavailability of the CVCS and CFDS for inventory addition. This initiating event includes the loss of AC power buses that result in a reactor trip. This initiator is assumed to result in a reactor trip (i.e., load share across AC buses or 100 percent turbine bypass is not credited).

The expected module response to a loss of support system is to align alternate power to the ELVS motor control centers. If power is restored, the sequence transfers to the TGS-TRAN-NPC event tree provided as Figure 19.1-11 (Sequence 1). Sequence 2 represents the situation that power is not restored within 24 hours. In that sequence, a reactor trip is expected on low AC voltage or high steam pressure followed by DHRS then ECCS actuation after 24 hours.

If both trains of the DHRS fail, heat-up of the primary coolant and pressurization of the RPV continues to the point of RSV demand. If one RSV successfully opens, the RCS depressurizes and the ECCS is demanded. Successful ECCS actuation removes heat through containment into the reactor pool by passive convection and conduction to cool the module to a safe, stable configuration (Sequence 4). If both RSVs fail to open, ECCS functioning remains a success path (Sequence 6).

The event tree consists of 11 accident sequences. Seven sequences involve successful actuation of the RTS. An ATWS may be mitigated with successful ECCS function (Sequences 8 and 10).

19.1.4.1.1.5 Data Sources and Analysis

This section provides the sources of numerical data in the Level 1 PRA. The discussion includes initiating event frequencies, component failure rates, equipment unavailabilities, human error probabilities, and common-cause failure (CCF) parameters.

Initiating Event Frequencies

Each of the IE categories in Table 19.1-7 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. The NuScale design 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 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 19.1-7 provides the mean frequency and error factor for each initiator. The following summarizes the method for assessing frequencies for each initiator.

As indicated in Table 19.1-7, the "Pipe Breaks and 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 capability to maintain core cooling by the passive ECCS is the same for all break sizes and inadvertent valve opening.

For piping breaks, 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-service water piping found in INL/EXT-21-65055. The occurrence failure rates in INL/EXT-21-65055 are converted to occurrences per module critical year by consideration of approximate line lengths and the number of hours in a year. The failure rate for the spurious operation of an RCS code safety valve is taken from INL/EXT-21-65055; there are two RSVs on a module RPV. The failure probability of an induced LOCA resulting from the pressurizer heaters failing to deenergize is calculated from INL/EXT-21-65055. Spurious opening of an ECCS valve is quantified using a fault tree model of potential failure mechanisms. The uncertainty associated with each IE frequency is assumed to be a lognormal distribution and assigned an error factor of 10.

- IE-CVCS--BREAK-IOC: This initiator consists of either an RCS injection line break or a pressurizer spray supply line break outside of containment. The distinguishing characteristic of this initiator is that makeup cannot be credited because the break would act as a flow diversion for CVCS makeup.
- IE-CVCS--BREAK-DOC: This initiator consists of RCS discharge line breaks outside of containment.
- IE-CVCS--ALOCA-IIC: This initiator consists of a break in the RCS injection line or pressurizer spray line inside containment or in a supply line to an ECCS reset valve. Breaks in these lines cannot be isolated because backflow from the RPV out the break into containment would persist even after closure of the CIVs.
- IE-RCS---ALOCA-IC: This initiator consists of a break in the RCS discharge line inside containment or in the RPV high point degasification line inside containment, the spurious operation of a reactor safety valve, or a pressurizer heater induced LOCA. Similar to the CVCS injection line LOCA inside containment, breaks in these locations cannot be isolated. The potential for an RPV rupture is included in the IE and is judged to be a negligible contributor.

- IE-ECCS--ALOCA-RV1: This initiator represents an inadvertent opening of an ECCS valve when the NPM is operating. The spurious opening of an RVV or an RRV is a breach of the reactor coolant pressure boundary resulting in RCS discharge into the CNV.

The “Steam Generator Tube Failure” category in Table 19.1-7 presents the potential challenge that reactor coolant is lost outside the CNV unless secondary system lines are isolated.

- IE-MSS---ALOCA-SG: This initiator is failure of a single steam generator tube; multiple tube failures are judged not be credible because of design characteristics. In the design, secondary coolant flows through the steam generator tubes. Therefore, the higher pressure is external to the tubes placing them in compression rather than in tension, as in a conventional PWR. In addition to this operational environment difference, the design is helical as opposed to the typical U-shaped or once-through steam generator tube design. Design differences of the heilical coil steam generator were taken into consideration to estimate potential failures by an independent study commissioned by NuScale. The IE frequency is based on that study, which employs a probabilistic physics of failure method because of lack of operating data for the helical steam generator design.

The “Secondary Line Break Category” category in Table 19.1-7 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 pipe breaks in the main steam, feedwater, or DHRS lines. NuScale commissioned an independent study to estimate the frequency for a secondary side line break. The study considered unique characteristics of the design and applicable relevant industry experience with feedwater and steam piping to develop failure the initiating event frequency.

As indicated in Table 19.1-7, 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 DC buses is included as an initiator, "Loss of DC Power."

- IE-EHVS--LOOP---: This initiator represents a loss of AC power to the station. The calculation of the IE frequency is based on generic data from 2006 through 2020 as reported in INL/EXT-21-65055. 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 data are assumed to fit a lognormal distribution.
- IE-EDAS--LODC---: This initiator represents a de-energization of at least two DC buses. A loss of two of four buses initiates a signal for

reactor shutdown and containment isolation. The IE frequency is based on generic data for loss of a DC bus, spurious operation of a DC circuit breaker, and generic common cause alpha factors for rate based failures as reported in INL/EXT-21-62940 (Reference 19.1-26).

As indicated in Table 19.1-7, 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. The source of data is a collection of event types taken from INL/EXT-21-65055.The event types postulated to contribute to a loss of component cooling water, loss of feedwater, loss of condenser heat sink, loss of service water, loss of instrument air, and general transients at PWRs are included.
- IE-TGS---TRAN-SS: This initiator represents the loss of support systems such as a partial loss of AC power thereby leading to the unavailability of the CVCS. The calculation of the IE frequency is based on generic data for loss of an AC bus as reported in INL/EXT-21-65055.

Component Failure Rates and Equipment Unavailability

Basic events in the PRA are based on generic failure probabilities, modified generic failure probabilities or 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 because of random causes, related or CCF, or unavailability due to testing and maintenance activities. The generic data source is INL/EXT-21-65055. Component boundaries are consistent with NUREG/CR-6928. When the generic data are collected from components that have similar component boundaries and applications as the NuScale plant-specific design, the generic failure data, including uncertainty distributions, can be used directly; otherwise, the generic data may be modified, or a separate special analysis performed, in order to characterize the failure probability.

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-based failure probabilities such as fail to start. Gamma distributions were used for rate-based events such as fail to run.

Table 19.1-8 identifies failure rates that were developed by modifying generic data to better represent the design.

Table 19.1-9 identifies failure rates for basic events that do not have generic data directly applicable to the design. These basic events may include component level, system level, and phenomenology dependent events. The table indicates the mean failure rate and associated error factor.

Thermal-Hydraulic Uncertainty

Because 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 is evaluated based upon methods outlined in EPRI 1016747 (Reference 19.1-8) and IAEA TECHDOC-1752 (Reference 19.1-9). 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. Thermal hydraulic uncertainty 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 is evaluated for the DHRS and the 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, core damage as defined in Section 19.1.4.1.1.3 is used as the metric; for the DHRS, the metric of exceeding RPV failure pressure with no other mitigating systems available is used.

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 19.1-10 for the ECCS and Table 19.1-11 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 19.1-9 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 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 (1987) to estimate pre-initiator operator actions using the Accident Sequence Evaluation Program Human Reliability Analysis Procedure methodology and primarily NUREG/CR-6883 (2005) to estimate the post-initiator operator actions using the Standardized Plant Analysis Risk-Human Reliability Analysis (SPAR-H) 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 Accident Sequence Evaluation Program Human Reliability Analysis Procedure 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 considered in the pre-initiator analysis 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 19.1-12 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 NUREG/CR-4772, 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 before 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. Tasks associated with an action include manually initiating a system, aligning and actuating a system for injection, recovering a failed automatic actuation, 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 19.1-13 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 NPM response after a potential initiating event; thus, the context is also identified.

The HEPs provided in Table 19.1-13 reflect 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.

Although individual calculations were performed for each post-initiator operator action, a generic HFE basic event quantification approach is used by setting the first mitigation HFE in a sequence to the bounding calculated post-initiator HEP, then considering dependencies. 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. Because the ECCS timer bypass action is performed following every reactor trip, following success of both the RTS and DHRS, and not in response to an equipment failure, it is quantified at its assessed valve in Table 19.1-13. For the case of a second HFE in a cutset with the ECCS timer bypass action, the dependency is assumed to have moderate dependence, and additional HFEs in a cutset are set to complete dependence. The HEP values, including dependency, consider implementation of a joint lower bound of 1.0E-05 for cutsets containing more than one HEP.

Recovery actions are actions taken in addition to those actions initially identified by the HRA. The actions are typically included to allow credit for operators to take control room actions to recover from equipment failures. Four actions identified in Table 19.1-13 are recovery actions, BPSS--HFE-0001C-FTS-N, CNTS--HFE-0001C-FTC-N, ECCS--HFE-0001C-FTO-N, and ELVS--HFE-0001C-FTC-N. These actions involve operator actions to re-align AC power or initiate safety systems in cases where the MPS or the ESFAS actuation fails.

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. For example, unisolating the CFDS during a LOCA inside containment to adversely affect potential consequences is not judged credible because in unisolating CFDS, the operator would also initiate injection to mitigate the situation. Thus, errors of commission are not modeled. Deliberate and malicious acts such as sabotage are also not modeled.

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. 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.

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. The source for generic data supporting the test and maintenance unavailability values is INL/EXT-21-65055.

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 because of 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 shared root cause. This shared root cause 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.

Common cause failure is modeled using the "Alpha Factor" approach (α-factor model) described in NUREG/CR-5485 (1998) 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.
- has a simpler statistical model compared to other parametric models that have the above two properties, and produces more accurate point estimates and uncertainty distributions.

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 conservatism in the failure probabilities. If multiple components are failed because of 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. The alpha factors used for CCF modeling are based INL/EXT-21-62940 (Reference 19.1-26).

19.1.4.1.1.6 Software

The PRA was created using 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 (June 2011). 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.

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 provided in Chapter 15. The PRA model modifications provide for best estimate analysis of module upset, beyond-design-basis transient analysis, evaluation of ATWS scenarios, and benchmarking the thermal hydraulics of the severe accident code, MELCOR. Thermal-hydraulic modeling performed with the MELCOR code simulates the progression of a severe accident. Starting from a nominal operating condition, the module state is advanced into severe accident space where phenomena such as cladding oxidation, core degradation, core relocation, and radionuclide release are evaluated.

The NRELAP5 code is used for modeling the transient system performance before core degradation. As such, the approach for 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 regard to severe accident phenomenology relies on the MELCOR code assessment to test data (Reference 19.1-14) and best practice recommendations for severe accident modeling from MELCOR code development staff and from published unique reactor consequence analyses using MELCOR (NUREG/CR-7008 (2014) and Reference 19.1-15). 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 primary areas of analysis. The first involves quantification of sequences that could lead to core damage; this analysis is the Level 1 PRA. The second involves quantification of the containment response to core damage sequences that could lead to a release of radionuclides to the environment; this analysis is the Level 2 PRA.

Both the Level 1 and Level 2 are combined into a single PRA project and quantified using the “fault-tree linking” approach. Under this approach, a set of event trees was developed for each general type of plant upset that could initiate an accident sequence (e.g., loss of coolant accident, transient). The event trees allow the systems and actions needed to keep the core cooled to be organized in a way that defines accident sequences that lead to core damage and large release. The potential for failure of each system or action is defined through the construction of a fault tree. The fault trees carry the modeling from the functional level down to the basic hardware and human failures that can contribute to a core damage or large release sequence. Using reliability data assembled from industry experience, the integrated model can be evaluated to yield estimates of the frequency of core damage and large release. Both probabilistic and deterministic analysis techniques are used to predict the containment response and magnitude of a potential radionuclide release as discussed in Section 19.2.

An appropriate truncation level ensures that dependencies and significant accident sequences are not eliminated from the evaluation. Rather than determining a truncation level by iteratively evaluating risk at decreasing truncation levels, a constant truncation level of 1E-15 per year is used for CDF and LRF, and is applied to all hazard analyses (e.g., internal events, external floods, low power and shutdown). This level is conservative for total plant risk, and a single truncation level ensures that risk insights are consistent across different hazards and operating modes.

Unless stated otherwise, results are point estimates from quantification of the PRA logic model. Because true mean values can be produced only by first generating a probability distribution, it is not practical to comprehensively perform an uncertainty analysis on all intermediate results. Because the basic event point estimate values used in the quantification are mean values, the point estimate results 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. While the propagation of mean values in a point estimate quantification should theoretically result in the final result being a mean value, because of approximations used in the quantification and different probability distributions assumed for the basic events, in practice there are 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 (Rev 1, 2017), two general types of uncertainty should be considered in risk informed decision making. Epistemic uncertainty is associated with the lack of knowledge about an event, system, phenomena, or model. Aleatory, or random, uncertainty is based on the randomness of the nature of the events or phenomena. In the PRA model, epistemic uncertainty is addressed by performing sensitivity studies during model quantification to determine the impact of assumptions related to the lack of knowledge. Aleatory uncertainty is addressed by developing an uncertainty distribution for each basic event and performing random sampling during quantification to determine upper and lower bounds on the risk metrics.

Because the scope of PRA is that of Standard Design 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 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-NP-A (Reference 19.1-7), "significance" for the NuScale Power Plant US460 standard design is 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 19.1-7 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 illustrated 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 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). As shown in the Table 19.1-19, threshold values are derived based on the calculated CDF and LRF. For a calculated CDF contribution below 1E-10 per mcyr and LRF contribution below 1E-11 per mcyr a component is not considered risk significant.

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 are 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. The CDF is several orders of magnitude less than the safety goal and is not dominated by a specific initiating event; instead, several initiators contribute to risk, including a variety of transients and LOCAs. The very small risk metrics result from the multiple passive system and component failures necessary to reach core damage.

Table 19.1-16 provides the contribution of each initiator to the CDF. Table 19.1-17 provides the dominant core damage sequences. Table 19.1-18 provides CDF cutsets that contribute individually more than one percent to CDF. Table 19.1-60 provides the CDF associated with internal events at full power for a single NPM.

The Level 1 PRA evaluation of CDF provides insights into the risk significance of SSC and operator actions that meet the risk significance threshold using the methodology described in Section 19.1.4.1.1.9. Table 19.1-20 provides the results of that evaluation. Table 19.1-21 summarizes the key assumptions associated with the Level 1, full-power internal events PRA.

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 19.1-14 summarizes important generic sources of model uncertainty, how those uncertainties are addressed, and their effects on the model. Table 19.1-15 summarizes key design specific sources of model uncertainty, how those uncertainties are addressed, and their effects on the model. Evaluating the effect of some uncertainties on PRA results required sensitivity studies.

To provide additional insights on the CDF and component importance measures, sensitivity studies are performed. Table 19.1-22 summarizes such studies, the basis for the study, and the effect on the CDF. The table includes sensitivity studies recommended by Reference 19.1-6 for generic uncertainties associated with human error probabilities and CCF as well as design-specific uncertainties. Section 19.1.9.3 provides a sensitivity study that credits only safety-related SSC to support the regulatory treatment of nonsafety systems (RTNSS) program.

Table 19.1-23 summarizes key insights from the Level 1 PRA. While derived considering internal initiating events, the insights are generally applicable to internal floods, internal fires, and external events. Key aspects of the module response are dependent on only physical conditions and are not dependent on whether an 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. Key systems are protected from external events through the design of the systems themselves as well as protection provided by the RXB.

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.

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 an NPM are such that multiple plant damage states need not be defined to support the PRA evaluation of a large release. As a result, a Level-2 event tree is a direct transfer from a Level 1 event tree sequence that has been evaluated to result in core damage. The Level 2 event tree models the progression of a severe accident from core damage to the point of a potential radionuclide release from containment. The Level 2 event tree is also referred to as the containment event tree (CET).

19.1.4.2.1.2 Containment Event Tree

Each core damage accident sequence that is not a success is directly linked to a CET by the transfer event “LEVEL2-ET” and propagated through the CET to an endpoint that depicts the containment release state as illustrated in Figure 19.1-13. The top event “CD-T01” provides a branch to quantify all Level 1 sequences with core damage end states. The CET terminates with one of three end states for each sequence. 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 that is associated with containment failure. Because of the small core used in the design, additional release categories to reflect a range of release possibilities is judged to be unnecessary.

Potential severe accident phenomena that could challenge containment are evaluated to determine their applicability to the NuScale design and need for consideration in a CET. The evaluation considers phenomena listed in Section 19.0 of the Standard Review Plan, the ASME/ANS PRA Standard (Reference 19.1-1), NUREG/CR-2300 (1983) and NUREG/CR-6595 (2004). The characteristics of the NuScale design provide an inherent degree of safety. As a result, severe accident phenomena that may challenge containment in typical current generation 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, as indicated by top event CNTS-T01. As a result, 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 19.1-13.

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. Because of 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.

19.1.4.2.1.3 Success Criteria

The Level 2 PRA is bounding in that it does not credit mitigating systems or physical characteristics that are relevant to mitigating a radionuclide release (e.g., deposition on RXB surfaces) or recovery of the containment boundary if it is failed. Thus, the only mitigating function that is modeled in the CET is containment isolation, as illustrated by top event "CNTS-T01" in Figure 19.1-13. Top event CNTS-T01 depicts containment isolation failure, and resulting bypass, associated with fault tree modeling for

- containment evacuation system (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. The CNTS pressure boundary is formed by the CNV and passive and active barriers. Passive containment isolation barriers include the flange connections, ECCS pilot valve bodies, and piping outside of the CNV. Passive containment isolation barriers provided from supporting systems are the closed steam generator system (SGS) loops inside containment and the closed DHRS loops outside of containment. The active isolation boundaries are the CIVs, which close to provide a leak-tight barrier between the CNV and the environment. The CIVs are located on the respective system lines that penetrate the CNV head. From the PRA perspective, penetrations are evaluated as (1) piping connections, (2) bolted flange inspection ports, including electrical penetration assemblies, or (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 electrical penetration assembly boundary is at the face of the CNV flange surface for the penetration opening and includes the bolting (studs and nuts). The electrical penetration assemblies are designed to the same pressure and temperature requirements as the CNV.

The RVV and RRV emergency core cooling system valve trip and reset pilot assembly penetrations are welded to and part of the CNV; each pilot valve has a double seal to provide a leak-tight barrier.

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 pressurizer level is credited for initiating a containment isolation signal.

Because the CNV is maintained at a vacuum, normally closed or sealed containment penetrations are not considered as contributors to containment isolation failure because they can be detected during normal operation and addressed. Similarly, random failures during the mission time are judged to be extremely unlikely, and screened.

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

19.1.4.2.1.4 Release Categories

The end states of the CET provided in Figure 19.1-13 are associated with potential radionuclide releases to the environment. The CET end states “NR” and “LR” are differentiated by their contribution to the LRF.

The LRF is the quantified result of the Level 2 PRA and is used to demonstrate conformance with the NRC policy statement safety goal (Reference 19.1-17). The large release definition is based on a threshold radionuclide dose that could result in early injuries. Specifically, NUREG-0396 (1978) specifies 200 rem acute whole body dose (red marrow) as the dose at which significant early injuries start to occur. This dose is used as the basis for defining a “large release” to a hypothetical individual located at the site boundary.

Based on simulation results using the MACCS code (NUREG/CR-6613, 1998), the iodine core inventory release fraction that results in an acute 200 rem whole body (red marrow) mean dose at the site boundary is calculated. Three types of potential radionuclide release to the environment are evaluated: a core damage sequence with containment and reactor pool bypassed, a core damage sequence with leakage of radionuclides through the CNV and reactor pool bypassed, and a release occurring at the bottom of the reactor pool. Key points of the calculation are:

- The site boundary is modeled as the minimum distance from the edge of the RXB to the site owner controlled fence, which is assumed to be 690 ft (0.131 miles).
- Dose receptors are stationary and unsheltered.
- The release is at ground level.
- The dose exposure duration is 96 hours following the radionuclide plume reaching a dose receptor.
- A two-hour release duration is assumed for containment bypass scenarios.
- For sequences involving an intact CNV, the release is 0.2 weight percent per day for the entire release with deposition in the CNV considered.
- For modeling a dropped module, radionuclide scrubbing by the pool is considered.
- The mean acute whole body dose over all weather trials in one year is used.
- Radionuclide deposition in the Reactor Building is not considered.

The iodine group release fraction from a single module that results in a 200 rem whole body mean dose at the site boundary is used to distinguish between Release Categories 1 and 2.

RC1: Core Damage with Successful Containment Integrity

A bounding analysis is performed to evaluate the potential source term for “RC1,” the release category associated with an intact containment as depicted by CET end state “NR.” The calculation of the whole body dose to an individual standing at the site boundary assuming leakage from a single module at the Technical Specification limit demonstrates that the maximum dose is a fraction of the dose associated with a large release.

RC2: Core Damage with Failure of Containment Integrity

This RC represents the release associated with core damage sequences that do not have successful isolation of the CNV and are not scrubbed by the UHS. These sequences have a Level 2 end state of “LR” and are associated with a "large" release. These sequences are contributors to the LRF and CCFP.

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

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. Rather than determining a truncation level by iteratively evaluating risk at decreasing truncation levels, a constant truncation level of 1E-15 per year is used for all hazard analyses (e.g., internal events, external floods, low power and shutdown). This level is conservative for total plant risk, and a single truncation level ensures that risk insights are consistent across different hazards and operating modes.

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. The LRF is several orders of magnitude less than the safety goal and is not dominated by a specific initiating event; instead, several initiators contribute to risk, including a variety of transients and LOCAs. The very small risk metrics result from the multiple passive system and component failures necessary to reach core damage.

Table 19.1-16 provides the contribution of each initiator to the LRF. Table 19.1-25 provides the dominant large release sequences. Table 19.1-26 provides LRF cutsets that contribute individually more than one percent to LRF. Table 19.1-60 provides the LRF associated with internal events at full power for a single NPM. The table also provides the CCFP, which is a composite metric of the full power, LPSD, and external hazard contributions.

The Level 2 PRA evaluation of LRF provides insights into the risk significance of SSC and operator actions that meet the risk significance threshold using the methodology described in Section 19.1.4.1.1.9. Table 19.1-20 provides the results of that evaluation. Table 19.1-21 summarizes the key assumptions associated with the Level 2, full-power internal events PRA.

Section 19.1.4.2.1.8 summarizes the types and treatment of uncertainties associated with the Level 2 PRA. Parameter uncertainty is characterized by probability distributions associated with the results. Table 19.1-27 summarizes important generic sources of model uncertainty, how those uncertainties are addressed and their effects on the model. Table 19.1-28 summarizes key design-specific sources of model uncertainty, how those uncertainties are addressed and their effects on the model. Evaluating the effect of some uncertainties on PRA results required sensitivity studies.

To provide additional insights on the LRF and component importance measures, sensitivity studies are performed. Table 19.1-22 summarizes such studies, the basis for the study, and the effect on the LRF.

Table 19.1-29 summarizes key insights from the Level 2 PRA. Severe accident challenges are evaluated using deterministic and probabilistic considerations and found not to challenge CNV integrity; Section 19.2 provides further discussion.

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 US460 standard design.

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 (Reference 19.1-2). Once the hazards are identified for consideration, the guidance in ASME/ANS RA-Sa-2009 (Reference 19.1-2) 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 19.1-30. The table provides preliminary and bounding screening criteria using the approach discussed in Part 6 of ASME/ANS RA-Sa-2009 (Reference 19.1-2).

Table 19.1-31 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 is based on assumptions regarding siting requirements. Site characteristics should be compared to those assumed in the high winds and external flood 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.

COL Item 19.1-7: An applicant that references the NuScale Power Plant US460 standard design 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 standard design.

19.1.5.1 Seismic Risk Evaluation

Evaluation of the risk due to seismic events is performed using a seismic margins assessment (SMA) to determine the plant-level high confidence of low probability of failure (HCLPF) ground motion capacity. A PRA-based SMA provides information related to the dominant contributors to seismic risk by determining plant responses from different ground motion demands, i.e., a range of reference earthquakes (REs). Because the plant lacks a reliance on electrical power, added water, or operator actions, the design is less susceptible to low capacity accident progressions (i.e., those from small ground motions) than typical operating nuclear power plants. Consequently, seismically-induced major structural failures associated with higher ground motions, which are typically a minor contributor to the seismic risk for operating plants, represent a significant risk contributor for the NuScale design. A PRA-based SMA is developed to confirm that plant responses initiated from large ground motions are accounted for.

The SMA for the NPM is performed in accordance with NRC guidance from Section 19.0 of NUREG-0800, Revision 3 and the applicable SMA guidance in Part 5 of ASME/ANS RA-Sa-2009 as endorsed by Regulatory Guide 1.200.

19.1.5.1.1 Description of the Seismic Risk Evaluation

The primary goal of an SMA is to identify the SSC that contribute to seismic risk. The SSC identification is done by evaluating SSC risk contributors and determining the plant-level HCLPF ground motion capacity. The plant-level HCLPF ground motion capacity must be 167 percent of the RE used for design, or the review level earthquake (RLE). The RE is the CSDRS with a horizontal PGA of 0.5g. Thus the plant-level HCLPF ground motion capacity requirement is 0.84g PGA (i.e., 1.67 * 0.5g). There are two main tasks associated with performing an SMA: seismic fragility analysis (structures and components), and seismic plant response analysis (accident sequence analysis and plant level response).

19.1.5.1.1.1 Seismic Analysis Methodology and Approach

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 are 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 is performed to establish a seismic equipment list (SEL) or safe shutdown equipment list (SSEL). SSC that contribute to the seismic margin are determined by applying the MIN-MAX method described in Section 19.1.5.1.2.

The HCLPF ground motion for SSC that contribute to the seismic margin is obtained by performing fragility analysis using the separation of variables method, as endorsed by Section 19.0 of NUREG-0800, Revision 3. Separation of variables, described in EPRI 103959 (Reference 19.1-23), 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., capacity, structure response, equipment response). The fragility parameters are then used to calculate the HCLPF. For SSC that don't contribute to the seismic margin, fragilities are described conservatively using the conservative deterministic failure margin method or by utilizing generic fragilities. The conservative deterministic failure margin method, described in EPRI NP-6041-SL (Reference 19.1-12) uses conservative input parameters (e.g., material strength, seismic demand) to calculate a conservative estimate of the HCLPF capacity directly. SSC with generically defined fragilities utilize conservative capacity values with a conservative application of design-specific seismic demands. In either case, a composite uncertainty is used to define the HCLPF capacity. As a result, the hybrid method, as described in EPRI NP-6041-NL, is used to define parameter estimates for randomness and modeling uncertainty specific to different types of SSC.

The controlling failure mode of the structural events and their direct consequences are shown in Table 19.1-32. For components, seismic failures are either considered functional failures or mapped to specific equivalent random failures (such as a valve failing to open on demand).

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: the NPM base support and module lug support system
- Structures directly connected to the module interface: the reactor bay walls, pool wall, and basemat
- Structures located above the module, where collapse could lead to physical damage to the module: includes the RXB crane (RBC) and the bioshield
- Structures providing support or anchorage to another SSC, where collapse could lead to physical damage to the module: the RBC support
- Structures that, if failed, impact an accident mitigation function (e.g., makeup) for an NPM: gallery area floor and ceiling slabs in the RXB.

These failures are not modeled to result in core damage and large release directly. Instead, they are modeled to initiate other accident sequence progressions (e.g., breaks outside containment)

Figure 1.2-3 provides perspective on the locations of major structures.

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 RBC design structural qualification calculation informs the identification of evaluated failure modes. All major structural elements of the RBC are included in the fragility evaluation (e.g., bridge girders, sill beams, seismic restraints). The controlling failure mode is identified as bending failure of the composite plate connecting the bridge girder and sill beam. 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 Crane Support

The RBC support is a steel frame structure anchored to the reactor building. The RBC travels on crane rails installed on the RBC support. RBC seismic restraints interface with the RBC support in the event of an earthquake, preventing vertical motion of the RBC.

The RBC support fragility includes all structure and connection interfaces and leverages the associated qualification calculation to identify relevant failure modes. The RBC support fragility is governed by failure of the weld connection between the stiffener top plate and a steel-plate composite wall. Like the RBC fragility, the bounding consequence of RBC support 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 determining the controlling failure mode of each type of major structural member, including:

- the four exterior RXB walls
- the four RXB pool walls
- the pool bay walls

- the RXB roof
- the basemat

The controlling member and failure mode is determined by calculating a conservative estimate of the HCLPF capacity for each member using the conservative deterministic failure margin method. Following this preliminary evaluation, the lowest resulting HCLPF capacity is selected for a fragility evaluation using the Separation of Variables method. The controlling member and failure mode is determined to be in-plane shear failure of the RXB roof. Given the interaction hazard presented by roof collapse on an NPM, failure is assumed to lead directly to core damage and large release.

Slab failures on the 55 ft, 70 ft, and 85 ft elevations are also evaluated for their potential to affect SSC supporting accident mitigation in the event of failure or to induce an initiating event (e.g., break outside containment). Each floor contains equipment supporting the NPM (e.g., CVCS makeup pumps, EDAS switchgear and batteries, MPS cabinets). The controlling slab member HCLPF capacity is determined conservatively using the conservative deterministic failure margin method. Randomness and modeling uncertainty parameters are then developed from the hybrid method. The slab fragility is governed by out-of-plane shear failure on the 85 ft elevation slab.

NuScale Power Module Supports

The NPM support fragility considers the structural members and connections of the base and lug supports. All failure modes evaluated in the qualification calculation are reviewed. Because there are minimal nonseismic loads associated with either support interface, the failure mode with the highest design demand-to-capacity ratio represents the governing failure mode evaluated in the fragility. The NPM support fragility is governed by failure of the base support; specifically, failure of the weld connection between the stiffener plate and a steel-plate composite wall. Given the loss of support to an NPM, failure is assumed to lead directly to core damage and large release. The designs of the NPM skirt restraint and the NPM lug restraint are discussed in Appendix 3B.

Bioshield

The bioshield fragility considers the major structural members (i.e., the horizontal slab and the vertical section) as well as the anchorages that provide support between the bioshield structures and the bay wall. The qualification calculations for the major members and the anchorages were reviewed to determine the controlling failure mode to evaluate with the separation of variables method.

The bioshield fragility is considered in two configurations for an NPM operating at full power. Nominally, a single horizontal slab and vertical section are anchored to the bay walls of an operating NPM. When an NPM is in a refueling outage, the associated horizontal slab member is removed and placed on top of the bioshield of an operating NPM. Thus, a second configuration exists for an operating NPM with two stacked horizontal slabs, in addition to the vertical section.

For an operating NPM, failure modes for each member relevant to both configurations are reviewed. For the configuration with a single horizontal slab, the controlling failure mode is shear failure of the bolts between the support plate and the bay wall uplift post. For the stacked horizontal slab configuration, each slab is anchored independently using the same design for providing seismic restraint, neither slab imparts a load on the other slab, and the controlling failure mode corresponds to shear failure of the bolts performing the same function for the stacked bioshield as the bolts that control the single slab configuration. Consequently, the fragility for the stacked configuration is the same as the single horizontal slab fragility for an operating NPM.

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 conservatively applied NuScale-specific seismic demands derived from RXB and NPM ISRS, and generic spectral acceleration capacities developed from EPRI 3002000507 (Reference 19.1-25) and NUREG/CR-2680 (1983).

The first modeling approach is used for SSC that contribute to the seismic margin, such as components located on top of or inside the NPM (e.g., containment isolation valves, ECCS valves, ECCS trip solenoid valves, reactor safety valves).

The second modeling approach is used for components located outside the NPM (e.g., diesel generators), or components that, if failed, would not directly affect safe shutdown. This approach 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. Components sharing seismically relevant characteristics are grouped based on these similarities. Seismic failures are assigned to groups and are modeled as basic events within the SMA model. For the purposes of seismic grouping, components of the same type in the same building (or general area) with the same elevation class are considered 100 percent correlated. Seismic groupings are independent of each other.

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, median capacity uncertainty, and fragility randomness.

Separation of variables fragility analysis is performed on SSC that contribute to the seismic margin and SSC for which the NuScale Power Plant US460 standard design is different from operating plants. These SSC are structures or components inside the NPM. Generic capacities and NuScale-specific response factors are 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 is 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 PGA-grounded capacity, the nominal value is divided by a conservatively applied seismic demand derived from RXB or NPM ISRS, and multiplied by the RE PGA (0.5g).

Conservative seismic demands are determined according to whether a component may be considered rigid (e.g., valves). If an SSC is rigid, indicating a high natural frequency, seismic demands are applied using a zero period acceleration. If an SSC is not rigid, the peak acceleration of the ISRS is used. For SSC located in the RXB, an enveloped floor ISRS for all locations on an elevation is used to describe the SSC seismic demand. For SSC located on or near the NPM, but do not contribute to the seismic margin (e.g., DHRS heat exchangers), broadened ISRS is used at the equipment anchorage location.

Each SSC fragility is calculated based on floor responses. Consequently, each fragility is multiplied by the PGA of the RE (0.5g) to anchor the median capacity to the seismic input defined for design (i.e., the CSDRS). Each component fragility is then determined as a function of design loads, 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.

Results of the fragility calculation for the NPM supports are shown in Table 19.1-32.

19.1.5.1.1.2 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 19.1-14. 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 0.0525g 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 19.1-14 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. 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 19.1-14 to other seismic event trees that represent plant response to breaks outside containment (Figure 19.1-15), LOCAs inside containment (Figure 19.1-16), SGTFs (Figure 19.1-17), and losses of offsite power (Figure 19.1-18). Figure 19.1-15 and Figure 19.1-17 include a transfer to a loss of DC power event tree (Figure 19.1-19) 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 and 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, breaks outside containment, SGTFs, and structural failures). In the event of a LOOP, consideration of the BDGs is given to provide backup AC electrical power to plant loads as illustrated in Figure 19.1-18. If the BDGs survive, the response to a general reactor trip is considered, as indicated by the transfer "TGS---TRAN--NPC-ET" (Figure 19.1-11). If the BDGs fail, offsite and onsite power has been lost and a station blackout exists. Because backup power is fragile relative to postulated SSC failures leading to other seismically-induced initiating events, off-site and on-site AC power sources are not considered for seismically-induced breaks outside containment, LOCAs, SGTFs, and structural failures.

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 BDGs. If 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 RSVs depressurize the RPV to the point where the IAB allows the ECCS RRVs to open.

Other seismically-induced failures include LOCAs inside containment (e.g., spurious opening of RSVs, ECCS valves), breaks outside containment (e.g., CVCS regenerative heat exchanger failure, RXB floor and ceiling slab failures, SGTFs) and (most severely) structural events. LOCAs inside containment, breaks outside containment, and SGTFs progress similarly to sequences initiated by random failures, though sources of AC power supporting equipment for accident mitigation is not available.

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 approach 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 19.1-13), 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.

19.1.5.1.1.3 Effects of Seismically Failed Structures, Systems, and Components on Surviving Structures, Systems, and Components

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 (Reference 19.1-1):

1. 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 are fail safe on loss of power, have very high seismic capacities, and are physically shielded from nonseismically qualified SSC by the seismically qualified CNV.

2. Structural failure and falling

   Falling and interaction hazards between structures or partitions and SSC housed in utility and gallery areas are negligible contributors to seismic risk. Due to the passive and fail-safe design of the NPM, SSC located in these areas are not relied on for safe shutdown, particularly at ground motion levels capable of damaging surrounding structures and SSC anchorages. Off-site and on-site sources of AC power are fragile in comparison, thus, SSC failed due to interaction hazards are unavailable at ground motion levels capable of compromising substructures and partitions.

   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 because of 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 before 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 before its bioshield being removed. In this configuration, safe shutdown is maintained by conduction from the RPV through to the CNV and reactor pool.

3. 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 the fourteen seismic event trees. Cutsets are reviewed to screen those that are not relevant to the determination of the plant-level HCLPF. Per the MIN-MAX screening cutsets are screened out if the combined probability of random failures is less than one percent. This approach 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 the seismic margin contributors, the SSC with the smallest HCLPF value provides the plant-level HCLPF. To demonstrate acceptably low seismic risk at the standard design stage, as indicated by Section 19.0 of NUREG-0800, Revision 3, the resultant plant-level HCLPF must be greater than or equal to 0.84 g, which is the plant-level HCLPF requirement of 1.67 times the SSE.

Each cutset generated from the seismic event trees is reviewed for seismic risk insights. Differing from the determination of the plant-level HCLPF, no probability-based screening is performed during the review process; all cutsets are considered for potential risk insights.

Plant Level High Confidence of Low Probability of Failure

Implementation of the screening process described above results in a plant-level HCLPF for the NuScale design of 0.92 g. 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 19.1-32 summarizes the fragility analysis for each of the structural events. 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 SMA accident sequence cutsets.

Structural events are by far the leading contributor to the seismic margin. The bounding structural event is failure of the RBC support weld connection between the stiffener top plate and the steel-plate composite wall, which is modeled to lead directly to RBC collapse, core damage, and large release.

A single SMA sequence contains all structural events and represents a significant percentage 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 method is why only the RBC support event HCLPF shows up at the sequence level.

Significant Structural Failures

Table 19.1-32 lists the structures and associated failure modes for which structural fragilities are calculated. The 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 unique passive safety features limit 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 show very low seismic failure probabilities. The fail-safe design of components that contribute to the seismic margin 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 are 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). The multiplier is applied 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 19.1-21 summarizes the key assumptions associated with the SMA.

Uncertainties

Parameters representing aleatory and epistemic uncertainty are used directly in evaluating the plant-level HCLPF. For each SSC fragility, randomness and modeling uncertainty parameters define the double lognormal fragility model describing capacity uncertainty and SSC failure probability. Each parameter is determined according to the associated fragility development methodology (e.g., separation of variables, conservative deterministic failure margin, hybrid). The determination of these uncertainty parameters for each fragility calculation sub-factor is performed in accordance with EPRI TR-103959 (Reference 19.1-23) and EPRI TR-1019200 (Reference 19.1-24).

The SMA contains uncertainty from many sources, including:

- equipment capacity and strength
- inelastic behavior

- equipment response
- structural response

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.

The plant-level HCLPF is a parameter defined by multiple layers of uncertainty (i.e., randomness and modeling uncertainty). It defines the limiting SSC driving seismic risk as a function of high confidence and low failure probability. The plant-level HCLPF is determined by the MIN-MAX method, which identifies the SSC with the most limiting HCLPF as the plant-level HCLPF. As a result, by definition, although the plant-level HCLPF is determined from a bounded analysis, it inherently includes considerations for uncertainty.

Parameter uncertainty for CCDP is characterized by setting the seismic demand to the HCLPF level and sampling each event in the SMA (fragilities and random events). Results indicate that CCDP uncertainty is consistent with uncertainty associated with the identified dominant seismic risk contributors.

Sensitivity Studies

No sensitivities are 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., 0.84 g). A structural failure sequence involving collapse of the RBC due to RBC support failure is the most important contributor to the seismic margin. 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 dominant cutsets contain structural events leading directly to core damage and large release. Other seismically-induced initiating events require multiple seismic or common-cause random failures for core damage. This seismic risk characteristic 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 NPM.

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. The internal fire PRA is developed in accordance with Part 4 of ASME/ANS RA-Sa-2009 (Reference 19.1-2), with consideration of the review clarifications provided in DC/COL-ISG-028, and the internal FPRA applies the methodology provided in NUREG/CR-6850 (September 2005); the methodology consists of multiple interrelated tasks.

Task 1: Global Boundary and Partitioning

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. Consistent with NUREG/CR-6850, this task is based on the locations of SSC that are associated with normal or emergency reactor operating or support systems as specified in the site plan. Fire "compartments" are defined to represent areas of fire damage potential and are mapped to plant fire areas that have been defined based on fire protection system design and/or operational considerations. Fire "areas" defined in the Fire Hazards Analysis, presented in Appendix 9A, are retained as fire compartments without further partitioning if that correspondence appropriately supports the Fire PRA.

Task 2: Component Selection

Components considered in the FPRA are determined by consideration of the Level 1 internal events PRA and the Post-Fire Safe Shutdown Analysis presented in Appendix 9A. Table 19.1-33 summarizes the applicability of the initiating events used in the internal events PRA to the FPRA; components associated with mitigation of these initiating events are evaluated in the fire PRA. The Post-Fire Safe Shutdown Analysis 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 (MSO). The MSO evaluation is consistent with the approach outlined in NEI 00-01, Revision 2 (Reference 19.1-18) and the applicable MSOs derived from the generic list provided in NEI 00-01, Revision 3 (Reference 19.1-19). Based on the MSO evaluation, fire-induced failures associated with MSIVs, FWIVs, CVCS, DHRS, and ECCS are included in the model.

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. 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

Fiber optic control cables are judged to be incapable of causing spurious component operation because a short circuit, such as a “hot short” as described in NEI 00-01, is not credible in a fiber optic cable. Thus, a fire that is capable of damaging a 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 fire PRA. 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 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 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.

Task 4: Qualitative Screening

Consistent with NUREG/CR-6850 (September 2005), a fire compartment is qualitatively screened from the fire model if all of the following criteria are met:

- 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. Table 19.1-33 summarizes the internal initiating events that could be induced by an internal fire. 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 a steam generator tube failure (MSS---ALOCA-SG) from consideration in the fire PRA.

The resulting initiators are 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 limiting challenge based on the following ranking:

- Fire-Induced LOCAs inside containment are the most limiting because DHRS actuation is not adequate to avoid core damage. ECCS actuation is needed but is not part of the initiating event.
- Fire-Induced ECCS demands are the next most limiting because DHRS actuation is not adequate to avoid core damage. ECCS actuation is needed and is part of the initiating event.
- Fire-induced LOOP is considered the next most limiting because DHRS cooling is potentially compromised by a partial ECCS actuation, which can occur after module specific EDAS battery depletion.
- Fire-induced LODC is considered the next most damaging event. CVCS injection has reduced reliability as one containment isolation valve from the affected division will require local operator action to restore a CVCS injection path.
- Fire-induced transients are considered the least limiting because they are mitigated by the widest array of systems, including the DHRS.

The fire compartments identified in the FHA that are not screened in Task 4 are mapped to fire-induced initiating events based on the failures that may be caused by fire damage to equipment or associated cable in the compartment. The fire-induced initiating events are then mapped to the internal events PRA initiating events. If more than one initiator could be associated with a fire, the most limiting challenge is assumed to occur.

There is a transfer event tree corresponding to each fire initiating event. Figure 19.1-20 is representative of the fire transfer trees. They have a similar structure which reflects modeling of fire growth and indicates the transfer to an internal event tree. 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 are developed using the generic frequencies provided in NUREG-2169 (2015) and NUREG-2178 (2020). In NUREG-2169, fire ignition frequencies are presented by grouping failures according to location and equipment type or "bins." 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 six-module plant and the NUREG-2169 generic frequencies. The fixed ignition frequencies for each fire compartment are developed from the generic frequencies considering the number of components and their locations. The transient ignition frequencies for each fire compartment are based on the NUREG-2169 generic frequencies. The ignition frequencies for each fire initiating event are 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 are given to potential circuit failures: material of construction of fire-affected cable and separation requirements of Regulatory Guide 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 Post-Fire Safe Shutdown Analysis, 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 involve failures that can be categorized as ungrounded DC control circuits or temperature sensitive electronics.

The probability of spurious operation of solenoid-operated valves powered by ungrounded DC power supplies is based on NUREG/CR-7150 (Vol 2, May 2014) and 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 seven minutes, a NUREG/CR-7150 value for the probability of a hot short to persist for longer than seven minutes is applied to include a long-term hot short condition. No factor is applied for hot shorts failing 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 is assumed to be 1.0.

Task 11: Detailed Fire Modeling

Fires postulated 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) is modeled with probability distributions.
- Main control room: If a control room fire results in conditions that challenge habitability or equipment controls, operators are assumed to manually trip the reactor prior to evacuating the control room. However, nonsafety-related equipment cannot be controlled outside of the control room, so makeup to the reactor is not possible in the event of an

incomplete ECCS actuation. Safety-related equipment capability is not credited because detailed fire analyses are not performed to determine a time window for success. As a result, hot shorts are assumed to cause spurious operation of ECCS valves in one division; separation requirements limit the fire effect to a single division.

- Multi-Compartment: A multi-compartment fire is a fire that originates in one fire compartment and subsequently spreads into a second compartment because of 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. Fires in an originating compartment are assumed to result in a challenge to fire compartment boundaries, such as by the formation of a hot gas layer. Credit is not taken for reducing the probability of these fires through the use of severity factors. Probabilities of non-suppression and fire barrier failure are included in the model.

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. 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. The assessment assumes that gross failure of structural steel does not occur, consistent with the assumption that structural steel forming part of or supporting fire barriers are protected to provide fire resistance equivalent to the barrier. Structural steel whose only purpose is to carry dynamic loads from a seismic event is protected if failure of the steel during a fire could cause failure of the fire barrier. Based on this assessment, the risk associated with seismic-fire interactions is judged to be small.

Task 14: Fire Risk Quantification

Quantification results are presented in Section 19.1.5.2.2.

Task 15: Uncertainty and Sensitivity Analyses

Uncertainty and sensitivity considerations are addressed in Section 19.1.5.2.2.

19.1.5.2.2 Results from the Internal Fire Risk Evaluation

The core damage frequency due to internal fires is dominated by sequences involving failures of the ECCS, including both random and fire-induced failures. The ECCS is demanded through both spurious actuation as part of the initiating event and also by being consequentially demanded due to extended low AC power to the battery charger following failure of the module-specific EMVS bus. Core damage occurs following a failure of makeup via the CVCS.

The large release frequency is dominated by a LOCA in containment that is initiated by fire-induced spurious operation of a CVCS makeup pump that causes sufficient overfilling of the reactor vessel to cause a reactor trip on high water level. The CVCS makeup pump fails when its suction valves close as a result of the reactor trip caused by the high reactor vessel water level. Random CCF of two RRV trip valves or two RVV trip valves leads to core damage since CVCS makeup is not available. With both divisions of containment isolation valves failed on the CVCS injection line, these sequences progress directly to a large release.

Table 19.1-60 provides the CDF and LRF. The CCFP is a composite metric which reflects the contribution from the internal fire hazard. Table 19.1-34 provides the dominant CDF and LRF cutsets.

Applying the methodology referenced in Section 19.1.4.1.1.9, the internal fire PRA identified the MPS, ECCS, UHS, and CNTS as candidate risk significant systems; there are no human actions identified as risk significant, as summarized in Table 19.1-20. Table 19.1-21 summarizes the key assumptions associated with the internal fire PRA.

Parameter uncertainty is characterized by probability distributions associated with the results. Section 19.1.4.1.2 identifies sources of uncertainty in the internal events model. Model uncertainties that are unique to the FPRA 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.

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. 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. 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, as indicated in Table 19.1-22.

In summary, the fire PRA results show that even using conservative and bounding assumptions, the risk from a fire is extremely low, indicative of the passive features of the design.

19.1.5.3 Internal Flooding Risk Evaluation

Consistent with ASME/ANS RA-Sa-2009 (Reference 19.1-2), 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 is performed for a single NPM.

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 which is supplemented by flood-specific modeling assumptions. The internal flooding PRA applies the five-step methodology provided in Part 3 of ASME/ANS RA-Sa-2009 (Reference 19.1-2) with consideration of the review clarifications provided in DC/COL-ISG-028. Transfer event trees for internal flooding initiating events are linked to the internal hazard event trees to evaluate the module response.

The "plant partitioning" activity evaluates the design and establishes 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 the 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 power distribution centers. If an area contains components that could cause a reactor trip, but flood protection features are required, and there is no flood source within the area that is itself protected by the flood control features, the area is removed from consideration in the PRA model. For example, 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. Flood sources are considered from within the RXB and from buildings and areas outside of the RXB (e.g., Turbine Generator Building). Mitigating equipment is located in the RXB as well as other areas (e.g., DWS skid).

Potential flooding sources may be:

- 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 that can lead to overfilling tanks, diversion of flow-through openings created to perform maintenance, or inadvertent action of fire-suppression systems.

The flooding potential associated with plant systems, characterized by their significance and potential flooding effects, are conservatively considered in the internal flooding evaluation.

Potential flooding scenarios consider propagation pathways, mitigation factors, and the affected equipment. Mitigation factors such as curbs, drains, sumps, watertight doors, and equipment mounting have not been considered with the exception of flood doors protecting certain electrical equipment in the RXB and CRB.

Flooding of areas containing equipment included in the PRA model is evaluated for the potential to damage equipment. 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 (MCCs), 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 protected; 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 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. 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.

Flood induced initiating events are determined by 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 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 the EDAS equipment is protected from flooding, and no internal flooding sources are associated with an area containing EHVS switchgear. However, an internal flood could initiate a transient because of potential effects on pumps, control panels or equipment. Thus, as summarized in Table 19.1-35, the internal event initiator "TGS---TRAN--NPC" is applicable to internal flooding.

The frequency of the internal flooding contribution to a transient initiator is assessed by comparing the design to generic data provided in NUREG/CR-2300, with consideration of similarities in the location and types of equipment in various buildings. 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 Utility 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 that could induce a plant trip are included in the TGB grouping. The potential effect on mitigating systems is determined by evaluating the effect of flooding areas containing equipment modeled in the top events of event tree TGS---TRAN--NPC. The results of the evaluation are summarized in Table 19.1-37. As indicated in the table, CVCS injection (event CVCS-T01) is failed for both the RXB and non-RXB floods.

There are no operator actions that are unique to the internal flooding PRA. Potential operator actions to limit or mitigate flooding events are not modeled.

The evaluation indicates unique event trees are not required to model the internal flooding hazard. Thus, Figure 19.1-21 and Figure 19.1-22, respectively, are used to indicate a pass-through from the internal flooding initiating events in the RXB and the other buildings to the TGS---TRAN--NPC event tree. Table 19.1-36 provides the internal flooding frequencies and associated error factors. Quantification of the internal flooding PRA is 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

The core damage frequency due to internal floods is dominated by sequences that include flooding-induced plant shutdown with successful DHRS but failure of the operators to bypass the ECCS timer, followed by incomplete ECCS actuation. The internal flood is assumed to cause loss of CVCS injection, because CVCS equipment is vulnerable to flooding in various locations in the RXB; and the DWS, upon which CVCS is dependent, could be affected by floods outside the RXB. The contributors to a large release are similar but also include failure of containment isolation. The containment isolation failures include failure of MPS actuation of ECCS and containment isolation, with failure of operator action to perform manual actuations; CCF of both containment evacuation system isolation valves to close; or CCF of both CVCS isolation valves to close.

Table 19.1-60 provides the CDF and LRF. The CCFP is a composite metric which reflects the contribution from the internal flooding hazard. Table 19.1-38 provides the dominant CDF and LRF cutsets.

Applying the methodology referenced in Section 19.1.4.1.1.9, the internal flooding PRA identified the MPS and UHS as risk-significant candidates, as summarized in Table 19.1-20. Table 19.1-21 summarizes the key assumptions associated with the internal flooding PRA.

Parameter uncertainty associated with the internal flooding PRA is characterized by probability distributions associated with the 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 frequency 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.

A sensitivity study is performed to assess the impact of the internal flooding PRA modeling assumption that a flood outside the RXB prevents operators from establishing makeup from the CVCS. Adding credit for CVCS makeup reduces the risk associated with internal flooding as indicated in Table 19.1-22.

In summary, 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 design.

19.1.5.4 External Flooding Risk Evaluation

An external flooding PRA for full power operations has been performed for a single NPM.

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 is supplemented by flood-specific failure modes. The external flooding PRA applies the methodology provided in Part 8 of ASME/ANS RA-Sa-2009 (Reference 19.1-2) with consideration of the review clarifications provided in DC/COL-ISG-028. The methodology is consistent with NEI 16-05 (Reference 19.1-20). The external flooding methodology encompasses hazard analysis, fragility evaluation and module response.

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 (Reference 19.1-2), a flood frequency of 2.0 E-3 with an error factor of 10 is assumed to estimate the likelihood of exceeding the design-basis flood 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 perform a controlled shutdown 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.

The fragility evaluation considers the susceptibility of SSC to an external flood. Flooding mitigation features in the RXB or CRB such as watertight doors, curbs, equipment mounting, drains, sumps, or operator actions to minimize the consequences of external flooding are not credited; similarly, temporary protective measures such as sand bags are not credited. 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.
- 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 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 protected; therefore flooding effects are not considered for equipment inside the CNV.

Based on building design requirements, the RXB and CRB walls are assumed to withstand the effects of external flooding. The TGB and backup diesel generator enclosures are not assumed to withstand external flooding.

Determining the module response to an external flood event involves identifying the applicable accident progression from the internal events PRA and incorporating the potential flooding effect on mitigating systems. 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 because of potential effects on pumps, control panels or equipment. An external flood could initiate a LOOP or LODC because of flooding in areas containing EDAS 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 because of a loss of power. Thus, the limiting plant response and accident progression model for an external flood is the LOOP event tree. Table 19.1-39 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 in areas containing equipment modeled in the PRA. This effect on event tree top event, is illustrated in Table 19.1-40. Based on this evaluation, a transfer event tree, Figure 19.1-23, includes a top event (EXT-FLD-LOOP) to account for the fraction of external floods for which there is insufficient warning time for the operating staff to initiate a controlled shutdown. The transfer tree links to the EHVS-LOOP tree. Table 19.1-36 provides the external flooding frequency and associated error factor.

Quantification of the external flooding PRA is 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.

19.1.5.4.2 Results from the External Flooding Risk Evaluation

The core damage frequency due to external flooding is dominated by sequences that involve an incomplete ECCS actuation. A common cause failure of both reactor vent valves transfers reactor coolant from the CNV to the reactor pressure vessel, but without recirculation results in core uncovery and eventual core damage. The contributors to a large release are similar but also include failure of containment isolation, caused by either CCF of both containment evacuation system isolation valves to close, or CCF of both CVCS isolation valves to close. Table 19.1-60 provides the CDF and LRF. The CCFP is a composite metric which reflects the contribution from the external flooding hazard. Table 19.1-41 provides the dominant CDF and LRF cutsets.

Applying the methodology referenced in Section 19.1.4.1.1.9, the external flooding PRA identified the ECCS, MPS, and UHS as candidate risk significant systems; ECCS trip valves are identified as candidate risk significant components, as summarized in Table 19.1-20. Table 19.1-21 summarizes the key assumptions associated with the external flooding PRA.

Parameter uncertainty associated with the external flooding PRA is characterized by probability distributions associated with the results. Section 19.1.4.1.2 identifies sources of uncertainty in the 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 and sensitivity studies.

Table 19.1-22 presents results of sensitivity studies which (i) modify the fraction of external floods with sufficient warning time to perform a controlled shutdown, and (ii) consider passive reactor vent valve operation.

In summary, the external flood PRA results show that equipment failures after the external flooding-induced LOOP are randomly occurring and independent of the initiator. Using conservative and bounding assumptions, the risk from external floods is extremely low, indicative of the passive nature of the design.

19.1.5.5 High-Wind Risk Evaluation

A high-wind risk assessment for full power operations is performed for a single NPM.

19.1.5.5.1 Description of High-Wind Risk Evaluation

The high-wind events considered in this evaluation are considered extreme high winds that exceed those evaluated in the internal events PRA. 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.

The high-wind PRA applies the methodology provided in Part 7 of ASME/ANS RA-Sa-2009 (Reference 19.1-2) with consideration of the review clarifications provided in DC/COL-ISG-028. The methodology consists of a hazard analysis, fragility evaluation, and plant response evaluation. The hazards analysis considers the occurrence frequency 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 event trees from the internal events PRA model are reviewed for applicability to high winds. As indicated in Table 19.1-42, only the LOOP event tree, EHVS--LOOP, is considered in the high-winds PRA because (i) systems or components whose failure would otherwise result in an initiating event are located inside protective structures like the RXB or (ii) the effects of the initiating event are bounded by the LOOP evaluation. Figure 19.1-24 and Figure 19.1-25 are the full power high-winds event trees for tornado and hurricane extreme winds, respectively. The event trees are simply a transfer to the internal events LOOP event tree.

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 standard design, a best estimate analysis for an average U.S. site is performed to assess the high-wind occurrence frequency. The high-wind initiating event frequencies are developed from the high-wind strike frequencies. For full power operation, the initiating event frequency conservatively assumes 100 percent module availability.

To assess the tornado frequency, the methodology provided in NUREG/CR-4461 (2007) 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. Table 19.1-36 provides the frequency of EF2 through EF5 tornadoes and the associated error factor.

The methodology for estimating a hurricane strike is based on U.S. LWR operating experience. Hurricane events and undefined high-wind events that resulted in a LOOP are obtained from INL/EXT-21-64151 (Reference 19.1-10). The number of events is then divided by the sum of the reactor operating years to determine the strike frequency. The hurricane initiating event for full power operations is the overall strike frequency adjusted by the availability factor. Table 19.1-36 provides the frequency of Category 3 or greater hurricanes and the associated error factor.

The high winds fragility evaluation evaluates the susceptibility of plant SSC as a function of the wind severity. Damage to equipment from extreme high winds can occur because of 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 19.1-43 summarizes building capacity to withstand high winds, which illustrates, for example, that Seismic Category I structures have only superficial damage by tornado winds categorized as EF5. Given the structural response to high winds provided in Table 19.1-43, a review of the top events in the LOOP and Level 2 event trees is performed for susceptibility to high winds.

To assess the potential for recovering power within 24 hours (to preclude a demand for the ECCS), data from INL/EXT-21-64151 (Reference 19.1-10) are reviewed; it includes data with the probabilities of exceedance versus duration for a LOOP. Based on these data a weather-related 24-hour LOOP non-recovery probability of 2.4E-01 (with an error factor of 10) is applied to tornado and hurricane events.

An operator action that is credited in the internal events PRA, but is judged not to be possible following a high-wind event is “operator loads the BDGs.” This action is judged not to be possible because the backup diesel generator enclosures are not assumed to withstand a high-wind event.

The other operator actions occur within the RXB and the CRB, which are not susceptible to high-wind damage. The human error probabilities from the internal events analysis are judged to be bounding and increased high wind-specific performance shaping factors (e.g., additional stresses) are judged not to be appropriate.

Quantification is based on the internal events SAPHIRE model with rules added to address high winds hazard (e.g., the probability of failing to recover offsite power for weather-related events) at a truncation level of 1E-15.

19.1.5.5.2 Results from the High-Wind Risk Evaluation

The core damage frequency due to high winds is dominated by sequences that involve an incomplete emergency core cooling system actuation. A common cause failure of both reactor vent valves will transfer reactor coolant from the CNV to the reactor pressure vessel, but without recirculation results in core uncovery and eventual core damage. The results for large release are similar but also include failure of containment isolation. The containment isolation failures include CCF of both containment evacuation system isolation valves to close, or CCF of both CVCS isolation valves to close.

Table 19.1-60 provides the CDF and LRF. The CCFP is a composite metric which reflects the contribution from the high wind hazard. Table 19.1-44 and Table 19.1-45 provide the dominant CDF and LRF cutsets associated with the hurricane and tornado high-wind risk evaluation, respectively.

Applying the methodology referenced in Section 19.1.4.1.1.9, the high-winds PRA identified the ECCS, MPS, and UHS as candidate risk significant systems; ECCS trip valves are identified as candidate risk significant components, as summarized in Table 19.1-20. There are no risk-significant human actions identified in the high-winds PRA. Table 19.1-21 summarizes the key assumptions associated with the high-winds PRA.

Parameter uncertainty associated with the high-winds PRA is characterized by probability distributions associated with the results. Section 19.1.4.1.2 identifies sources of uncertainty in the internal events model. Model uncertainties that are unique to the high-winds PRA include the IE 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.

Table 19.1-22 presents results of sensitivity studies that (i) increase the frequency of high winds that result in a LOOP, (ii) increase the probability of not recovering offsite power, and (iii) consider passive reactor vent valve operation. The results are presented for hurricane high winds because hurricane risk is higher; sensitivity results are comparable for tornado risk.

The results of the high-winds evaluation indicate that equipment failures after a high winds-induced LOOP are randomly occurring and independent of the initiator. Based on this assessment, the risk associated with a high-winds event is extremely low.

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.

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

An LPSD evolution is defined 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 18-month refueling cycle corresponds to a refueling frequency of 0.67 per year, and a nominal refueling outage is projected last approximately 10 days. Refueling operations are described in Section 9.1.4 and Section 9.1.5.

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 NPM arrangement, POSs are defined based on the activity being performed and availability of systems that can cause or be used to mitigate an initiating event. Each POS is described in detail below.

POS1: Shutdown and Initial Cooling: The NPM 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. To prevent brittle fracture of the RPV, low temperature overpressure protection (LTOP) is enabled when the RCS temperature is below the LTOP enable temperature; for the purposes of this analysis LTOP is assumed to be enabled for the entire duration of POS1. Containment flood begins and the main steam and feedwater systems are removed from service. The NPM exits POS1 when CNV flooding is complete.

POS2: Cooling Through Containment: The NPM enters POS2 when the CNV flood is complete. Decay heat is passively conducted through the flooded CNV to the reactor pool. The CVCS continues to operate to establish and maintain RCS chemistry until shortly before the ECCS valves are opened. Once passive cooling is established with the open ECCS valves, the CNV is isolated and the NPM disconnected from its operating bay. The RBC is connected to the NPM lift points in preparation for transport. The NPM exits POS2 when it is lifted by the RBC.

POS3: Transport: POS3 includes all NPM transport operations and occurs twice in a refueling outage: first when the NPM is transported from its operating bay to the refueling pool, and again when the NPM is transported from the refueling pool back to its operating bay. The NPM enters POS3 when the NPM is lifted by the RBC and exits POS3 when the NPM is lowered into the containment flange tool (CFT) for disassembly. The NPM enters POS3 again when it is lifted out of the CFT after reassembly, and then exits POS3 when it is lowered into its operating bay.

POS4: Disassembly, Refueling, and Reassembly: The NPM enters POS4 when the RBC lowers the NPM into the CFT. While in POS4, the NPM is disassembled in preparation for refueling, the upper vessels are moved to the dry dock, and refueling and maintenance activities are performed. After the NPM is disassembled, the core remains in the RPV lower head in the refueling pool while the upper vessels are far enough from the refueling pool that the core is not affected by an RBC failure. Reassembly also occurs in POS4, following the same process in reverse. The NPM exits POS4 after when it is lifted out of the CFT to be moved back to its operating bay.

POS5: Reconnection: The NPM enters POS5 when the RBC lowers it into its operating bay. Piping and power connections are restored, instrumentation is transferred back to its operating configuration, steam generator cleanup begins, the RVVs and RRVs are closed, and CVCS begins operating to establish RCS chemistry. The NPM exits POS5 when CNV drain begins.

POS6: Heatup: The NPM enters POS6 when CNV drain begins. 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 NPM exits POS6 when control rods are withdrawn to criticality.

POS7: Low Power Operation: The NPM enters POS7 when control rods are withdrawn and the core reaches criticality. Systems credited in the full power PRA are available, with the only difference in configuration being that the turbine is bypassed. When the turbine is synchronized with the grid the NPM exits POS7.

Table 19.1-46 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 is developed by identifying the safety functions that are required during LPSD. The LPSD safety functions are

- decay heat removal.
- RCS inventory control.
- RCS integrity.
- reactivity control.
- core orientation.
- containment integrity.

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 for LPSD are the same as the applicable systems in the full power PRA. The safety function of “core orientation” reflects the possibility of an NPM falling over during transport, which may disrupt heat removal.

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 19.1-22) is also reviewed for applicability to the design.

Initiating events are identified for each POS by considering the POS configuration and the potential to challenge a safety function. 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. 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, the module is completely disconnected and unaffected by any at-power initiating events. Coolant recirculation by the CVCS is in place for portions of POS2 and POS5 when the ECCS valves are closed; however, CVCS line break outside and inside containment are modeled for the full duration of the POS in accordance with the convention of assuming constant plant conditions in a POS.

Table 19.1-47 summarizes the full power initiating events and their applicability during LPSD.

Potential initiating events that are unique to the LPSD mode relate to low temperature overpressurization, module drop, mechanical damage during fuel movement, and alternate system alignments.

To maintain the RCS integrity safety function during cold RCS conditions, the low temperature overpressure protection (LTOP) function is enabled when the RCS temperature is below the LTOP enable temperature. Because a gas or steam bubble is maintained in the PZR, the PZR is not water-solid and a pressurization transient must first fill the PZR before the RPV would experience brittle fracture. Pressurization 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 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 RPV is challenged, the presence of automatic MPS signals and alarms, and the high reliability of the RVVs to open on demand.

The NPM transport is unique to the NuScale refueling process, as discussed in Section 9.1.

Accordingly, the initiator “IE-RBC---DROP” associated with failure of the RBC is included in the LPSD risk assessment. This initiator is applicable to POS3. Table 19.1-49 provides the frequency for IE-RBC---DROP, which is determined by multiplying the probability per refueling outage with the refueling frequency.

To develop the NPM drop probability per refueling outage, an evaluation of the RBC is performed to identify combinations of failures that could lead to a NPM drop. These “upset events” disrupt the refueling process and could result in a load drop; they are identified using three approaches. The first is an operation-based approach that identifies faults as a result of incorrect RBC operation during NPM transport; the second is a protection-based approach that identifies potential upsets based upon the protective devices required in the RBC design; and the third is a component-based approach that uses an FMEA to identify component failures that would upset the NPM transport. For each NPM drop upset event, a fault 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 NPM drop. Only a fully assembled NPM is considered in this analysis, therefore the scope of the NPM transport is between the operating bay and the containment flange tool (CFT). If the RBC were to fail after removing the lower containment vessel, pool water would enter the reactor pressure vessel through the open RVVs and RRVs to cover the core and prevent core damage.

The NPM drop upset events are identified by considering potential causes of RBC failure during all stages of NPM movement. The RBC movement is modeled as being controlled by an operator or semi-autonomously by the control system, each with a probability of 0.5, with the RBC control system providing backup safety and mitigation features at all times. Contributors to the NPM drop probability include operator error and hardware failures. Table 19.1-48 summarizes upset events with their means of detection and mitigation. Quantification of the fault trees associated with the NPM drop upset events identified in Table 19.1-48, and accounting for the time that an NPM is being moved, produces probabilities of an NPM drop for POS3 as indicated in Table 19.1-49. As indicated in the table, a module drop does not transfer to an internal event tree because mitigation is not considered when evaluating the consequences as discussed in Section 19.1.6.1.3.

Fuel assemblies remain in the pool at all times during refueling operations and as such they remain covered and cooled. An upset event that causes mechanical damage to fuel cladding, such as a fuel handling accident or a heavy load dropped onto fuel assemblies, does not elevate the cladding temperature, although fission products will be released through the damaged cladding. For completeness, the release of fission products caused by mechanical fuel damage is compared to the large release definition described in Section 19.1.4.2.1.4.

The systems analysis methodology assesses each system for potential alternate alignments and success criteria that may have changed due to the POS conditions, and fault trees are edited or replaced with new fault trees as necessary. If no changes are identified, the fault trees from the model are used without modification. The model systems analysis also identifies components that may be unavailable due to testing or maintenance, and events representing such unavailability are not altered or removed for the LPSD PRA. It is reasonable to expect that maintenance will be deferred until the equipment is taken out of service during the refueling outage. This is a conservative simplification, and is reasonable due to the small contribution of test and maintenance events to the overall risk. The refueling process does not require supplemental systems be placed into service (e.g., a residual heat removal system), and does not require alternate system alignments, therefore no additional initiating events are identified.

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 are developed to depict the NPM response to an initiating event. The changes in the NPM 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 conditions. The LPSD plant operating states exhibit lower decay heat levels than the full power PRA because of the NPM 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 NPM is subcritical.
- CFDS-T01: The containment flooding system is assumed to succeed for the POS in which the CNV is already flooded.
- 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 the 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 NPM is already shutdown, it is unlikely that the pressure increases enough to open the RSVs when DHRS is successful.

- ECCS-T01: The ECCS valves are open for POS2 and POS5
- ECCS-T03: Operators confirm shutdown margin and bypasses the 8 hour ECCS timer in POS1, POS2, POS5 and POS6 as part of the controlled shutdown procedure.

A representative LPSD transfer event tree is provided as Figure 19.1-26. The tree is used to transfer the initiating event of a spurious opening of an ECCS valve occurring in POS1 to the full power event tree ECCS--ALOCA-RV1 for evaluation of the mitigating system response. Similar transfer trees are used for each of the unscreened LPSD events indicated in Table 19.1-47.

The NPM drop scenarios are those that may lead to core damage because of 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; because of uncertainty in calculations of PCT, core damage is assumed to occur. The NPM drop scenarios in which the NPM 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. The NPM drop scenarios are defined by whether the drop results in the NPM remaining upright or tipping over. The probability of the NPM remaining upright is discussed in Section 19.1.6.1.4.

The event tree used to evaluate the end state of an RBC failure and module drop event is provided as Figure 19.1-27. The top event RBC-T01 depicts the possibility of the NPM tipping if dropped. If the NPM remains upright, cooling from natural circulation and conduction through the flooded CNV is unaffected and the NPM remains cooled. If the NPM remains upright, no core damage occurs and the sequence results in an "OK" end state. If the NPM falls over, core damage is assumed to occur, and the sequence is assigned the end state "CD-MD." 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 NPM with a damaged CNV results in a radionuclide release that is a fraction of that associated with a large release. The radionuclide release is limited because of the scrubbing effect of the reactor pool. Mechanical damage to fuel during transport operations is evaluated as an instantaneous release of 100 percent of the fission product gases in the fuel-cladding gap; the potential consequences are bounded by the results of the dropped module with core damage evaluation.

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 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 because of 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 NPM transport is designed to the single-failure proof criteria described in NUREG-0612 (1980) and NUREG-0554 (1979), thus is highly reliable. The generic data from INL/EXT-21-65055 and the Quanterion Automated Databook (Reference 19.1-21) 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. The mechanics of an NPM failing to remain upright is not modeled in detail due to the complexity and inherent unpredictability of factors such as the deformation of the CNV support skirt upon impact with the reactor pool floor. The probability of the NPM remaining upright is therefore modeled with a probability of 0.5 and uncertainty is characterized with a uniform distribution.

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 is used to be consistent with other hazard analyses.

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

The core damage frequency due to low power and shutdown is dominated by sequences in POS1 and POS6 initiated by either a loss of support systems transient or a LOOP, which contains failure of the BPSS, DHRS, and ECCS. The contributors to a large release are similar. The containment isolation failures include failure of containment isolation, with failure of operator action to perform manual actuations; or thermally induced steam generator tube failure after the onset of core damage.

Table 19.1-60 provides the CDF and LRF. The CCFP is a composite metric which reflects the contribution from LPSD operation. Table 19.1-50 provides the dominant CDF and LRF cutsets.

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 and LRF for the LPSD mode. Table 19.1-20 summarizes the candidate risk-significance SSC. There are no risk-significant human actions identified in the LPSD probabilistic risk assessment. The key assumptions are summarized in Table 19.1-21.

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

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 NPM -- There is considerable uncertainty regarding the potential damage to an NPM in the unlikely event of a drop.

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

The values of CDF and LRF reported in Table 19.1-60 are truncated at 1E-15, which is consistent with other hazard analyses. Table 19.1-22 presents results of sensitivity studies which increase the failure probability of CES. Applying the sensitivity values to the CES containment isolation valves and actuation modules does not generate new cutsets above the truncation level.

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, because of radionuclide 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.
- The POS with the longest duration, POS4, has 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 full power operation and LPSD states. A nominal refueling outage for a single NPM is provided in Table 19.1-46 and occurs every 18 months. Using this information results in a 1.8 percent probability that the NPM is in a state other than full power operation. 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 NPM is therefore approximately two orders of magnitude more likely to be at full power 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 NPM. When the RBC is not bearing the load of the NPM, stresses on crane supports and seismic restraints from earthquake loadings are less, resulting in more margin to failure. At other times during refueling, the NPM 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.

Considering the nominal outage duration outlined in Table 19.1-46, the transportation time to the refueling area, and the transportation and reconnection time after refueling, the RBC is under load for about four percent of a nominal outage duration. As such, the relative seismic risk to an NPM suspended by the RBC in a LPSD configuration is low.

Furthermore, because the RBC fragility analysis is performed considering a loaded NPM, seismic risk is overestimated for a condition when the RBC is unloaded. The specific seismic risk to the NPM 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

To assess LPSD fire risk, an evaluation of each POS during LPSD operations is performed and presented in Table 19.1-51, 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 NPM 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

To assess LPSD internal flood risk, an evaluation of each POS during LPSD operations is performed and presented in Table 19.1-52 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 NPM 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

To assess LPSD external flood risk, an evaluation of each POS during LPSD operations is performed and presented in Table 19.1-53 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 NPM 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

To assess LPSD high-wind risk, an evaluation of each POS during LPSD operations is performed and presented in Table 19.1-54 along with its susceptibility to high-wind. The analysis for the high-wind risk during LPSD concludes that because of the limited time (frequency and duration) that the NPM is in any POS during LPSD operations, as discussed in Section 19.1.6.1, and the fail-safe nature of the safety systems, high-wind contributes an insignificant amount to the risk when in LPSD modes. Thus, a CDF and LRF for external floods during LPSD are not calculated.

19.1.7 Multiple-Module Risk Evaluation

The risk associated with operation of a single NPM is discussed in Section 19.1.4 through Section 19.1.6. This section addresses the risk associated with operation of multiple NPMs. Section 19.1.7.1 describes the internal events risk evaluation of multiple NPM operation. The systematic multi-module assessment approach is illustrated in Figure 19.1-28. 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 NPM provides the basis for evaluating the risk associated with a multiple NPM plant; the intent of the multiple NPM (multi-module) PRA is to identify and quantify postulated accident sequences that lead to core damage in multiple NPMs. The MM modeling approach described in this section does not identify the specific NPM or set of NPMs involved in an accident sequence. Rather, the methodology identifies the characteristics and associated risk to two or more NPMs given an accident involving one NPM.

The MM-PRA uses the single NPM PRA accident sequence logic and makes parametric adjustments to single NPM basic events to account for MM configurations and the associated likelihood of extension to multiple NPMs. The intent is to identify the possible ways in which NPMs could be coupled from a risk perspective. The simplest coupling of multiple NPMs 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 NPM 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 that has occurred in one NPM occurs in more than one NPM. 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 NPM that does not directly affect another NPM. Rather, the occurrence of the error for one NPM increases the likelihood that such an error could occur in additional NPMs. 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 NPM. Potential mechanisms that could couple an initiating event in one NPM to multiple NPMs 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 19.1-56 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 assignment implies that for a loss of off-site power event, the effects are wide spread throughout the plant and affect all NPMs. 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 NPM, there is a one percent chance that a similar pipe break occurs in at least one additional NPM 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 NPM PRA is evaluated in terms of a multiple NPM "classification" to assign an MMAF for the multiple NPM PRA.

- Single Failure -- A single failure refers to a single structure, system, or component 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 an independent event, there is the possibility that coupling mechanisms are present that could propagate a specific failure to other NPMs. 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 NPMs given occurrence in one NPM. 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 because of a single shared cause. The MMAF for CCFs represents the extension of existing CCF events in the single PRA model for one NPM to other NPMs. An estimate of 30 percent is applied as a conditional probability of CCF extended to two or more NPMs given a CCF in one NPM using engineering judgment.
- Shared SSC (Single failure) -- Represents the potential for a failure due to a shared component affecting multiple NPMs. An example of a common system is the CFDS, which is shared among six NPMs; an example of a shared structure is the reactor pool, which is common to all NPMs. To be classified as shared SSC for the MM-PRA, the failure event must nominally affect two or more NPMs simultaneously, not necessarily all six. Basic events in representing shared equipment are assigned an MMAF of 1.0. Table 19.1-55 summarizes the effect of a system failure for each of the systems shared by multiple NPMs. Systems associated with only a single NPM and systems used for LPSD operations or security are excluded from the evaluation. The postulated failure is considered to be inoperability or unavailability of all functions of that system.
- The CCF of Shared SSC -- In the same manner as MMAFs are 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 SSC equipment or function unavailability due to the action (or inaction) of a human. An MMPSF is applied to account for the added complexity of servicing a multiple NPM plant configuration compared to a single NPM.
- Shared Human Events -- Some HFEs involve operator actions on shared systems (e.g., 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 that would affect multiple NPMs simultaneously, hence a similar response for the multiple NPM analysis. In the PRA, there is one event with a similar response characteristic: recovery of offsite power before depletion of backup battery power. The response to recover offsite power is modeled as the same for every NPM 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 NPMs, hence an MMAF of 1.0 is applied.
- Passive Safety System Reliability ECCS Events -- Basic events are included in the single NPM 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 NPM 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 NPM-specific constituent parameters, an MMAF of 1.0 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 NPMs, the test and maintenance event for that component is also a shared event with the associated MMAF.
- The SGTF events are assigned a value of 0.1. This value 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 NPMs.
- The 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 NPMs.

Table 19.1-57 summarizes the coupling characteristics, the associated MMAFs and their bases for basic events. For example, as indicated in the table, shared SSC faults affect all NPMs as indicated by an MMAF of 1.0.

19.1.7.1.3 Quantification of Multiple-Module Risk

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 NPM PRA results. Thus, the CDF for two or more NPMs is quantified using the single NPM internal events PRA and applying multi-module post processing rules to add the coupling factors to each cutset. Quantification is performed with the SAPHIRE code using a 1.0E-15 truncation level.

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

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

Another consideration not addressed 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 NPM are not likely to be closely coupled to the RVVs in another NPM, even for adjacent NPMs. 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

In the multi-module assessment, it is conservatively assumed that, if more than one NPM is affected, all NPMs in the plant are affected. Thus, when evaluating the risk from multiple NPM operation, the multi-module risk applies to a two-NPM configuration up to, and including a six-NPM configuration.

The CDF is several orders of magnitude less than the safety goal and is not dominated by a specific initiating event; instead, several initiators contribute to risk, including a variety of transients and LOCAs. The small risk metrics result from the multiple passive system and component failures necessary to reach core damage. Several initiators, including losses of offsite power, reactor coolant system LOCAs inside containment, and various transients, contribute to multi-module risk.

Table 19.1-58 provides the dominant CDF and LRF cutsets. Table 19.1-59 provides a summary of contributions to MM-CDF and MM-LRF by initiator. Table 19.1-60 provides the 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.

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

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

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

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

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

Some external events have the potential to cause damage in multiple modules because of their site-wide effect in a common time frame. The potential for a seismic event, internal fire, internal flood, external flood or high winds to cause damage to multiple NPMs is discussed below. Table 19.1-61 summarizes the potential coupling effects associated with external events on systems modeled in the PRA. The table summarizes whether an additional contribution to system unavailability is included in the PRA model due to the external event.

Earthquakes, by their nature, affect multiple NPMs simultaneously. The modeling of multi-module seismic effects is outside the scope of a margin assessment. It should be noted, however, that bounding a single NPM core damage scenario as applying to all NPMs is likely conservative for the higher likelihood, lower severity earthquakes. As ground accelerations become larger and larger, the conditional probability of inducing core damage in the first NPM, as well as multiple NPMs, approaches 1.0.

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

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

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

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

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

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

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

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

In terms of initiating an upset to steady-state operations, 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, external flooding could result in a loss of AC power and offsite power to all six NPMs.

The system insights show that the common systems susceptible to external flooding include the loss of AC power that results in a reactor trip of all six NPMs. Because of the passive nature of the safety systems, once they actuate, there is no further need for electric power or operator actions.

The impact of external flooding is basically that of a station blackout following a loss of power, which is analyzed in the full power internal events PRA. Although external flooding will impact all six NPMs, the review of mitigating systems shows that there is no indication of any coupling mechanisms that would affect the ability of multiple NPMs to safely shutdown. Given the fail-safe design of the DHRS, 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 was to occur in the first NPM.

High Winds

In terms of initiating an upset to steady-state operations, a high-wind event results in a LOOP including loss of the BDGs 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 that results in a reactor trip of all six NPMs, and loss of the BDGs. On a loss of AC power, numerous safety systems will actuate. Because of the passive nature of the safety systems, once they actuate, there is no further need for electric power or operator actions.

The impact of a high winds event is initially that of a station blackout due to loss of power, which is analyzed in the full power internal events PRA. Although high winds will impact all six NPMs, the review of mitigating systems shows that there is no indication of any coupling mechanisms that would affect the ability of multiple NPMs to safely shut down. Given the fail-safe design of the DHRS, 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 was to occur in the first NPM.

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

Evaluation of full-power multiple NPM operation provides insights into the risk associated with LPSD. The full-power evaluations of internal and external initiating events indicate that NPMs are largely independent. As discussed in Section 19.1.6.1, the NPM 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 NPMs.

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

- Single NPM accident -- The dropped NPM falls toward the centerline of the reactor pool. The NPM comes to rest horizontally on the floor.
- Two-NPM accident -- The dropped NPM strikes an operating NPM, a bioshield, or bay wall at an angle such that it is deflected toward the center of the reactor pool, and comes to rest horizontally to the floor of the reactor pool; the operating NPM is struck near its top.
- Three-NPM accident -- The dropped NPM, which falls toward an operating NPM and strikes it near the top. The bottom of the dropped NPM then slides across the floor and strikes a third NPM on the other side of the reactor pool; the third NPM is struck near its bottom.

A three-NPM accident, requires that the dropped NPM first strike an operating NPM at a sufficient inclination to begin sliding backwards after the contact. The dropped, sliding NPM may then contact a second operating NPM at its base. Additionally, a three-NPM accident is judged to be not credible if the NPM drop occurs in the refueling area, because its base is angled away from the operating area and would slide farther from the operating NPMs.

If the dropped NPM remains partially upright, such as if it is supported by another NPM 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 NPM being struck by a dropped NPM are determined by engineering judgment. The closest analog for an accident sequence for a struck NPM is a general reactor trip. It is reasonable to expect that operators will be closely monitoring a NPM transport, and will manually trip nearby NPMs if the RBC fails.

If the NPM is struck near the top, the CVCS injection line and DHRS heat exchanger piping at the front of the NPM is likely to be damaged, rendering these systems unavailable. If the NPM is struck near its bottom, the low speed of the impact and distance from important components will allow safety systems to be nominally available. In both cases, the CNVs of both NPMs are unlikely to be breached due to the relatively low velocity of impact, caused by the dropped NPM falling only a short distance through the resistive medium of reactor pool water. Likewise, either struck NPM being dislodged from its operating bay is not judged to be credible as the seismic restraints limit horizontal motion, and the weight of the NPM and downward angle at which it is struck will prevent it from being lifted high enough to escape its bay.

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

The PRA supporting the standard design has been used to support the NuScale design. 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.

19.1.8.2 Probabilistic Risk Assessment Input to the Maintenance Rule Implementation

Use of the 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. The PRA developed for the standard design provides the basis for an as-built, as-operated PRA. 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 (1994), SECY-95-132 (1995) and related guidance, has been implemented 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. 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 SSC that operating experience or PRA has shown to be significant to public health and safety. The PRA is used to identify SSC meeting this criterion by applying the quantitative criteria discussed in Section 19.1.4.1.1.9. (Section 16.1.1.)

- Surveillance frequencies in the technical specifications are consistent with assumptions made in the 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 US460 standard 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 19.1-60, 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 several orders of magnitude lower as compared to the CDF safety goal of 1.0 E-4 per reactor year.
  - The ATWS contribution to CDF is several orders of magnitude less than the target of 1.0E-5 per reactor year provided in SECY 83-293 (1983).
  - With regard to a multi-module configuration, the MM-CDF is about 20 percent of the CDF.
- The mean value of the LRF of an NPM is several orders of magnitude lower 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 3 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 19.1-17. 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 x 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 x 10^{-4} per reactor year.

COL Item 19.1-8: An applicant that references the NuScale Power Plant US460 standard design will confirm the validity of the “key assumptions” and data used in the standard design approval application 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 CDF, LRF and CCFP risk metrics, the risk of operating a NuScale Power 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, structures, systems, and components that are not safety-related are assumed to be failed. The focused PRA is performed as a sensitivity study to the full-power, internal events PRA. The results illustrate that safety goals for CDF and LRF are met without reliance on nonsafety-related SSC. A focused PRA is 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 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 the UHS. This capability is illustrated by the following accident sequence from Figure 19.1-9, Sequence 3:

- A LOOP occurs as indicated by initiating event EHVS--LOOP.
- Onsite AC power sources are initially unavailable and not recovered.
- Automatic reactor shutdown occurs.
- The DHRS valves open.
- The 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 all 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 U.S. Nuclear Regulatory Commission, "Assessing the Technical Adequacy of the Advanced Light-Water Reactor Probabilistic Risk Assessment for the Design Certification Application and Combined License Application," DC/COL-ISG-028, 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, 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, November 2006.

19.1-6 Electric Power Research Institute, "Treatment of Parameter and Model Uncertainty for Probabilistic Risk Assessments," EPRI #1016737, EPRI, Palo Alto, CA, 2008.

19.1-7 NuScale Power, LLC, "Risk Significance Determination," TR-0515-13952-NP-A, Revision 0.

19.1-8 Electric Power Research Institute, "Program on Technology Innovation: Comprehensive Risk Assessment Requirements for Passive Safety Systems," EPRI #1016747, EPRI, Palo Alto, CA, 2008.

19.1-9 International Atomic Energy Institute, "Progress in Methodologies for the Assessment of Passive Safety System Reliability in Advanced Reactors," IAEA-TECHDOC-1752, Vienna, Austria, 2014.

19.1-10 INL/EXT-21-64151 Idaho National Laboratory, “Analysis of Loss-of-Offsite Power Events, 2020 Update,” November 2021.

19.1-11 Electric Power Research Institute, "ATWS: A Reappraisal. Part 3. Frequency of Anticipated Transients," EPRI NP-2230, EPRI, Palo Alto, CA, 1982.

19.1-12 Electric Power Research Institute, "A Methodology for Assessment of Nuclear Power Plant Seismic Margin (Revision 1)," EPRI NP-6041-SL, EPRI, Palo Alto, CA, 1991.

19.1-13 Idaho National Laboratory “Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants: 2020 Update,” INL/EXT-21- 65055, November 2021.

19.1-14 Sandia National Laboratories, "MELCOR Computer Code Manuals," (Version 2.2), Vol. 1 and Vol. 2, Albuquerque, NM, January 2021.

19.1-15 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.

19.1-16 Electric Power Research Institute, "Advanced Light Water Reactor Passive Plant Utility Requirements Document," Rev. 13, EPRI 3002003129, EPRI, Palo Alto, CA, 2014.

19.1-17 U.S. Nuclear Regulatory Commission, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement; Republication," *Federal Register*, Vol. 51, No. 162, August 21, 1986, pp. 30028-30033.

19.1-18 Nuclear Energy Institute, "Guidance for Post Fire Safe Shutdown Circuit Analysis," NEI 00-01, Revision 2, May 2009.

19.1-19 Nuclear Energy Institute, "Guidance for Post Fire Safe Shutdown Circuit Analysis," NEI 00-01, Revision 3, October 2011.

19.1-20 Nuclear Energy Institute, "External Flooding Integrated Assessment Guidelines," NEI 16-05, Revision 0, April 2016.

19.1-21 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.

19.1-22 Electric Power Research Institute, "An Analysis of Loss of Decay Heat Removal and Loss of Inventory Event Trends (1990-2009)," EPRI #1021167, EPRI, Palo Alto, CA, 2010.

19.1-23 Electric Power Research Institute, "Methodology for Developing Seismic Fragilities," EPRI #103959, EPRI, Palo Alto, CA, 1994.

19.1-24 Electric Power Research Institute, "Seismic Fragility Applications Guide Update," EPRI #1019200, EPRI, Palo Alto, CA, 2009.

19.1-25 Electric Power Research Institute, "Advanced Light Water Reactor Passive Plant Utility Requirements Document," Rev. 13, EPRI #3002000507, EPRI, Palo Alto, CA, 2014.

19.1-26 Idaho National Laboratory, “CCF Parameter Estimates, 2020 Update,” INL/EXT-21-62940, November 2021.

Table 19.1-1: Uses of Probabilistic Risk Assessment at the Design Phase

Use	Applicable Section
Identify dominant risk contributors	Section 19.1.4, Section 19.1.5, Section 19.1.6, Section 19.1.7
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, Section 19.1.5
Evaluate conformance with NRC safety goals	Section 19.1.4, Section 19.1.9
Assess the balance of preventive and mitigative features and consistency with SECY-93-087 (1993) and associated staff requirement memorandum	Section 19.2.2
Support Design Reliability Assurance Program including RTNSS classification of structures, systems, and components	Section 17.4, Section 19.3
Potential design improvements	Section 19.2.6
Support Regulatory Oversight Processes, for example, • Mitigating Systems Performance Index • Significance Determination Process	Section 19.1.8
Technical Specifications support • Design-specific surveillance frequencies • Criterion 4 of 10CFR50.36(c)(2)(ii)(D)	Section 19.1.8
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	The 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 primary system cooling loop.	• No external reactor cooling system pipe results in less likelihood of a pipe break outside of containment. • 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 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	The ECCS consists of 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. • The ECCS is effective in maintaining core cooling for possible LOCA and pipe break sizes. • No reliance on external sources of inventory addition to the RPV.
Passive fail-safe DHRS	Passive, natural circulation, closed-loop isolation condensers remove 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 response to unplanned reactor trip.
Small reactor core	Reactor core in each module is a fraction of the size of a typical large PWR core.	• Small reactor core is easier to keep cool under normal and abnormal conditions. (Passive safety systems maintain core cooling.) • Each core, in a multiple NPM plant, 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 the RPV lower head in the unlikely event a severe accident results in core relocation to the lower head; as a result, evaluation indicates core debris is retained in the RPV.
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. • The 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 rapid equalizing 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 their design for full RCS operating system pressure and temperature significantly decreases the likelihood of an interfacing system LOCA.
Seismic Category I UHS	The UHS pool is a large body of borated water in the RXB. The pool is stainless steel lined with a leak detection system embedded in the floor.	• The UHS is not susceptible to becoming unavailable as a result of biofouling, weather-related conditions (e.g., freezing) or catastrophic external event.
Robust, aircraft impact resistant (for safety-related portions) RXB	Each NPM includes an RPV and a CNV. All NPMs and the UHS are all housed in a safety-related portion of the RXB, able to withstand a local and global effects of an 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.	• The 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.
Small coolant flow paths in the upper riser	Small holes in the upper riser permit reactor coolant to bypass the top of the riser.	• Eliminates the potential for significant boron concentration gradients between the core/riser and downcomer during extended DHRS operation.

Table 19.1-3: Use of Probabilistic Risk Assessment in Selection of Design Alternatives

Design Issue	Purpose
CVCS flow area restriction	Adding venturi flow restrictors to the CNV safe ends of the CVCS lines supports the passive mitigation of CVCS breaks outside containment where CVCS isolation has failed. Including passive mitigation of unisolated CVCS breaks reduces LRF, thereby decreasing the conditional containment failure probability.
CVCS check valve location	A design decision to relocate valves (e.g., the reverse flow check valves) to support inspections and access includes locating them as close as possible to their respective CIVs; this location minimizes the likelihood of a break outside containment.
Alternate power alignment	Including the ability to provide a backup power supply to the module-specific medium voltage AC electrical distribution system switchgear reduces the likelihood of losing AC power to an NPM.
ECCS actuation	Adding module protection system actuation signals for high-high RCS pressure and high-high average RCS temperature provides over pressure protection in beyond design basis events.
CES resize	When pipe diameter increased, piping was upgraded to support full RCS pressure and CES valves also get containment isolation signal.
RCS injection	Design iterations including adding valve hand wheels to ensure that operators can align flowpaths to support makeup injection if support systems (e.g., AC power) are lost.
CIV bypass	Including manual O-1 override switches to allow operators to bypass an active containment isolation signal and open closed CIVs to support makeup injection.
Failure probability for RBC	Evaluate failure probability for RBC used for NPM movements.
ECCS valve reliability	Estimates the failure probability that an ECCS valve fails to open on demand.
Spurious opening of ECCS valves	Estimates the frequency of spurious ECCS valve operation, including a spurious partial opening of an ECCS vent or recirculation valve.
DHRS design options	Optimize DHRS configuration that are passive, single-active-failure-proof, and provide at least 72 hours of cooling.
FWS design options	Provide system reliability (unreliability) values for the various options considered in the feedwater/auxiliary feedwater design decision.
DHRS CIVs	Evaluate potential DHRS CIV configurations.
Arrangement of reactor trip breakers	Sensitivity study of the number and arrangement of reactor trip breakers on the reliability of the MPS.
Main steam isolation valve options	Evaluate feedwater and main steam isolation valve options.
Conditional core damage probability for station blackout	Examine a station blackout and the safe shutdown capability.
MPS CCF and availability	Evaluate MPS CCF failures and the impact of doing online maintenance.

Table 19.1-4: Systems Modeled in the Probabilistic Risk Assessment

System	Description
boron addition system (BAS)	The BAS is modeled as two parallel pumps drawing suction from the common boric acid storage tank, which discharges into a common header that feeds the CVCS. The BAS is the initial inventory source because the demineralized water supply isolation valves are signaled to close on a reactor trip.
chemical and volume control system (CVCS)	The CVCS provides a means of adding reactor coolant to the RCS and is modeled as a single loop with the BAS and DWS as the suction sources 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)	The CFDS is modeled as two parallel pumps and associated valves, used to provide inventory, taken from the reactor pool and piped to the CNV, to remove core heat during a severe accident.
containment system (CNTS)	The CNTS is modeled as the CIVs that isolate the CNV and contain fission products in the event of a severe accident.
control rod drive system (CRDS)	The control rod drive system is modeled as the control rod assemblies which insert negative reactivity into the core; the control rod drive system is actuated by RTS.
decay heat removal system (DHRS)	The DHRS is modeled as two redundant trains, one feeding each steam generator. 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)	The DWS is modeled as 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, EDAS, BPSS)	The electrical system is modeled as parts of five plant systems- high voltage AC electrical power distribution system (EHVS), medium voltage AC electrical distribution system (EMVS), low voltage AC electrical distribution system (ELVS), the module-specific portion of the augmented DC power system (EDAS), and the backup power supply system (BPSS). The electrical systems provide power to the required loads during a plant transient.
emergency core cooling system (ECCS)	The ECCS is modeled as two independent reactor vent valves (RVVs) and two independent reactor recirculation valves (RRVs), which open to allow recirculation of reactor coolant water between the RPV and the CNV to remove of core heat during a plant transient.
module protection system (MPS)	The MPS is modeled as four separated groups of instrumentation that supply signals to two divisions of the RTS and the engineered safety features actuation system (ESFAS), which then provide signals to the main control room display for use by the operator, as well as data for control and indication.
reactor coolant system (RCS)	The RCS is modeled as two redundant reactor safety valves (RSVs) that respond to sequences which include increases in primary system pressure to the point of an RSV demand.
ultimate heat sink (UHS)	The UHS is modeled as a water pool that supports DHRS and ECCS passive heat removal and provides suction to the CFDS.

Table 19.1-5: System Dependency Matrix

		Frontline PRA Systems/Functions							
		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				
	EDAS[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		

<u>Notes on support system dependencies:</u>

1. The BAS is the initial inventory source to support CVCS injection. If inventory beyond the BAS is needed, operators can also locally align DWS to support injection. The BAS and DWS pumps and valves are powered from the ELVS.
2. The CNTS includes opening CIVs (i.e., CFDS and CVCS) and closing isolation valves (i.e., MSS and FWS).
3. The EDAS is powered from ELVS with backup from batteries.
4. In the PRA, EHVS is powered from offsite power.
5. The design is fail-safe; in response to a loss of all power (AC and DC), MPS actuates the RTS and ESFAS (i.e., CIV closure, DHRS, and ECCS).

<u>Notes on PRA frontline systems/functions:</u>

A. The BPSS includes two backup diesel generators (BDGs).
B. As a frontline system, CNTS is modeled to close CIVs, and MSS and FWS backup isolation valves.
C. In the PRA, the RCS is modeled as the RSVs to provide RPV pressure relief.
D. In the PRA, the RTS includes the reactor trip breakers and the control rod drive system (i.e., control rod assembly insertion).

Table 19.1-6: Success Criteria per Top Event

Top Event	Mitigating System[1]	Description
CFDS-T01	CFDS	In sequences with a continued loss of RCS inventory (e.g., unisolated pipe break) and success of ECCS, the CFDS can provide RCS makeup inventory. Actuation requires an operator action that includes unisolating containment and activating a CFDS pump (CFDS--HFE-0001C-FOP-N).
CVCS-T02	CVCS isolation	Following an injection line break outside of containment, closure of either CIV in the injection line isolates the line and minimizes the loss of RCS inventory.
CVCS-T03	CVCS isolation	Following a discharge line break outside of containment, closure of either CIV in the discharge line isolates the line and minimizes the loss of RCS inventory.
CVCS-T01	CVCS makeup	The CVCS can provide RCS makeup via the injection or pressurizer spray line.
CVCS-T04	CVCS makeup	Following a CVCS injection or spray line break inside containment, RCS makeup can be provided via the alternate line; the injection line following a spray line break, or the spray line following an injection line break. Actuation requires an operator action to unisolate containment and activate a CVCS makeup pump (CVCS--HFE-0001C-FOP-N). The BAS and the DWS provide inventory to support the PRA mission.
DHRS-T01	DHRS	The DHRS provides fuel assembly heat removal. The DHRS is a passive cooling system that removes fuel assembly heat by circulating coolant through the SGs and DHRS condensers that transfer heat to the UHS. One of two trains is required and each requires opening an actuation valve and closing the respective secondary system CIVs or backup valves in the MSS and the FWS.
DHRS-T02	DHRS	Following an SGTF, the DHRS in the unaffected SG provides fuel assembly heat removal.
ECCS-T01	ECCS	The ECCS provides fuel assembly heat removal and control of RCS inventory without the need for makeup inventory or containment isolation[2]. Success of the ECCS requires the opening of one RVV and one RRV. The system passively circulates coolant by removing heat from the reactor core through the CNV to the UHS. The main ECCS RRVs include a passive opening feature. If a valve fails to open because of a failure in the hydraulic actuator (i.e., closed trip valve or closed IAB), the valve passively opens when the spring force overcomes the differential pressure force across the valve disc[3]. Thermal-hydraulic simulations were performed to confirm the effectiveness of the low differential pressure opening mechanism, including the timing of opening of the valves. Only passive opening of the RRVs is credited in the PRA[4]. Actuation signals include low RCS level, high-high RCS pressure, high-high RCS average temperature, the reactor trip 8-hour timer, and the low AC voltage 24-hour timer. Loss of two or more EDAS buses also deenergizes the solenoids to open the ECCS valves.
ECCS-T02	ECCS	Following an unisolated break outside containment, the opening of both RVVs and both RRVs can provide RCS heat removal and control of RCS inventory without the need for makeup inventory. An operator action to actuate the ECCS in cases where automatic initiation fails is considered (ECCS--HFE-0001C-FTO-N).
ECCS-T03	ECCS	Following normal post-trip response with the RTS and the DHRS, bypassing the reactor trip 8-hour timer (after confirming shutdown margin) precludes an ECCS actuation. An operator action to bypass the timer is considered (ECCS--HFE-0002C-FTB-N).

Table 19.1-6: Success Criteria per Top Event (Continued)

Top Event	Mitigating System[1]	Description
BPSS-T01	Electric Power	Backup power via a BDG precludes an ECCS actuation and allow for RCS makeup (i.e., CVCS, CFDS) if needed. Alignment of a BDG requires operator action (BPSS--HFE-0001C-FTS-N).
EHVS-T01	Electric Power	Recovery of the EHVS via offsite power within 24 hours (following bypass of the reactor trip 8-hour timer) precludes an ECCS actuation.
EHVS-T02	Electric Power	Recovery of the EHVS via offsite power within 8 hours (following failure to bypass the reactor trip 8-hour timer) will preclude an ECCS actuation.
RCS-T01	RSV opens	The RSVs provide pressure relief. Although a cycling RSV can serve as a backup to DHRS heat removal, when the RCS level reaches the low level setpoint, the ECCS is actuated.
RCS-T04	SGTF isolation	Following an SGTF, closure of the CIVs or backup isolation valves in the affected MSS and FWS lines minimizes the loss of RCS inventory and isolates the faulted SG.
RCS-T05	RSV not demanded	This event accounts for the possibility that primary pressure does not increase to the point of reaching the RSV setpoint (e.g., one train of the DHRS may remove heat quickly enough to prevent an RSV demand to open).
RCS-T06	RSV closes	Closure of the RSV after opening re-establishes RCS integrity. This top event is only considered in scenarios with DHRS success where there is a single RSV cycle. In scenarios with DHRS failure or an ATWS, the RSV cycles many times. When RCS level reaches the low level setpoint, the ECCS is actuated, regardless of RSV closure.
RTS-T01	RTS	The RTS provides reactivity control.

Notes:

1. The PCS is not considered as a mitigating system in the PRA. Because almost any unplanned transient results in actuation of the DHRS, the PCS is isolated (i.e., MSS and FWS lines).
2. The ECCS provides passive cooling without additional inventory or closure of normally open CIVs.
3. The main valve control chamber can be depressurized through the internal orifice located in the body of the valve disk (i.e., passive opening); as differential pressure lowers, the main valve spring assisted by reactor coolant pressure opens the valve.
4. The PRA NRELAP5 runs show the low differential pressure across the RVVs (i.e., passive opening) is not reached in time to prevent core damage.

Table 19.1-7: Level 1 Internal Probabilistic Risk Assessment Initiating Events

Category	Initiator	Label	Description	Mean Frequency (mcyr^{-1})	Error Factor
Pipe Breaks and Loss of Coolant Accidents	CVCS Pipe Break Outside Containment - Injection Line	IE-CVCS--BREAK-IOC	Breaks in the injection flowpath (RCS injection line and pressurizer spray supply line break outside of containment) to the RPV.	1.7E-05	10
	CVCS Pipe Break Outside Containment - Discharge Line	IE-CVCS--BREAK-DOC	Breaks in the RCS discharge line outside of containment.	2.5E-06	10
	CVCS LOCA Inside Containment - Injection Line	IE-CVCS--ALOCA-IIC	Breaks in the RCS injection line or pressurizer spray line inside containment, or in a supply line to an ECCS reset valve.	4.1E-04	10
	LOCA Inside Containment	IE-RCS---ALOCA-IC	Break in the RCS discharge line inside containment or a break in the RPV high point degasification line inside containment, the spurious operation of a reactor safety valve, or a pressurizer heater induced LOCA.	1.3E-03	10
	Spurious Opening of an ECCS Valve	IE-ECCS--ALOCA-RV1	Unintended actuation of an ECCS valve (RVV or RRV).	7.2E-04	10
Steam Generator Tube Failure	Steam Generator Tube Failure	IE-MSS---ALOCA-SG-	Failure of a single steam generator tube.	4.6E-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 inside and outside of containment, as well as spurious operation of the relief valves.	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.	2.5E-02	10
	Loss of DC Power	IE-EDAS--LODC-----	De-energization of at least two augmented DC buses.	2.6E-04	10
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.	5.8E-01	10
	Loss of support systems	IE-TGS---TRAN--SS	The partial loss of AC power support systems resulting in unavailability of the CVCS and the CFDS to provide inventory.	5.2E-03	10

Table 19.1-8: Basic Events with Modified Generic Data

Description	NuScale Mean Value	Uncertainty
Given actuation at least 2 of 16 rods fail to insert	9.3E-06	EF = 10; lognormal
CCF of 2 of 4 ECCS: • RRV trip valves fail to open • RVV trip valves fail to open	2.2E-05	EF = 10; lognormal
Offsite power not restored within 24 hours	7.0E-02	EF = 5; lognormal
Offsite power not restored within 8 hours	2.0E-01	EF = 3; lognormal
Offsite power not restored within 24 hours (high winds)	2.4E-01	EF = 3; lognormal
Offsite power not restored within 8 hours (high winds)	4.2E-01	UB =8.4E-01; uniform
ECCS main valve fail to open	3.1E-04	EF = 10; lognormal
ECCS inadvertent actuation block valve (IAB) fails to operate	1.2E-04	EF = 10; lognormal
MPS module failures: • Equipment interface module fails to operate • Scheduling and bypass module fails to operate • Safety function module fails to operate • Scheduling and voting module fails to operate	4.1E-08	EF = 10; lognormal
Equipment interface module discrete control element fails to trip	7.6E-05	EF = 10; lognormal

Table 19.1-9: Basic Events Requiring Design-Specific Analysis

Description	Mean	Uncertainty	Comment
ECCS reactor recirculation valve passive opening at low differential pressure	1E-01	N/A	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 = 10; 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 = 10; lognormal	Following successful actuation of the ECCS, this event represents a failure of passive heat transfer (i.e., natural circulation) to the UHS over the mission time.
Temperature induced SGTF	2.5E-02	EF = 5; lognormal	The conditional probability that a helical coil steam generator tube (in compression) fails following core damage.

Table 19.1-10: Phenomena Affecting Emergency Core Cooling System Passive Performance

Parameter	Significance*
Decay power	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 temperature increases heat transfer through the CNV and decreases pressure in the CNV, reducing the RPV level.
Actuation setpoints	Actuating the ECCS on a lower level delays the time in which recirculation may be established.

*Note: Parameter significance is provided with respect to the passive reliability of the ECCS to facilitate liquid coolant recirculation to the RPV.

Table 19.1-11: Phenomena Affecting Decay Heat Removal System Passive Performance

Parameter	Significance*
Decay power	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.
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.
UHS Pool Temperature	A higher pool temperature decreases the effectiveness of the DHRS.

*Note: Parameter significance is provided with respect to the passive reliability of the DHRS to remove sufficient decay heat to prevent RPV overpressurization.

Table 19.1-12: Pre-initiator Operator Actions

Description	HEP Value	Uncertainty
During test and maintenance, operator misaligns: • MDP 00012A BAS train A manual valves • MDP 00012B BAS train B manual valves	9.7E-04	EF = 5; lognormal
During test and maintenance, operator misaligns: • DGN 0001X ELVS standby diesel generator • DGN 0002X ELVS standby diesel generator	8.0E-04	EF = 10; lognormal
During test and maintenance, operator misaligns: • MDP 0004A CFDS train A manual valves • MDP 0004B CFDS train B manual valves • MDP 0098A CVCS train A manual valves • MDP 0098B CVCS train B manual valves	9.7E-04	EF = 5; lognormal
During test and maintenance, operator miscalibrates: • pressurizer level SFMs • pressurizer pressure SFMs • riser level SFMs • containment pressure SFMs • main steam pressure SFMs	5.3E-04	EF = 10; lognormal

Table 19.1-13: Post-initiator Operator Actions

Description	HEP Value [1] (Diagnosis + Action)	Uncertainty
Operator fails to load BDG (BPSS--HFE-0001C-FTS-N [2])	4.2E-04	EF = 10; lognormal
Operator fails to unisolate containment and initiate CFDS injection (CFDS--HFE-0001C-FOP-N [2])	4.0E-03	EF = 5; lognormal
Operator fails to isolate containment (CNTS--HFE-0001C-FTC-N [2])	2.2E-04	EF = 10; lognormal
Operator fails to unisolate containment and initiate CVCS injection (CVCS--HFE-0001C-FOP-N [2])	4.0E-03	EF = 5; lognormal
Operator fails to locally unisolate containment and initiate CVCS injection (CVCS--HFE-0002C-FOP-N [2])	4.0E-03	EF = 5; lognormal
Operator fails to open ECCS valves[3] (ECCS--HFE-0001C-FTO-N [2])	2.2E-04	EF = 10; lognormal
Operator fails to bypass ECCS timer after confirming shutdown margin (ECCS--HFE-0002C-FTB-N)	1.1E-04	EF = 10; lognormal
Operator fails to align alternate power to module-specific ELVS (ELVS--HFE-0001C-FTC-N [2])	4.2E-04	EF = 10; lognormal

Notes:

1. A review of the individual HEP results was performed; the individual HEP results are reasonable compared to each other and the context to which they are used in the scenarios. Typical post-initiator HEPs are generally in the range of 1E-1 to 1E-4. In the NuScale design there is extensive redundancy and automation, and the PRA scenarios analyzed include ample time for diagnosing and executing the postulated actions.
2. Post-initiator action is a mitigation action (i.e., in response to equipment failures).
3. These simple actions could also be performed from the MPS cabinets, located in the reactor building.

Table 19.1-14: Generic Sources of Level 1 Model Uncertainty

Uncertainty Source	Description (Reference 19.1-6)	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 are 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, a sensitivity study provided in Table 19.1-22 is 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.	The 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 19.1-14: Generic Sources of Level 1 Model Uncertainty (Continued)

Uncertainty Source	Description (Reference 19.1-6)	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 the 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 overpressurization 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 because of 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 overpressurization 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. A sensitivity study discussed in Section 19.1.9.3 addresses the effect of not crediting nonsafety-related systems in the PRA; this special study is a "focused PRA.”

Table 19.1-14: Generic Sources of Level 1 Model Uncertainty (Continued)

Uncertainty Source	Description (Reference 19.1-6)	Level 1 Assumption	Effect on Model
Battery life calculations	Station Blackout events are important contributors to baseline CDF at nearly every US nuclear power plant. 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 power-operated relief valves (PORVs) required for bleed and feed-PWRs	The 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	Because of 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).	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 focused PRA discussed in Section 19.1.9.3 captures this source of model uncertainty.

Table 19.1-14: Generic Sources of Level 1 Model Uncertainty (Continued)

Uncertainty Source	Description (Reference 19.1-6)	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 19.1-15: 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 standard design.	The PRA model reflects the current state of design for the standard design.	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).	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 are used, a lognormal distribution with an error factor of 10 is used to bound the uncertainty. Sensitivity studies provided in Table 19.1-22 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 is performed to estimate the frequency of an SGTF based on a probabilistic physics of failure approach.	A sensitivity study (provided in Table 19.1-22 illustrates that an increase in the frequency of an SGTF has no 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 is performed to analyze system design to estimate the frequency of a secondary line break.	A sensitivity study provided in Table 19.1-22 illustrates that an increase in the frequency of a secondary line break has no impact on the results. As such, this is judged not to be a significant source of model uncertainty
Accident Sequence Analysis and Success Criteria			
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.	A sensitivity study provided in Table 19.1-22 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 (RRVs) operating mode with no plant experience.	The probability of the ECCS low differential pressure (RRVs) opening mode is assumed to be 0.1.	A sensitivity study provided in Table 19.1-22 evaluated the effect of increasing the failure probability as small. In addition, a sensitivity study addressed uncertainty in ECCS actuation because of CCF.

Table 19.1-15: Design-Specific Sources of Level 1 Model Uncertainty (Continued)

Uncertainty Source	Description	Level 1 Assumption	Effect on Model
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 are used, a lognormal distribution with an error factor of 10 is used to bound the uncertainty.
Component failure data	Reliability data with no plant experience.	Generic data are 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.
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 the 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 a sensitivity study provided in Table 19.1-22, 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 a sensitivity study (provided in Table 19.1-22, which addresses HEP.
Latent actions	The potential for overcounting 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.

Table 19.1-15: Design-Specific Sources of Level 1 Model Uncertainty (Continued)

Uncertainty Source	Description	Level 1 Assumption	Effect on Model
Commission errors	The potential for commission errors based on a new design with no design-basis operator actions.	A review of potential commission errors is performed, but no impactful errors of commission are identified.	Consideration is given to the potential of defeating the 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 the ECCS. Therefore, this is judged not to be a significant source of model uncertainty.
Systems Analysis			
PCS unavailability	Availability of the PCS following an initiating event with no plant experience.	In the current design, the PCS is not expected to be available following an initiating; the PRA does not model the PCS as a mitigating system.	This is best estimate; there may be a slight conservatism in the results by not crediting the PCS.
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.	A sensitivity study provided in Table 19.1-22 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).	Instrumentation and controls 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 19.1-16: Initiating Event Contribution to Risk

Initiating Event	Contribution to CDF (Percentage)	Contribution to LRF (Percentage)
Loss of support system (TGS---TRAN--SS)	33.6	33.0
Loss of offsite power (EHVS-LOOP)	27.1	8.2
General reactor trip (TGS---TRAN-NPC)	19.9	33.0
Reactor coolant system LOCA inside containment (RCS---ALOCA-IC)	9.2	4.0
Chemical and volume control system LOCA injection line inside containment (CVCS-ALOCA-IIC)	4.3	0.7
Spurious opening of an emergency core cooling system valve (ECCS--ALOCA-RV1)	4.2	1.2
Loss of DC power (EDAS-LODC)	1.8	< 0.1
CVCS injection line break outside containment (CVCS--BREAK-IOC)	< 0.1	20.0
CVCS discharge line break outside containment (CVCS--BREAK-DOC)	< 0.1	0.5
Steam generator tube failure (MSS---ALOCA-SG)	< 0.1	< 0.1
Secondary side line break (TGS---FMSLB-UD)	< 0.1	< 0.1

Table 19.1-17: Dominant Core Damage Sequences (Full Power, Internal Events, Single Module)

Event Tree Initiator	Sequence	Contribution (% CDF)	Sequence Description
Loss of support system (TGS---TRAN---SS)	Figure 19.1-12 Sequence 3	33.3	Loss of support system initiating event followed by failure to align alternate power to module-specific low voltage AC electrical distribution system (ELVS), and failure of ECCS.
Loss of offsite power (EHVS-LOOP)	Figure 19.1-9 Sequence 4	12.6	A LOOP initiating event followed by failure of the backup diesel generators (BDGs), failure to restore power before the batteries deplete, and failure of ECCS.
Loss of offsite power (EHVS-LOOP)	Figure 19.1-9 Sequence 12	12.6	A LOOP initiating event with an RSV cycle followed by failure of the BDGs, failure to restore power before the batteries deplete, and failure of ECCS.
General reactor trip (TGS-TRAN-NPC)	Figure 19.1-11 Sequence 11	12.4	Transient initiating event with an RSV demand and failure of the RSVs to reclose, failure of ECCS, and failure to makeup inventory via the CVCS.
RCS LOCA inside containment (RCS---ALOCA-IC)	Figure 19.1-5 Sequence 3	9.3	An RCS LOCA inside containment initiating event followed by failure of ECCS, and failure to makeup RCS inventory via CVCS.
CVCS LOCA injection line inside containment (CVCS--ALOCA-IIC)	Figure 19.1-4 Sequence 3	4.3	A CVCS injection line LOCA inside containment initiating event followed by failure of ECCS, and failure to makeup inventory via CVCS.
Spurious Opening of an ECCS Valve (ECCS--ALOCA-RV1)	Figure 19.1-6 Sequence 3	4.3	A spurious opening of an ECCS valve followed by failure of ECCS and failure to makeup inventory via CVCS.
General reactor trip (TGS-TRAN-NPC)	Figure 19.1-11 Sequence 8	3.7	Transient initiating event with an RSV cycle followed by failure to bypass the 8 hour shutdown margin timer, and failures of ECCS and makeup inventory via CVCS.
General reactor trip (TGS-TRAN-NPC)	Figure 19.1-11 Sequence 4	3.7	Transient initiating event followed by failure to bypass the 8 hour shutdown margin timer, and failures of ECCS and makeup inventory via CVCS.
Loss of DC power (EDAS-LODC)	Figure 19.1-10 Sequence 3	1.8	A loss of DC power initiating event followed by failures of ECCS and failure to makeup inventory via CVCS.
Loss of offsite power (EHVS-LOOP)	Figure 19.1-9 Sequence 19	1.1	A LOOP initiating event with an RSV demand and failure of the RSVs to reclose, failure of the BDGs, and failure of ECCS.
Other sequences	All	1.0	

Table 19.1-18: Dominant Core Damage Cutsets (Full Power, Internal Events, Single Module)

Cutset	Frequency	Contribution	Description
1	4.5E-10	8.3	
			Loss of Support System
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
2	1.7E-10	3.1	
			Loss of Support System
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
3	1.7E-10	3.1	
			Loss of Support System
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
4	1.5E-10	2.8	
			General Reactor Trip
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
5	1.1E-10	2.1	
			LOCA Inside Containment
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
6	9.7E-11	1.8	
			General Reactor Trip
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER

Table 19.1-18: Dominant Core Damage Cutsets (Full Power, Internal Events, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET FOLLOWING ECCS SDM TIMER BYPASS HFE
			RCS Reactor Safety Valve Not Demanded to Open
7	9.7E-11	1.8	
			General Reactor Trip
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET FOLLOWING ECCS SDM TIMER BYPASS HFE
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
8	9.7E-11	1.8	
			Loss of Support System
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			CBL 3011X1 ELVS MODULE-SPECIFIC CIRCUIT BREAKER FAILS TO CLOSE
9	9.7E-11	1.8	
			Loss of Support System
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			CBL 3011X2 ELVS MODULE-SPECIFIC CIRCUIT BREAKER FAILS TO CLOSE
10	9.7E-11	1.8	
			Loss of Support System
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			CBL 3021X2 ELVS MODULE-SPECIFIC CIRCUIT BREAKER FAILS TO CLOSE
11	9.7E-11	1.8	
			Loss of Support System
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			CBL 3021X1 ELVS MODULE-SPECIFIC CIRCUIT BREAKER FAILS TO CLOSE
12	7.6E-11	1.4	
			Loss Of Offsite Power
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN

Table 19.1-18: Dominant Core Damage Cutsets (Full Power, Internal Events, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
13	7.6E-11	1.4	
			Loss Of Offsite Power
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			RCS Reactor Safety Valve Not Demanded to Open
14	6.3E-11	1.2	
			Spurious Opening of an ECCS Valve
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
15	5.8E-11	1.1	
			Loss of Support System
			OPERATOR FAILS TO OPEN ECCS VALVES
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			CCF OF 3 OF 4 RCS RPV LEVEL SENSORS FAIL TO OPERATE ON DEMAND
16	5.7E-11	1.1	
			General Reactor Trip
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
17	5.7E-11	1.1	
			General Reactor Trip
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			RCS REACTOR SAFETY VALVE 0003A FAILS TO RECLOSE
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN

Table 19.1-19: Criteria for Risk Significance

Parameter	Core Damage Criteria for Risk Significance[1]	Large Release Criteria for Risk Significance[1]
Component	CCDF ≥ 3E-06	CLRF ≥ 3E-07
System	CCDF ≥ 1E-05	CLRF ≥ 1E-06
Component[2]	Total FV = 0.005 if CDF > 1E-07	Total FV = 0.005 if LRF > 1E-08
Component	Total FV = 0.2 if (1E-07 ≥ CDF > 1E-08)	Total FV = 0.2 if (1E-08 ≥ LRF > 1E-09)
Component	Total FV = 0.5 if (1E-08 ≥ CDF > 1E-09)	Total FV = 0.5 if (1E-09 ≥ LRF > 1E-10)
Component	Total FV = 0.9 if (1E-09 ≥ CDF ≥ 1E-10)	Total FV = 0.9 if (1E-10 ≥ LRF ≥ 1E-11)

Notes:

1.Risk values are provided in units of per mcyr.

2.Risk values are based on Condition 4 of the SER, which requires CDF to be approximately 1E-07/year or less, along with the CCFP goal of 0.1.

Table 19.1-20: Summary of Candidate Risk-Significant Structures, Systems, and Components

System	Description	CCDF[3]	CLRF[3]	FVCDF[2, 3]	FVLRF[2, 3]
CNTS	Containment system	FI	FI		
ECCS	Emergency core cooling system	FP-IE, FI,HW,EF	Not Met		
MPS[1]	Module protection system (includes ESFAS & RTS)	FP-IE, LPSD, IF, FI,HW,EF	FP-IE, LPSD, IF, FI,HW,EF		
UHS	Ultimate heat sink	FP-IE, IF, FI,HW,EF	IF, FI		
Component	**Description**	**CCDF**	**CLRF**	**FVCDF[2, 3]**	**FVLRF[2, 3]**
ECCS--SOV-0101A1	SOV 0101A1 ECCS RVV 0001A Trip Valve	Not Met	Not Met	HW,EF	Not Met
ECCS--SOV-0101A2	SOV 0101A2 ECCS RVV 0001A Trip Valve	Not Met	Not Met	HW,EF	Not Met
ECCS--SOV-0101B1	SOV 0101B1 ECCS RVV 0001B Trip Valve	Not Met	Not Met	HW,EF	Not Met
ECCS--SOV-0101B2	SOV 0101B2 ECCS RVV 0001B Trip Valve	Not Met	Not Met	HW,EF	Not Met
Human Action	**Description**	**CCDF**	**CLRF**	**FVCDF**	**FVLRF**
None					
Initiating Event	**Description**	**CCDF**	**CLRF**	**FVCDF[3]**	**FVLRF**
IE3RBC---DROP-----	RBC Failure and NPM Drop - POS3			LPSD$_{MD}$	Not Met

Notes:

- Spaces that are ‘greyed out’ indicate categories in which the criteria do not apply.
- Seismic risk significance is characterized by plant-level HCLPF, rather than by importance measures.

1. The MPS fault tree model includes actuation sensor failures and components are assumed to fail as-is.
2. In the absence of industry consensus implementation details, CCFs are conservatively included in the FV calculation for individual components.
3. The following abbreviations are used to identified listed hazards-
   - full power internal events (FP-IE)
   - internal fires (FI)
   - internal flooding (IF)
   - external flooding (EF)
   - high-winds (HW)
   - low power and shutdown (LPSD)
   - low power and shutdown module drop (LPSD$_{MD}$)

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

FULL POWER, INTERNAL EVENTS
Accident Sequence
If makeup inventory is needed, operators are assumed to initially align CVCS for coolant addition through the pressurizer spray line. If the RPV water level continues decreasing and operators observe increasing core temperatures, operators are assumed to realign CVCS coolant addition through the injection line.
Success Criteria
Procedures are assumed to direct operators to preserve the key safety function to remove fuel assembly heat even in cases where they would need to breach the containment boundary (e.g., operators would open the CVCS CIVs to inject makeup following incomplete ECCS actuation).
In the absence of an effective heat removal mechanism during a nominally intact reactor coolant pressure boundary scenario (that is, DHRS fails and RSVs fail to open), the RPV is expected to develop a leak (e.g., pressurizer heater access port bolted flange), and core damage is assumed.
Systems Analysis
Equipment is assumed to be operable without HVAC to support the PRA function. The small size of the equipment together with the slower progression of events provide sufficient time for any mitigating actions that might be needed.
Valve alignment for mitigating systems is assumed to include the capability to open following a loss of support systems (e.g., loss of instrument air) and accessibility for local access.
Shared systems (e.g., CFDS, DWS), are assumed to be available to support accident mitigation.
Failures are assumed to be “as-is”; failure constitutes the lack of signal generation, transmission, or interpretation through MPS equipment to the end-device.
Human Reliability Analysis
Maintenance on multiple system trains is assumed to be performed on a staggered basis; a maintenance error in the first train is assumed to be discovered before an error in the second train could occur.
For scenarios in which operators unisolate containment to initiate injection, but fail to prevent core damage, they are assumed to restore containment isolation.
Post-initiator human actions that include use of the O-1 override are assumed to require operators open the reactor trip breakers or wait until the high pressurizer level signal is no longer present, if needed.
Operators are assumed to control CVCS flow to provide necessary inventory for cooling; makeup actions are intended to maintain pressurizer level in the normal operating band.
Data Analysis
Passive safety system reliability of the DHRS and ECCS natural circulation heat transfer mechanisms are representative of the as-built, as-operated module
Component failure rates, based on design-specific analyses, are representative of the as-built module. Examples include “fails to operate” for the ECCS hydraulic-operated valve and equipment interface module.
FULL POWER, EXTERNAL EVENTS
Internal Flooding PRA
Flooding frequencies are assumed based on generic data for turbine and auxiliary buildings, including human-induced mechanisms. This is likely conservative since the NuScale design has fewer systems (hence fewer potential sources of internal flooding).
An internal flood does not result in an RSV demand if RTS and DHRS are successful.
Internal Fire PRA
Redundant divisions of safe shutdown equipment and cabling are assumed to be appropriately separated to assure at least one safe shutdown train is available following a fire.
Fire barriers are assumed between fire compartments and provide a fire resistance rating of 3 hours.
Seismic Margin Assessment
Generic spectral acceleration capacities for general component types (e.g., valves, heat exchangers, circuit breakers) are assumed applicable to components used in the NuScale design.
Generic fragilities are assumed applicable to components in the NuScale design. The RXB is assumed to meet the seismic margin requirements of 167% of the reference earthquake for site-specific and soil-dependent seismic hazards (e.g., sliding, overturning, slope failure [instability], liquefaction). This is a design expectation.

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

Seismically-induced damage to reactor internals (e.g., fuel assembly, core supports, riser structure) such that the core may not be cooled is assumed to be not credible. This is a design expectation.
High Winds PRA
Although the plant is expected to use forecasting tools, a high winds event is assumed to result in a loss of offsite power with safety system actuation on low AC voltage (i.e., RTS, DHRS, and isolation of CIVs).
A tornado strike hazard is determined from methods described in NUREG/CR-4461.
A hurricane strike hazard is determined from U.S. LWR operating experience.
Seismic Category I structures and equipment in Seismic Category I structures are not susceptible to damage from high winds events.
External Flooding PRA
An external flood that exceeds the design basis flood level is assumed to have a recurrence interval of 500 years; external flooding frequency is 2E-3/yr.
Although the plant is expected to use forecasting tools, 90 percent of external floods are assumed to include significant warning time for operators to perform a controlled shutdown, the remaining 10 percent are assumed to result in a loss of offsite power with safety system actuation on low AC voltage (i.e., RTS, DHRS, and isolation of CIVs). Controlled shutdowns are assumed to result in negligible risk, and are not evaluated. Most natural flooding occurs as a result of excessive precipitation, which is relatively slow developing.
LOW POWER and SHUTDOWN[1]
The mean probability that a dropped NPM fails to remain upright is 0.5, and uncertainty is characterized with a uniform distribution.
MULTIPLE MODULE EVALUATION
Accident timing for multiple modules is not considered; that is, multiple module failures are assumed to occur within the same 72-hour mission time as the single module event.
Operator actions for inventory makeup from the CVCS and CFDS occur sequentially rather than simultaneously.
Site-wide events are assumed to affect all modules equally.
Calculated risk metrics apply to a multiple module event, irrespective of the number of installed modules; that is, all modules are assumed to be affected because of to an initiating event.
SEVERE ACCIDENT MODELING (Level 2)
In RPV overpressure scenarios, core damage is assumed with no impact on containment integrity.

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

Table 19.1-22: Sensitivity Studies

Sensitivity Description	Factor Change in CDF	Factor Change in LRF
Full Power, Internal Events		
Double the LOOP initiating event frequency	1.3	1.2
Decrease LOOP initiating event frequency by an order of magnitude	0.8	0.9
Increase steam generator tube failure initiating event frequency by more than an order of magnitude, to the generic data value	1.0	1.0
Increase secondary line break initiating event frequency by more than 2 orders of magnitude, to the generic data value	1.0	1.0
Double the LODC initiating event frequency	1.0	1.0
Double the CVCS LOCA initiating event frequency	1.0	1.0
Increase CVCS line break outside containment initiating event frequency by an order of magnitude	1.0	3.9
Increase failure probability of passive heat removal by an order of magnitude	1.0	1.0
Increase failure probability of ECCS low differential pressure (RRVs) by a factor of 5	1.2	1.0
Include ECCS low differential pressure opening for RVVs	0.4	0.3
Decrease probability of post-trip RSV demand by a factor of 50	0.9	1.0
Assume core damage RPV overpressure sequences also result in large release	N/A	1.0
All HEPs set to 5th percentile	0.6	0.4
All HEPs set to 95th percentile	2.8	6.4
All CCF set to 0	0.1	<0.1
All CCF set to 95th percentile	>100[1]	>100[1]
Full Power, External Events		
Credit CVCS makeup in non-RXB internal floods	0.8	1.0
Set fire PRA growth to false, which stops fires before they damage mitigating equipment	0.1	<0.01
Set fire PRA growth to true, which ensures fires damage mitigating equipment	14.3	2.5
Double the fraction of external floods that result in a LOOP	2.0	2.1
Include possibility of RVV low differential pressure opening in the external flood PRA	0.4	0.4
Increase probabilities of not recovering offsite power in the hurricane high winds PRA by 50%	1.5	1.5
Double the frequency of a hurricane induced LOOP	2.1	2.1
Include possibility of RVV low differential pressure opening in the hurricane high winds PRA	0.4	0.4
Low Power and Shutdown		
Double the failure probability of CES in POS6	1.0	1.0
Multiple Module		
Decrease MMAFs by an order of magnitude so that NPM-equipment is less correlated	0.6	0.3
Decrease MMPSF for module-specific HFEs by a factor of 5	0.5	<0.01

Note 1: Failures assumed to be "as-is" on loss of MPS

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 and the ECCS successfully actuates.	The RSV cycling and ECCS actuation 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 the DHRS is unnecessary if RSVs cycle.	The SGs and the DHRS provide effective heat removal paths to prevent core damage, but are unnecessary if RSV cycling and ECCS actuation allows heat transfer to reactor pool.
The ECCS functions to preserve RCS inventory, which is sufficient to allow core cooling without RCS makeup from external source.	The 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 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 because of 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 because of 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. Because of 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.

Table 19.1-24: Containment Penetrations

Penetration Number[6]	System Isolated	First CIV	Second CIV	Normal Position
CNV 1	FWS 1	HOV	AOV	open[1]
CNV 2	FWS 2	HOV	AOV	open[1]
CNV 3	MSS 1	HOV	AOV	open[1]
CNV 4	MSS 2	HOV	AOV	open[1]
CNV 5	RCCWS return	HOV	HOV	open[2]
CNV 6	RCS injection	HOV	HOV	open
CNV 7	Pressurizer spray supply	HOV	HOV	open
CNV 8-9	Instrumentation and control (I&C) division 1 and 2	N/A	N/A	sealed[3]
CNV 10	CES	HOV	HOV	open
CNV 11	CFDS	HOV	HOV	closed[3]
CNV 12	RCCWS supply	HOV	HOV	open[2]
CNV 13	RCS discharge	HOV	HOV	open
CNV 14	RPV high point degas	HOV	HOV	closed[3]
CNV 15-16	Electrical 1 & 2 (pressurizer heater)	N/A	N/A	sealed[3]
CNV 17-20	I&C channels A-D	N/A	N/A	sealed[3]
CNV 21	N/A	N/A	N/A	N/A
CNV 22	DHRS 1[7]	N/A	N/A	closed[4]
CNV 23	DHRS 2[7]	N/A	N/A	closed[4]
CNV 24	CNV manway access port 1	N/A	N/A	closed[3]
CNV 25	Control rod drive mechanism (CRDM) access hatch	N/A	N/A	closed[3]
CNV 26	CNV manway access port 2	N/A	N/A	closed[3]
CNV 27-30	Steam generator access ports 1-4	N/A	N/A	closed[3]
CNV 31-32	Pressurizer heater access port 1 and 2	N/A	N/A	sealed[3]
CNV 33	RVV trip/reset 1	N/A	N/A	sealed[5]
CNV 34	RVV trip/reset 2	N/A	N/A	sealed[5]
CNV 35	RRV trip/reset 1	N/A	N/A	sealed[5]
CNV 36	RRV trip/reset 2	N/A	N/A	sealed[5]
CNV 37	Electrical CRDM power 1	N/A	N/A	sealed[3]
CNV 38-39	I&C rod position indication group 1 and 2	N/A	N/A	sealed[3]
CNV 40-43	I&C separation groups A-D	N/A	N/A	sealed[5]
CNV 44	Electrical CRDM power 2	N/A	N/A	sealed[5]

Table 19.1-24: Containment Penetrations (Continued)

Penetration Number[6]	System Isolated	First CIV	Second CIV	Normal Position
CNV 45	DHRS 1[7]	N/A	N/A	closed[4]
CNV 46	DHRS 2[7]	N/A	N/A	closed[4]

Notes:

1. Because these lines are not connected directly to the RCS, an SGTF is also required for a release.
2. The RCCWS is a closed loop inside the CNV and is therefore screened.
3. Normally closed or sealed penetrations are screened.
4. The DHRS lines are not connected directly to the RCS and are therefore screened.
5. The ECCS trip/reset pilot assembly safe-end penetrations are welded to the external side of the penetration nozzle. Because each has a double seal with monitoring capability, they are screened.
6. While not identified by a penetration number, the CNV is designed in two parts that connect at the main flange; the main flange is a normally closed and sealed penetration and therefore screened.
7. DHRS lines connected to the CNV top head (i.e., CNV 45 and CNV 46) branch from the MSS lines and carry steam to the DHRS condensers. DHRS lines connected to lower nozzles (i.e., CNV 22 and CNV 23) connect to the FWS lines.

Table 19.1-25: Dominant Large Release Sequences (Full Power, Internal Events, Single Module)

Event Tree Initiator	Sequence	Contribution (% LRF)	Sequence Description
Loss of support system (TGS---TRAN---SS)	Figure 19.1-12 Sequence 3	33.3	Loss of support system initiating event followed by failure to align alternate power to module-specific ELVS, and failures of ECCS, and containment isolation.
General reactor trip (TGS-TRAN-NPC)	Figure 19.1-11 Sequence 14	18.2	Transient initiating event followed by failure of decay heat removal system (DHRS), a cycling RSV, and failures of ECCS, CVCS, and containment isolation.
CVCS injection line break outside containment, (CVCS--BREAK-IOC)	Figure 19.1-2 Sequence 11	13.6	A CVCS injection line break outside containment initiating event followed by failure to isolate the break, and failure of ECCS.
General reactor trip (TGS-TRAN-NPC)	Figure 19.1-11 Sequence 11	5.2	Transient initiating event followed by failures of the RSVs (to close), and failures of ECCS, CVCS, and containment isolation.
General reactor trip (TGS-TRAN-NPC)	Figure 19.1-11 Sequence 8	4.2	Transient initiating event with an RSV cycle followed by failure to bypass the 8 hour shutdown margin timer, and failures of ECCS, CVCS, and containment isolation.
General reactor trip (TGS-TRAN-NPC)	Figure 19.1-11 Sequence 4	4.4	Transient initiating event followed by failure to bypass the 8 hour shutdown margin timer, and failures of ECCS, CVCS, and containment isolation.
RCS LOCA inside containment (RCS---ALOCA-IC)	Figure 19.1-5 Sequence 3	3.9	An RCS LOCA inside containment initiating event followed by failures of ECCS, CVCS, and containment isolation.
Loss of offsite power (EHVS-LOOP)	Figure 19.1-9 Sequence 12	3.3	A LOOP initiating event with an RSV cycle followed by failure of the BDGs, failure to restore power before the batteries deplete, and failures of ECCS and containment isolation.
Loss of offsite power (EHVS-LOOP)	Figure 19.1-9 Sequence 4	3.3	A LOOP initiating event followed by failure of the BDGs, failure to restore power before the batteries deplete, and failures of ECCS and containment isolation.
CVCS injection line break outside containment, (CVCS--BREAK-IOC)	Figure 19.1-2 Sequence 19	3.0	A CVCS injection line break outside containment initiating event followed by failure of the control rods to insert and failure to isolate the break.
Other sequences		7.6	

Table 19.1-26: Dominant Large Release Cutsets (Full Power, Internal Events, Single Module)

Cutset	Frequency	Contribution	Description
1	4.7E-14	13.9	
			General Reactor Trip
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			OPERATOR FAILS TO OPEN ECCS VALVES
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR THIRD HFE IN CUTSET
			CCF OF 2 OF 3 DIVISION I ESFAS SCHEDULING AND VOTING MODULES
			CCF OF 2 OF 3 DIVISION II ESFAS SCHEDULING AND VOTING MODULES
2	1.5E-14	4.4	
			Loss of Support System
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
3	1.5E-14	4.4	
			Loss of Support System
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
4	1.2E-14	3.6	
			CVCS Break Injection Line Outside Containment
			CCF OF 2 OF 2 CNTS CVCS PRESSURIZER SPRAY LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
5	1.2E-14	3.6	
			CVCS Break Injection Line Outside Containment
			CCF OF 2 OF 2 CNTS CVCS INJECTION LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
6	5.6E-15	1.7	
			Loss of Support System
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE

Table 19.1-26: Dominant Large Release Cutsets (Full Power, Internal Events, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
7	5.6E-15	1.7	
			Loss of Support System
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
8	5.6E-15	1.7	
			Loss of Support System
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
9	5.6E-15	1.7	
			Loss of Support System
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
10	5.2E-15	1.5	
			CVCS Break Injection Line Outside Containment
			GIVEN ACTUATION AT LEAST 2 OF 16 RODS FAIL TO INSERT
			CCF OF 2 OF 2 CNTS CVCS INJECTION LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
11	5.2E-15	1.5	
			CVCS Break Injection Line Outside Containment
			GIVEN ACTUATION AT LEAST 2 OF 16 RODS FAIL TO INSERT
			CCF OF 2 OF 2 CNTS CVCS PRESSURIZER SPRAY LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE

Table 19.1-27: Generic Sources of Level 2 Model Uncertainty

Uncertainty Source	Description (Reference 19.1-6)	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 conservatively addressed, 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 large early release frequency 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 before 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 19.1-27: Generic Sources of Level 2 Model Uncertainty (Continued)

Uncertainty Source	Description (Reference 19.1-6)	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 large early release frequency. 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 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. The design also includes a passive autocatalytic recombiner.	This is judged not to be a source of significant model uncertainty based on conservative, plant-specific analysis of the potential for hydrogen deflagration.

Table 19.1-28: 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.	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 19.1-29: Key Insights from Level 2 Evaluation

Insight		Comment	
Containment Isolation	The primary purpose of the CNTS is to retain primary coolant inventory within the CNV. With primary coolant inventory maintained in the RPV or the 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.	
	The 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		
Severe Accident Containment Challenges	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. The passive autocatalytic recombiner eliminates the potential for long-term hydrogen combustion. In addition, conservative AICC analyses predict containment pressures that do not exceed the design pressure.	
	In-vessel steam explosions are not likely because of 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.	

Table 19.1-29: Key Insights from Level 2 Evaluation (Continued)

Insight		Comment
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	There are no risk-significant, post-accident human actions associated with the full-power internal events Level 2 PRA.	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.
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 because of the passive features of the design that are not affected by the external events and plant systems (CNTS) that are protected against external event challenges.

Table 19.1-30: 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 19.1-31: External Events Considered for Operations at Power

1. Aircraft impacts	
Description of hazard	An aircraft impact could damage 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 BPSS, 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 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 BPSS, 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 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, and does not result in worse consequences. Therefore, this hazard is not considered in the PRA. When a site is selected and site cooling 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, and does not result in worse consequences. Therefore, this hazard is not considered in the PRA. When a site is selected and site cooling water system details are finalized, screening this hazard should be confirmed.
Similar hazards	• low lake or river water level • river diversion

Table 19.1-31: External Events Considered for Operations at Power (Continued)

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 trip or shutdown (on one or multiple NPMs), and impact equipment important to safety.
Screening criteria	Evaluated in Section 19.1.5.4.
Subsumed hazards	• coastal erosion • high tide • hurricane - flooding • ice cover - that results in blockage and subsequent flooding • precipitation, intense • river diversion - flooding • seiche • 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 SSC (including the switchyard and equipment important to safety) because of 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, 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.

Table 19.1-31: External Events Considered for Operations at Power (Continued)

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. 4 - High summer temperatures that result in a forced shutdown due to loss of ACC is subsumed in the internal events general transient event.
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.
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 will not impact cooling water intakes or ACC operation. 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, 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) originating inside the plant buildings/structures.
Screening criteria	Evaluated in Section 19.1.5.3.

Table 19.1-31: External Events Considered for Operations at Power (Continued)

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 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 BPSS is expected to be significantly less than an external flood induced LOOP (~5E-3 per year) and does not result in worse consequences. A bounding assessment of RXB roof loading is also included in Appendix C. 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, 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
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 ultimate heat sink.
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 SSC (including the switchyard and equipment important to safety), and cause a plant trip.
Screening criteria	Not applicable. A bounding assessment is 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, 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.

Table 19.1-31: External Events Considered for Operations at Power (Continued)

25. Release of chemicals from onsite 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, 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. 4 - River diversions that result in flooding are subsumed in hazard 6, external flooding.
Similar hazards	• low lake or river level • drought
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.
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 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 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 (i.e., contract) when the water dries up. Significant expansion or contraction due to changes in moisture content can damage the foundations of the plant buildings and structures.
Screening criteria	2 - This event does not result in a plant trip; therefore, it is not considered in the PRA.

Table 19.1-31: External Events Considered for Operations at Power (Continued)

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, 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 expected to be significantly less than the internal event LOOP, and does not result in worse consequences. Therefore, this hazard is not considered in the PRA.
37. Volcanic activity	
Description of hazard	Hazards associated with volcanic activity include lava flows and volcanic ashes. Either could damage 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 BPSS is expected to be significantly less than an external flood-induced LOOP (~5E-3 per year), 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. Grass Fires	
Description of hazard	Grass fires are those that occur in grass areas outside the site boundary. 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 grass fire, however, the frequency would be significantly less than the internal event LOOP, 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 19.1-31: External Events Considered for Operations at Power (Continued)

40. Nonsafety building fire	
Description of hazard	Nonsafety building fires are those that occur inside the site boundary, but originate from buildings that do not contain safety related SSCs. Uncontrolled spread of a fire could challenge nearby safety-related structures. Fires could also result in ventilation and control room habitability concerns and inhibit site access and operations.
Screening criteria	4 - Nonsafety building fires are subsumed in the internal fire PRA analysis.
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 because of 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, 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.
42. Heavy load drop	
Description of hazard	The mishandling or dropping of heavy loads can damage plant SSCs, including the an NPM or potentially multiple NPMs.
Screening criteria	Not applicable; evaluated in Section 19.1.6.
43. Electro-magnetic interference	
Description of hazard	Electromagnetic interference (EMI), 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.
44. 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 NPM; however, the frequency of a core damage and large release from another NPM is extremely low and significantly less than the frequency of the internal events LOOP, and does not result in worse consequences. Therefore, this hazard is not considered in the PRA.

Table 19.1-32: Seismic Margin Assessment Fragility

SSC	HCLPF (g)	Controlling Failure Mode	Assumed Consequence
Reactor Building Crane Supports	0.92g	Weld failure	Core damage/Large Release
Bioshield - normal operation (single stack)	0.93g	Bolt shear failure	Core damage/Large Release
Bioshield - refueling of adjacent NPM (double stack)	0.93g	Bolt shear failure	Core damage/Large Release when configuration present
Reactor Building	0.97g	Roof in-plane shear failure	Core damage/Large Release
Reactor Building Crane	1.11g	Plate bending failure	Core damage/Large Release
NPM Supports	1.14g	Weld failure	Core damage/Large Release
Reactor Recirculation Valves	1.38g	Valve body deformation	Valve failure to open
Reactor Vent Valves	2.69g	Valve body deformation	Valve failure to open
Containment Isolation Valves	3.92g	Valve body deformation	Valve failure to open
Reactor Safety Valves	6.00g	Valve body deformation	Valve failure to open
Trip Valves for Reactor Recirculation Valves	7.14g	Valve body deformation	Valve failure to open
Trip Valves for Reactor Vent Valve	8.44g	Valve body deformation	Valve failure to open

Note:

- HCLPF = High-Confidence (95%) of a Low Probability (5%) of Failure (EPRI 103959)

Table 19.1-33: Applicability of Internal Initiating Events to Fire Probabilistic Risk Assessment

Initiating Event	Applicability to Fire PRA	Comments
CVCS injection line LOCA inside containment (CVCS--BREAK-IOC)	No	A fire is judged not to induce a pipe or vessel leak or break
CVCS discharge line pipe break outside containment (CVCS--BREAK-DOC)	No	A fire is judged not to induce a pipe or vessel leak or break
CVCS injection line LOCA inside containment (CVCS--ALOCA-IIC)	No	A fire is judged not to induce a pipe or vessel leak or break or LOCA
Spurious opening of an ECCS valve (ECCS--ALOCA-RV1)	Yes	A fire could spuriously operate an ECCS valve.
Loss of DC power (EDAS--LODC)	Yes	A fire could damage electrical distribution equipment in the EDAS that could lead to a LODC
Loss of offsite power (EHVS---LOOP)	Yes	A fire could damage electrical distribution equipment in the EHVS that could lead to a LOOP.
SG tube failure (MSS---ALOCA-SG)	No	A fire is judged not to induce a pipe or vessel leak or break.
LOCA inside containment (-RCS---ALOCA-IC)	Yes	Multiple spurious operations in combination with random failures could lead to a LOCA induced by a CVCS pump operation. Spurious operation of the pressurizer heaters could lead to a small LOCA but is bounded by spurious ECCS operation caused by the same fire.
Secondary line break (TGS---FMSLB-UD)	No	A fire is judged not to induce a pipe or vessel leak or break.
General reactor trip (TGS---TRAN--NPC)	Yes	A fire could result in various failures that manifest as a general reactor trip. For example, a fire could result in the spurious closure of both MSIVs.
Loss of support system (TGS---TRAN-SS)	Yes	A fire could result in various failures that manifest as a loss of a support system. For example, a fire could result in a ground fault to the electrical supply to an EMVS bus that causes a plant trip.

Table 19.1-34: Dominant Cutsets (Internal Fires, Full Power, Single Module)

Cutset	Frequency	Contribution	Description
			CDF Cutsets
1	2.2E-10	5.3	
			Fire Induces Spurious ECCS Actuation - Division I Affected - Room 170 -134
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			FIRE GROWTH - LOOP or Main Control Room
			RCS Reactor Safety Valve Not Demanded to Open
2	2.2E-10	5.1	
			Fire Induces Transient - NPM-01 ELVS BOP PDC
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			FIRE GROWTH - GENERAL
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
3	1.1E-10	2.6	
			Fire Induces Transient - Loss of EMVS Bus
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			FIRE GROWTH - GENERAL
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
4	8.4E-11	2.0	
			Fire Induces Spurious ECCS Actuation - Division I Affected - Room 170 -134
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			FIRE GROWTH - LOOP or Main Control Room
			RCS Reactor Safety Valve Not Demanded to Open
5	8.4E-11	2.0	
			Fire Induces Spurious ECCS Actuation - Division I Affected - Room 170 -134
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			FIRE GROWTH - LOOP or Main Control Room
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-34: Dominant Cutsets (Internal Fires, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
6	8.2E-11	1.9	
			Fire Induces Transient - NPM-01 ELVS BOP PDC
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			FIRE GROWTH - GENERAL
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
7	8.2E-11	1.9	
			Fire Induces Transient - NPM-01 ELVS BOP PDC
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			FIRE GROWTH - GENERAL
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
8	7.1E-11	1.7	
			Fire Induces Spurious ECCS Actuation - Division II Affected - Room 010 -411
			OPERATOR FAILS TO LOCALLY UNISOLATE AND INITIATE CVCS INJECTION
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			FIRE GROWTH - GENERAL
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			MSW 2006X MANUAL DIVISION II ECCS ACTUATE SPURIOUSLY OPERATES DUE TO HOT SHORT
9	6.7E-11	1.6	
			Multi-Compartment Scenario - Fire Spread from 010-206 to 010-307 Induces Loss of DC Div I
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			FIRE GROWTH - GENERAL
10	4.6E-11	1.1	
			Fire Induces Transient - NPM-01 ELVS BOP PDC
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			CBL 3011X1 ELVS MODULE-SPECIFIC CIRCUIT BREAKER FAILS TO CLOSE
			FIRE GROWTH - GENERAL
11	4.6E-11	1.1	
			Fire Induces Transient - NPM-01 ELVS BOP PDC
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			CBL 3011X2 ELVS MODULE-SPECIFIC CIRCUIT BREAKER FAILS TO CLOSE
			FIRE GROWTH - GENERAL

Table 19.1-34: Dominant Cutsets (Internal Fires, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
12	4.6E-11	1.1	
			Fire Induces Transient - NPM-01 ELVS BOP PDC
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			CBL 3021X2 ELVS MODULE-SPECIFIC CIRCUIT BREAKER FAILS TO CLOSE
			FIRE GROWTH - GENERAL
13	4.6E-11	1.1	
			Fire Induces Transient - NPM-01 ELVS BOP PDC
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			CBL 3021X1 ELVS MODULE-SPECIFIC CIRCUIT BREAKER FAILS TO CLOSE
			FIRE GROWTH - GENERAL
LRF Cutsets			
1	8.4E-13	9.6	
			Fire Spuriously Operates CVCS Makeup Pump
			CCF OF 2 OF 2 CNTS CVCS INJECTION LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			FIRE GROWTH - GENERAL
2	8.4E-13	9.6	
			Fire Spuriously Operates CVCS Makeup Pump
			CCF OF 2 OF 2 CNTS CVCS PRESSURIZER SPRAY LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			FIRE GROWTH - GENERAL
3	3.6E-13	4.1	
			Fire Spuriously Operates CVCS Makeup Pump
			GIVEN ACTUATION AT LEAST 2 OF 16 RODS FAIL TO INSERT
			CCF OF 2 OF 2 CNTS CVCS PRESSURIZER SPRAY LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			FIRE GROWTH - GENERAL
4	3.6E-13	4.1	
			Fire Spuriously Operates CVCS Makeup Pump
			GIVEN ACTUATION AT LEAST 2 OF 16 RODS FAIL TO INSERT
			CCF OF 2 OF 2 CNTS CVCS INJECTION LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			FIRE GROWTH - GENERAL

Table 19.1-34: Dominant Cutsets (Internal Fires, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
5	3.2E-13	3.6	
			Fire Spuriously Operates CVCS Makeup Pump
			CCF OF 2 OF 2 CNTS CVCS INJECTION LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			FIRE GROWTH - GENERAL
6	3.2E-13	3.6	
			Fire Spuriously Operates CVCS Makeup Pump
			CCF OF 2 OF 2 CNTS CVCS PRESSURIZER SPRAY LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			FIRE GROWTH - GENERAL
7	3.2E-13	3.6	
			Fire Spuriously Operates CVCS Makeup Pump
			CCF OF 2 OF 2 CNTS CVCS INJECTION LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			FIRE GROWTH - GENERAL
8	3.2E-13	3.6	
			Fire Spuriously Operates CVCS Makeup Pump
			CCF OF 2 OF 2 CNTS CVCS PRESSURIZER SPRAY LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			FIRE GROWTH - GENERAL

Table 19.1-35: Applicability of Internal Initiating Events to Internal Flooding Probabilistic Risk Assessment

Initiating Event	Applicability to Internal Flooding	Evaluation
CVCS injection line LOCA inside containment (CVCS--ALOCA-IIC)	No	Passive components are not susceptible to flood damage; an internal flood does not result in a CVCS injection line loss-of-coolant accident (LOCA) inside the containment vessel (CNV). The CVCS injection line rupture itself causes flooding that is confined to the CNV and is thus not an internal flooding scenario.
CVCS injection line pipe break outside containment (CVCS--BREAK-IOC)	No	Passive components are not susceptible to flood damage. An internal flood does not result in a CVCS injection line LOCA outside the CNV.
CVCS discharge line pipe break outside containment (CVCS--BREAK-DOC)	No	Passive components are not susceptible to flood damage. An internal flood does not result in a CVCS discharge line LOCA 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 and control solenoids are not susceptible to damage from flooding; they are located inside the CNV or submerged in the reactor pool and designed to operate in harsh environments.
Loss of DC power (EDAS---LODC)	No	Although flood-induced damage to the EDAS switchgear could physically result in a loss of two or more EDAS power channels, this event is not considered because internal flood sources were not identified near this equipment and the EDAS equipment are protected from flooding effects.
Loss of offsite power (EHVS---LOOP)	No	Although flood-induced damage to the high voltage AC electrical power distribution system switchgear could physically result in a loss of offsite power, this event is not considered because internal flood sources were not identified near this equipment.
SG tube failure (MSS---ALOCA-SG)	No	Passive components are not susceptible to flood damage; an internal flood does not result in a steam generator tube failure.
RCS LOCA inside containment (RCS---ALOCA-IC)	No	Passive components are not susceptible to flood damage; an internal flood does not result in a reactor coolant system (RCS) LOCA.
Secondary 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 capable of resulting in a general transient. Flood induced failures may realistically result in a reactor trip and subsequent transient.
Loss of support system (TGS---TRAN-SS)	No	The loss of support system initiator is loss of module-specific EMVS AC power. The module-specific EMVS equipment is housed in power distribution centers located outside. There are no flood sources in the power distribution centers. Therefore, an internal flood causing a support system loss is not considered.

Table 19.1-36: External Event Frequencies

External Event (Label)	Description	Frequency (mcyr-1)	Error Factor	Transfers to Internal Event Trees
Internal Flood-RXB (IE-INTNLFLOOD-RXB)	Internal flooding in RXB	1.9 E-2	10	TGS---TRAN--NPC
Internal Flood-outside the RXB (IE-INTNL-FLOOD-OTH)	Internal flooding outside RXB	4.9 E-3	10	TGS---TRAN--NPC
External Flooding (IE-EXTNL-FLOOD-FP)	External flood, once per 500 years	2.0 E-3	10	EHVS-LOOP
High Winds-Tornado (IE-HW--TORNADO)	Tornado EF2 & Above	2.3 E-4	10	EHVS-LOOP
High Winds-Hurricane (IE-HW--HURRICANE)	Hurricane Category 3 & Above	1.7 E-3	10	EHVS-LOOP
Compartment fire	Single compartment fire	2.1 E-1[1]	26	CVCS--BREAK-IOC ECCS-ALOCA-RV1 EDAS--LODC EHVS--LOOP TGS---TRAN--NPC TGS---TRAN--SS
Fire- spurious ECCS actuation (IE-FIRE-4-ECCS-FC-170-134)	Main control room fire	2.1 E-3	32	ECCS-ALOCA-RV1 TGS---TRAN--NPC
Multi-compartment fire	Fire affecting multiple compartments	3.6 E-4[1]	10	CVCS--BREAK-IOC ECCS-ALOCA-RV1 EDAS--LODC TGS---TRAN--NPC
Seismic	Not applicable for SMA			

Notes:

[1] The internal fire frequency listed is the highest of the compartments in that group.

Table 19.1-37: Evaluation of Internal Flooding on Mitigating Systems

Top Event	RXB	TGB and Other Buildings	Evaluation
RTS-T01	None	None	An internal flood does not mechanically challenge the reactor trip system or control rods' ability to insert into the core. The MPS control cabinets are not susceptible to a flood.
DHRS-T01	None	None	The mechanical portions of this system are not susceptible to the effects of internal flooding. The MPS control cabinets (providing power to the DHRS valves) are not susceptible to a flood.
RCS-T05, RCS-T01	None	None	An internal flood has no impact on the demand or operation of the RSVs.
RCS-T06	None	None	An internal flood has no affect the ability of an RSV to reclose.
ECCS-T03	None	None	This is an operator action performed in the control room, which is not susceptible to a flood.
ECCS-T01	None	None	The mechanical portions of the ECCS are not susceptible to the effects of internal flooding. The MPS control cabinets (providing power to the ECCS valves) are not susceptible to a flood.
CVCS-T01	Yes	Yes	Flooding in some areas of the RXB is assumed to challenge the ability of the CVCS makeup pumps. In addition, CVCS can be the source of a flood. The CVCS is assumed to be nominally available following a flood in other buildings, but the DWS is susceptible to flooding from the UWS and PWS, which are located near the DWS. Since DWS provides the long term water source for CVCS, it is assumed that CVCS is lost in a flood outside the RXB; this is a very conservative assumption, the impact of which is investigated in a sensitivity case provided in Table 19.1-22.

Table 19.1-38: Dominant Cutsets (Internal Flooding, Full Power, Single Module)

Cutset	Frequency	Contribution	Description
CDF Cutsets			
1	4.5E-11	30.2	
			Internal Flooding Event in the RXB
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			RCS Reactor Safety Valve Not Demanded to Open
2	1.7E-11	11.4	
			Internal Flooding Event in the RXB
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			RCS Reactor Safety Valve Not Demanded to Open
3	1.7E-11	11.4	
			Internal Flooding Event in the RXB
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			RCS Reactor Safety Valve Not Demanded to Open
4	1.2E-11	7.8	
			Internal Flooding Event Outside the RXB
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			RCS Reactor Safety Valve Not Demanded to Open
5	4.4E-12	2.9	
			Internal Flooding Event Outside the RXB
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			RCS Reactor Safety Valve Not Demanded to Open
6	4.4E-12	2.9	
			Internal Flooding Event Outside the RXB
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-38: Dominant Cutsets (Internal Flooding, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
7	4.2E-12	2.8	
			Internal Flooding Event in the RXB
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 2 APL MODULES IN ECCS REACTOR VENT VALVES FAILS TO OPERATE
			RCS Reactor Safety Valve Not Demanded to Open
8	3.8E-12	2.6	
			Internal Flooding Event in the RXB
			GIVEN ACTUATION AT LEAST 2 OF 16 RODS FAIL TO INSERT
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
9	3.4E-12	2.3	
			Internal Flooding Event in the RXB
			CCF OF 4 OF 4 DHRS ACTUATION VALVES FAIL TO OPEN
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
10	1.6E-12	1.1	
			Internal Flooding Event in the RXB
			DHRS TRAINS FAIL DUE TO THERMAL HYDRAULIC PROBLEMS
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
11	1.5E-12	1.0	
			Internal Flooding Event in the RXB
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			CCF OF 3 OF 4 PRESSURIZER PRESSURE PROCESS LOGIC ELEMENTS
LRF Cutsets			
1	3.1E-15	51.0	
			Internal Flooding Event in the RXB
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			OPERATOR FAILS TO OPEN ECCS VALVES
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			CCF OF 2 OF 3 DIVISION I ESFAS SCHEDULING AND VOTING MODULES
			CCF OF 2 OF 3 DIVISION II ESFAS SCHEDULING AND VOTING MODULES

Table 19.1-38: Dominant Cutsets (Internal Flooding, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
2	1.5E-15	24.5	
			Internal Flooding Event in the RXB
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			RCS Reactor Safety Valve Not Demanded to Open
3	1.5E-15	24.5	
			Internal Flooding Event in the RXB
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-39: Applicability of Internal Initiating Events to External Flooding Probabilistic Risk Assessment

Internal Event PRA Initiating Event	Applicability to External Flood PRA	Comments
CVCS Injection Line LOCA Inside Containment (CVCS--ALOCA-IIC)	No	Passive components are not susceptible to flood damage; an external flood does not result in a LOCA inside containment.
CVCS Injection Line Break Outside Containment (CVCS--BREAK-IOC)	No	Passive components are not susceptible to flood damage; an external flood does not result in a pipe break outside containment.
CVCS Discharge Line Break Outside Containment (CVCS--BREAK-DOC)	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	External flooding does not result in spurious operation of an ECCS valve. If power is lost to an ECCS solenoid operated valve, an ECCS actuation occurs; the LOOP event tree captures the loss of power and de-energization of ECCS solenoid valves.
Loss of DC Power (EDAS--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.
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--SS)	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 19.1-40: Evaluation of External Flooding Impact

System Top Event[1]	Flooding Susceptibility	Comments
BPSS-T01, BDGs	Yes	An external flood is expected to penetrate BDG structures, and preclude the ability to use the BDGs as a backup power source
RTS-T01, Reactor trip system	No[2]	The design and location of the reactor trip breakers and control rods precludes flooding susceptibility.
DHRS-T01, DHRS	No[2]	The design and location of DHRS components precludes flooding susceptibility.
RCS-T05, RCS-T01, RCS-T06 Reactor safety valve opens/closes	No	The design and location of the reactor safety valves (RSVs) precludes flooding susceptibility.
ECCS-T03, Operations confirms shutdown margin & bypasses 8 hour ECCS timer	Yes[2]	An external flood is expected to penetrate the CRB, and preclude the ability of the operators to take mitigating actions
EHVS-T02, Offsite power recovered	Yes	An external flood is expected to preclude the ability to recover offsite power.
ECCS-T01, ECCS	No[2]	The design and location of ECCS components precludes flooding susceptibility.
CVCS-T01, CVCS for reactor coolant system (RCS) injection	Yes	An external flood is expected to penetrate the RXB and prohibit the use of CVCS for makeup injection. The loss of AC power also prohibits use of the CVCS makeup pumps.
CNTS-T01, Containment isolation	No[2]	The design and location of the CIVs precludes flooding susceptibility

Notes:

1. Top events listed are from the LOOP event tree, except CNTS-T01, which is in the Level 2 event tree.
2. An external flood is postulated to result in a loss of AC and DC power, which results in safety system actuation

Table 19.1-41: Dominant Cutsets (External Flooding, Full Power, Single Module)

Cutset	Frequency	Contribution	Description
CDF Cutsets			
1	2.2E-09	24.4	
			External Flood Initiator
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			External Flood Results in LOOP
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
2	2.2E-09	24.4	
			External Flood Initiator
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			External Flood Results in LOOP
			RCS Reactor Safety Valve Not Demanded to Open
3	8.2E-10	9.2	
			External Flood Initiator
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			External Flood Results in LOOP
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
4	8.2E-10	9.2	
			External Flood Initiator
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			External Flood Results in LOOP
			RCS Reactor Safety Valve Not Demanded to Open
5	8.2E-10	9.2	
			External Flood Initiator
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			External Flood Results in LOOP
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
6	8.2E-10	9.2	
			External Flood Initiator
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			External Flood Results in LOOP
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-41: Dominant Cutsets (External Flooding, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
7	2.0E-10	2.3	
			External Flood Initiator
			External Flood Results in LOOP
			CCF OF 2 OF 2 APL MODULES IN ECCS REACTOR VENT VALVES FAILS TO OPERATE
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
8	2.0E-10	2.3	
			External Flood Initiator
			External Flood Results in LOOP
			CCF OF 2 OF 2 APL MODULES IN ECCS REACTOR VENT VALVES FAILS TO OPERATE
			RCS Reactor Safety Valve Not Demanded to Open
			LRF Cutsets
1	7.1E-14	7.8	
			External Flood Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			External Flood Results in LOOP
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
2	7.1E-14	7.8	
			External Flood Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			External Flood Results in LOOP
			RCS Reactor Safety Valve Not Demanded to Open
3	7.1E-14	7.8	
			External Flood Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			External Flood Results in LOOP
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN

Table 19.1-41: Dominant Cutsets (External Flooding, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
4	7.1E-14	7.8	
			External Flood Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			External Flood Results in LOOP
			RCS Reactor Safety Valve Not Demanded to Open
5	5.4E-14	6.0	
			External Flood Initiator
			External Flood Results in LOOP
			CCF OF 2 OF 3 DIVISION I ESFAS SCHEDULING AND VOTING MODULES
			CCF OF 2 OF 3 DIVISION II ESFAS SCHEDULING AND VOTING MODULES
6	4.0E-14	4.4	
			External Flood Initiator
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			External Flood Results in LOOP
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
			CCF OF 3 OF 4 RCS PRESSURIZER LEVEL SENSORS FAIL TO OPERATE ON DEMAND
7	4.0E-14	4.4	
			External Flood Initiator
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			External Flood Results in LOOP
			CCF OF 3 OF 4 RCS PRESSURIZER LEVEL SENSORS FAIL TO OPERATE ON DEMAND
			RCS Reactor Safety Valve Not Demanded to Open
8	3.1E-14	3.4	
			External Flood Initiator
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			External Flood Results in LOOP
			CCF OF 3 OF 4 PRESSURIZER LEVEL PROCESS LOGIC ELEMENTS
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-41: Dominant Cutsets (External Flooding, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
9	3.1E-14	3.4	
			External Flood Initiator
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			External Flood Results in LOOP
			CCF OF 3 OF 4 PRESSURIZER LEVEL PROCESS LOGIC ELEMENTS
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
10	2.7E-14	3.0	
			External Flood Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			External Flood Results in LOOP
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
11	2.7E-14	3.0	
			External Flood Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			External Flood Results in LOOP
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
12	2.7E-14	3.0	
			External Flood Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			External Flood Results in LOOP
			RCS Reactor Safety Valve Not Demanded to Open
13	2.7E-14	3.0	
			External Flood Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			External Flood Results in LOOP
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-41: Dominant Cutsets (External Flooding, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
14	2.7E-14	3.0	
			External Flood Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			External Flood Results in LOOP
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
15	2.7E-14	3.0	
			External Flood Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			External Flood Results in LOOP
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
16	2.7E-14	3.0	
			External Flood Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			External Flood Results in LOOP
			RCS Reactor Safety Valve Not Demanded to Open
17	2.7E-14	3.0	
			External Flood Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			External Flood Results in LOOP
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-42: Applicability of Internal Initiating Events to High-Winds Probabilistic Risk Assessment

Initiating Event	Applicability to HW PRA	Comments
CVCS Injection Line LOCA Inside Containment (CVCS--ALOCA-IIC)	No	The CVCS injection lines (and ECCS reset lines) are located inside the CNV and, therefore, are protected; high winds do not result in a LOCA inside containment.
CVCS Injection Line Break Outside Containment (CVCS--BREAK-IOC)	No	A high-winds induced break of a CVCS injection line outside containment is unlikely and readily mitigated by closure of either safety-related CIVs. Therefore, wind-induced CVCS injection line breaks were screened.
CVCS Discharge Line Break Outside Containment (CVCS--BREAK-DOC)	No	A high-winds induced break of the CVCS discharge line outside containment is unlikely and readily mitigated by closure of either safety-related CIVs. Therefore, a wind-induced CVCS discharge line break was screened.
Spurious Opening of an ECCS Valve ((ECCS--ALOCA-RV1))	No	The ECCS valves are safety-related and protected from the possibility of high winds causing a spurious ECCS actuation.
Loss of DC Power (EDAS--LODC)	Bounded by LOOP	A high-wind induced loss of DC power is unlikely based on the location of equipment within the RXB. A loss of DC power, due to a loss of AC power, is bounded by the LOOP evaluation.
Loss Of Offsite Power (EHVS--LOOP)	Yes	High winds are assumed to result in a LOOP.
SGTF (MSS---ALOCA-SG)	No	Reactor coolant system components are integral to the RPV and therefore protected from high winds.
LOCA Inside Containment (RCS---ALOCA-IC)	No	Reactor coolant system components and lines are located inside the RPV or the CNV and therefore protected from high winds.
Secondary Side Line Break (TGS---FMSLB-UD)	No	A high-winds induced break of a feedwater or main steam line outside containment is unlikely and readily mitigated by closure of either the safety-related CIV or the secondary isolation valve. Therefore, wind-induced feedwater or main steam line breaks were screened.
General Reactor Trip (TGS---TRAN--NPC)	Bounded by LOOP	A high-wind induced reactor trip is bounded by the LOOP evaluation. The accident progression following a reactor trip is identical to that following a LOOP when not crediting AC power.
Loss of Support System (TGS---TRAN--SSS)	Bounded by LOOP	A high-wind induced support system loss is bounded by the LOOP evaluation. The accident progression following a trip is identical to that following a LOOP when not crediting AC power.

Table 19.1-43: 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.	Significant wind and missile damage to the structure and to SSC within the structure.
EF5	5	Superficial damage to outer walls.	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 19.1-44: Dominant Cutsets (Hurricanes, Full Power, Single Module)

Cutset	Frequency	Contribution	Description
			CDF Cutsets
1	4.4E-09	24.1	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
2	4.4E-09	24.1	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
3	1.7E-09	9.1	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
4	1.7E-09	9.1	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
5	1.7E-09	9.1	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
6	1.7E-09	9.1	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN

Table 19.1-44: Dominant Cutsets (Hurricanes, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
7	4.1E-10	2.3	
			High Winds Hurricane Category 3 & Above Initiator
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			CCF OF 2 OF 2 APL MODULES IN ECCS REACTOR VENT VALVES FAILS TO OPERATE
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
8	4.1E-10	2.3	
			High Winds Hurricane Category 3 & Above Initiator
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			CCF OF 2 OF 2 APL MODULES IN ECCS REACTOR VENT VALVES FAILS TO OPERATE
			RCS Reactor Safety Valve Not Demanded to Open
LRF Cutsets			
1	1.5E-13	11.6	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFFSITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
2	1.5E-13	11.6	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFFSITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
3	1.5E-13	11.6	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFFSITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-44: Dominant Cutsets (Hurricanes, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
4	1.5E-13	11.6	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFFSITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
5	5.5E-14	4.4	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OFFSITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
6	5.5E-14	4.4	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OFFSITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
7	5.5E-14	4.4	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OFFSITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
8	5.5E-14	4.4	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OFFSITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN

Table 19.1-44: Dominant Cutsets (Hurricanes, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
9	5.5E-14	4.4	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OFFSITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
10	5.5E-14	4.4	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OFFSITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
11	5.5E-14	4.4	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OFFSITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
12	5.5E-14	4.4	
			High Winds Hurricane Category 3 & Above Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OFFSITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN

Table 19.1-45: Dominant Cutsets (Tornadoes, Full Power, Single Module)

Cutset	Frequency	Contribution	Description
CDF Cutsets			
1	6.1E-10	24.1	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
2	6.1E-10	24.1	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
3	2.3E-10	9.11	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
4	2.3E-10	9.11	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
5	2.3E-10	9.11	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
6	2.3E-10	9.11	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN

Table 19.1-45: Dominant Cutsets (Tornadoes, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
7	5.7E-11	2.25	
			High Winds Tornado EF2 & Above Initiator
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			CCF OF 2 OF 2 APL MODULES IN ECCS REACTOR VENT VALVES FAILS TO OPERATE
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
8	5.7E-11	2.25	
			High Winds Tornado EF2 & Above Initiator
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			CCF OF 2 OF 2 APL MODULES IN ECCS REACTOR VENT VALVES FAILS TO OPERATE
			RCS Reactor Safety Valve Not Demanded to Open
LRF Cutsets			
1	2.0E-14	13.1	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
2	2.0E-14	13.1	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
3	2.0E-14	13.1	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-45: Dominant Cutsets (Tornadoes, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
4	2.0E-14	13.1	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
5	7.5E-15	4.9	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
6	7.5E-15	4.9	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
7	7.5E-15	4.9	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
8	7.5E-15	4.9	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN

Table 19.1-45: Dominant Cutsets (Tornadoes, Full Power, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
9	7.5E-15	4.9	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
10	7.5E-15	4.9	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			RCS Reactor Safety Valve Not Demanded to Open
11	7.5E-15	4.9	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
12	7.5E-15	4.9	
			High Winds Tornado EF2 & Above Initiator
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS (HIGH WINDS)
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN

Table 19.1-46: Plant Operating States for Low Power and Shutdown Probabilistic Risk Assessment

POS	Description	Time Entering POS (hours after shutdown)	NPM Configuration Entering POS	Time Exiting POS (hours after shutdown)	NPM Configuration Exiting POS	Duration (hours)
1	Shutdown and initial cooling	0.0	Control rods inserted and NPM subcritical	6.0	CNV flood complete	6.0
2	Cooling through containment	6.0	CNV flood complete	47.5	NPM lifted by RBC	41.5
3	Transport to refueling pool	47.5	NPM lifted by RBC	53.5	Upper NPM moved to dry dock	6.0
3	Transport to operating bay	186.0	Upper NPM moved out of dry dock	189.0	NPM placed in operating bay	3.0
4	Disassembly, refueling, and reassembly	53.5	Upper NPM moved to dry dock	186.0	Upper NPM moved out of dry dock	132.5
5	Reconnection	189.0	NPM placed in operating bay	229.5	CNV drain begins	40.5
6	Heatup	229.5	CNV drain begins	244.5	Control rods withdrawn to criticality	15.0
7	Low power operation	244.5	Control rods withdrawn to criticality	245.5	Turbine synchronized with grid	1.0

Table 19.1-47: Applicability of Internal Initiating Events to Low Power and Shutdown Probabilistic Risk Assessment

Full Power Initiating Event	Applicability to Low Power and Shutdown	Evaluation
CVCS Injection Line LOCA Inside Containment (CVCS--ALOCA-IIC)	POS1, POS2, POS5, POS6, POS7	This initiating event is applicable to POSs in which CVCS is operating and the ECCS valves are closed (POS1, POS2, POS5, POS6, POS7) and not applicable when the NPM is disconnected from CVCS piping (POS3, POS4)
CVCS Injection Line Break Outside Containment (CVCS--BREAK-IOC)	POS1, POS2, POS5, POS6, POS7	
CVCS Discharge Line Break Outside Containment (CVCS--BREAK-DOC)	POS1, POS2, POS5, POS6, POS7	
Spurious Opening of an ECCS Valve (ECCS--ALOCA-RV1)	POS1, POS6, POS7	This initiating event is applicable when the ECCS valves are closed and containment is not flooded (POS1, POS6, POS7). In POS2 and POS5, the ECCS valves are closed for a portion of the POS, however the containment is flooded and a spurious ECCS valve opening will not cause a loss of coolant to containment. In POS3 and POS4, the ECCS valves are open.
Loss of DC Power (EDAS--LODC)	POS1, POS6, POS7	
Loss Of Offsite Power (EHVS--LOOP)	POS1, POS6, POS7	This initiating event causes a loss of normal secondary cooling by removing power to the pumps in the feedwater system and is applicable when normal secondary cooling is active (POS1, POS6, POS7). In POS2 and POS5, decay heat is passively conducted to the reactor pool through the flooded containment. In POS3, a loss of power is modeled as a contributor to RBC failure and NPM drop, therefore it is not included for POS3. In POS4, the NPM is disconnected from power.
Steam Generator Tube Failure (MSS---ALOCA-SG)	POS1, POS6, POS7	
LOCA Inside Containment (RCS---ALOCA-IC)	POS1, POS6, POS7	This initiating event is applicable when the NPM is in its operating bay, the reactor coolant pressure boundary is intact, and containment is not flooded (POS1, POS6, POS7). In POS2 and POS5 the containment is flooded, precluding a LOCA into containment. In POS3 and POS4, the ECCS valves are open.
Secondary Side Line Break (TGS---FMSLB-UD)	POS1, POS6, POS7	This initiating event causes a loss of normal secondary cooling by removing power to the pumps in the feedwater system and is applicable when normal secondary cooling is active (POS1, POS6, POS7). In POS2 and POS5, decay heat is passively conducted to the reactor pool through the flooded containment. In POS3, a loss of power is modeled as a contributor to RBC failure and NPM drop, therefore it is not included for POS3. In POS4, the NPM is disconnected from power.
General Reactor Trip (TGS---TRAN--NPC)	POS1, POS6, POS7	
Loss of Support System (TGS---TRAN--SS-)	POS1, POS6, POS7	

Table 19.1-48: Module Drop Upset Events and Mitigating Features

Type	Upset Events[1]	Detections	Mitigations
Load hangup	• Bridge position error • Trolley position error • Hoist position error	• Hoist weigh system • Operator action (visual detection)	• Bridge brakes • Trolley brakes • Hoist brakes
Two-blocking	• Hoist position error	• Upper geared limit switches (2) • Ultimate upper limit switch • Hoist weigh system • Operator action (visual detection)	• Hoist brakes
Slack rope	• Hoist position error	• Lower geared limit switches (2) • Hoist weigh system • Operator action (visual detection)	• Hoist brakes
Hoist overspeed	• Hoist motor fault	• Overspeed switches • Operator action (visual detection)	• Hoist brakes
Mis-spooling	• Bridge position error • Trolley position error • Drum groove mechanical damage	• Mis-spooling switches • Operator action (visual detection)	• Hoist brakes
Loss of power	• Electrical bus failure • Loss of off-site power	• Guaranteed based on the upset	• Hoist brakes
Load path failure	• Wire rope failure • Hoist gearbox failure	• n/a	• None

Notes:

1.The term “upset event” is used in this analysis to distinguish disruptions to RBC operation from initiating events used in other PRA analyses.

Table 19.1-49: Low Power and Shutdown Initiator Frequencies

Initiator	Description	Frequency (per mcyr)	Error Factor	Transfers to Internal Event Tree
IE3-RBC---DROP	RBC Failure and NPM Drop - POS3	3.5 E-8	10	N/A
IE2CVCS--ALOCA-IIC	CVCS LOCA Injection Line Inside Containment - POS2	1.3 E-6[1]	10	CVCS--ALOCA-IIC
IE2CVCS--BREAK-DOC	CVCS Break Discharge Line Outside Containment - POS2	7.9 E-9[1]	10	CVCS--BREAK-DOC
IE2CVCS--BREAK-IOC	CVCS Break Injection Line Outside Containment - POS2	5.4 E-8[1]	10	CVCS--BREAK-IOC
IE6ECCS--ALOCA-RV1	Spurious Opening of an ECCS Valve - POS6	1.1 E-6[2]	10	ECCS-ALOCA-RV1
IE6EDAS--LODC	Loss of DC Power - POS6	3.0 E-7[2]	10	EDAS--LODC
IE6EHVS--LOOP	Loss of Offsite Power - POS6	2.9 E- 5[2]	10	EHVS--LOOP
IE6MSS---ALOCA-SG	Steam Generator #2 Tube Failure - POS6	5.3 E-8[2]	10	MSS---ALOCA-SG
IE6RCS---ALOCA-IC	LOCA Inside Containment - POS6	1.5 E-6[2]	10	RCS---ALOCA-IC
IE6TGS---FMSLB-UD	Secondary Side Line Break - POS6	5.0 E-8[2]	10	TGS---FMSLB-UD
IE6TGS---TRAN--NPC	General Reactor Trip - POS6	6.6 E-4[2]	10	TGS---TRAN--NPC
IE6TGS---TRAN--SS	Loss of Support System - POS6	5.9 E- 6[2]	10	TGS---TRAN--SS

Notes:

1. The initiator with the highest frequency is listed: similar initiators (e.g., IE1CVCS--ALOCA-IIC, IE5CVCS--ALOCA-IIC) are considered for POS1, POS5, POS6, and POS7.
2. The initiator with the highest frequency is listed: similar initiators (e.g., IE1ECCS--ALOCA-RV1, IE7ECCS--ALOCA-RV1) are considered for POS1 and POS7.

Table 19.1-50: Dominant Cutsets (Low Power and Shutdown, Single Module)

Cutset	Frequency	Contribution	Description
CDF Cutsets			
1	2.5E-12	7.5	
			Loss Of Offsite Power - POS6
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
2	1.8E-12	5.2	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
3	1.4E-12	4.2	
			Loss Of Offsite Power - POS6
			CCF OF 2 OF 2 BPSS BACKUP DIESEL GENERATORS FAIL TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
4	9.8E-13	2.9	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO START
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
5	9.8E-13	2.9	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO START
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
6	9.5E-13	2.8	
			Loss Of Offsite Power - POS1
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET

Table 19.1-50: Dominant Cutsets (Low Power and Shutdown, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
7	9.5E-13	2.8	
			Loss Of Offsite Power - POS6
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
8	9.5E-13	2.8	
			Loss Of Offsite Power - POS6
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
9	6.7E-13	2.0	
			Loss Of Offsite Power - POS1
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
10	6.6E-13	2.0	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
11	6.6E-13	2.0	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
12	5.4E-13	1.6	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO START
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO START
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN

Table 19.1-50: Dominant Cutsets (Low Power and Shutdown, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
13	5.4E-13	1.6	
			Loss Of Offsite Power - POS1
			CCF OF 2 OF 2 BPSS BACKUP DIESEL GENERATORS FAIL TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
14	5.3E-13	1.6	
			Loss Of Offsite Power - POS6
			CCF OF 2 OF 2 BPSS BACKUP DIESEL GENERATORS FAIL TO RUN (48 HOURS)
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
15	5.3E-13	1.6	
			Loss Of Offsite Power - POS6
			CCF OF 2 OF 2 BPSS BACKUP DIESEL GENERATORS FAIL TO RUN (48 HOURS)
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
16	5.1E-13	1.5	
			Loss of Support System - POS6
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
17	5.0E-13	1.5	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR UNAVAILABLE DUE TO TEST AND MAINTENANCE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
18	5.0E-13	1.5	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR UNAVAILABLE DUE TO TEST AND MAINTENANCE
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
19	4.9E-13	1.5	
			Loss Of Offsite Power - POS6
			CCF OF 2 OF 2 BPSS BACKUP DIESEL GENERATORS FAIL TO START
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN

Table 19.1-50: Dominant Cutsets (Low Power and Shutdown, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
20	3.7E-13	1.1	
			Loss Of Offsite Power - POS1
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO START
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
21	3.7E-13	1.1	
			Loss Of Offsite Power - POS1
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO START
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
22	3.7E-13	1.1	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO START
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
23	3.7E-13	1.1	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO START
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
24	3.7E-13	1.1	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO START
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
25	3.7E-13	1.1	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO START
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN

Table 19.1-50: Dominant Cutsets (Low Power and Shutdown, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
26	3.6E-13	1.1	
			Loss Of Offsite Power - POS1
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
27	3.6E-13	1.1	
			Loss Of Offsite Power - POS1
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
LRF Cutsets			
1	3.8E-13	11.5	
			Loss Of Offsite Power - POS6
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
2	1.6E-13	4.9	
			Loss Of Offsite Power - POS6
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			OPERATOR FAILS TO OPEN ECCS VALVES
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR THIRD HFE IN CUTSET
			CCF OF 3 OF 4 RCS RPV LEVEL SENSORS FAIL TO OPERATE ON DEMAND

Table 19.1-50: Dominant Cutsets (Low Power and Shutdown, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
3	1.4E-13	4.4	
			Loss Of Offsite Power - POS1
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
4	1.4E-13	4.4	
			Loss Of Offsite Power - POS6
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
5	1.4E-13	4.4	
			Loss Of Offsite Power - POS6
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
6	1.2E-13	3.8	
			Loss Of Offsite Power - POS6
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			OPERATOR FAILS TO OPEN ECCS VALVES
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR THIRD HFE IN CUTSET
			CCF OF 3 OF 4 RPV LEVEL PROCESS LOGIC ELEMENTS

Table 19.1-50: Dominant Cutsets (Low Power and Shutdown, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
7	7.7E-14	2.3	
			Loss of Support System - POS6
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
8	6.4E-14	2.0	
			Loss Of Offsite Power - POS6
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			SGT 0201X SGS SG2 TEMPERATURE INDUCED STEAM GENERATOR TUBE FAILURE
9	6.4E-14	2.0	
			Loss Of Offsite Power - POS6
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			SGT 0101X SGS SG1 TEMPERATURE INDUCED STEAM GENERATOR TUBE FAILURE
10	6.1E-14	1.9	
			Loss Of Offsite Power - POS1
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			OPERATOR FAILS TO OPEN ECCS VALVES
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR THIRD HFE IN CUTSET
			CCF OF 3 OF 4 RCS RPV LEVEL SENSORS FAIL TO OPERATE ON DEMAND

Table 19.1-50: Dominant Cutsets (Low Power and Shutdown, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
11	5.4E-14	1.7	
			Loss Of Offsite Power - POS1
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
12	5.4E-14	1.7	
			Loss Of Offsite Power - POS1
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
13	4.7E-14	1.4	
			Loss Of Offsite Power - POS1
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			OPERATOR FAILS TO OPEN ECCS VALVES
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR THIRD HFE IN CUTSET
			CCF OF 3 OF 4 RPV LEVEL PROCESS LOGIC ELEMENTS
14	4.5E-14	1.4	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			SGT 0101X SGS SG1 TEMPERATURE INDUCED STEAM GENERATOR TUBE FAILURE

Table 19.1-50: Dominant Cutsets (Low Power and Shutdown, Single Module) (Continued)

Cutset	Frequency	Contribution	Description
15	4.5E-14	1.4	
			Loss Of Offsite Power - POS6
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			SGT 0201X SGS SG2 TEMPERATURE INDUCED STEAM GENERATOR TUBE FAILURE
16	3.6E-14	1.1	
			Loss Of Offsite Power - POS6
			CCF OF 2 OF 2 BPSS BACKUP DIESEL GENERATORS FAIL TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			SGT 0201X SGS SG2 TEMPERATURE INDUCED STEAM GENERATOR TUBE FAILURE
17	3.6E-14	1.1	
			Loss Of Offsite Power - POS6
			CCF OF 2 OF 2 BPSS BACKUP DIESEL GENERATORS FAIL TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			SGT 0101X SGS SG1 TEMPERATURE INDUCED STEAM GENERATOR TUBE FAILURE
18	3.5E-14	1.1	
			Loss Of Offsite Power - POS6
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			CCF OF 2 OF 2 APL MODULES IN ECCS REACTOR VENT VALVES FAILS TO OPERATE
19	3.3E-14	1.0	
			Loss of Support System - POS6
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			OPERATOR FAILS TO OPEN ECCS VALVES
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR THIRD HFE IN CUTSET
			CCF OF 3 OF 4 RCS RPV LEVEL SENSORS FAIL TO OPERATE ON DEMAND

Table 19.1-51: Internal Fire Susceptibility During Low Power and Shutdown Plant Operating States

Plant Operating State	Internal Fire Susceptibility
POS1	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 temperature. Fires are not expected to be capable of causing the spurious operations of the CVCS makeup pump and the valves providing low temperature overpressure protection in the same fire compartments.
POS2	Once the ECCS is actuated, reclosing the valves to terminate passive cooling requires the spurious operation of two solenoid valves for each of the ECCS valves and 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	An internal fire event may result in a loss of power to the reactor building crane; however the crane is designed to fail safe on a loss of power or failure of communication or control components, applying the brakes and holding the NPM in position.
POS4	In this POS all decay heat is being removed by the UHS and accordingly there is no impact from an internal fire during this POS.
POS5	Once the ECCS is actuated, reclosing the valves to terminate passive cooling requires the spurious operation of two solenoid valves for each of the ECCS valves and 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.
POS6	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 low temperature overpressure protection in the same fire compartments.
POS7	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 19.1-52: Internal Flooding Susceptibility During Low Power and Shutdown Plant Operating States

Plant Operating State	Internal Flooding Susceptibility
POS1	The plant response in this POS is essentially the same as that when the NPM is at power, but the duration is much less. The electrical equipment modeled in the PRA is not susceptible to flooding damage. If the secondary systems were affected by an internal flood, the DHRS, which is unaffected by flooding, would be available to remove decay heat and bring the NPM to safe shutdown. The ECCS, which is also not affected by flooding, would be available as an additional decay heat means. Therefore, internal flooding impacts are not considered in POS1.
POS2	There is no impact from an internal flood during this POS; the NPM can be maintained in POS2 indefinitely without electric power or operator action, and SSC that support core cooling are not susceptible to flooding hazards.
POS3	In the event that an internal flooding event resulted in a loss of power to the crane, the crane is designed with redundant brakes that fail in a safe position on a loss of power. Because of the limited duration in this POS, the low probability of a randomly induced internal flood, the small chance it could interrupt power to the crane, and the redundant fail-safe crane braking system, internal floods were not considered during POS3.
POS4	In this POS, all decay heat is being removed by the UHS. As such, there is no impact from an internal flood during this POS. The NPM can be maintained in POS4 indefinitely without electric power or operator action, and SSC that support core cooling are not susceptible to flooding hazards.
POS5	Similar to POS2, there is no impact from an internal flood during this POS; the NPM can be maintained in this POS indefinitely without electric power or operator action, and SSCs that support core cooling are not susceptible to flooding hazards.
POS6	Similar to POS1, the plant response in this POS is essentially the same as that when the NPM is at power. With the control rods inserted, the impacts from an internal flood would be limited to delaying heatup. Secondary cooling can be provided by the passive DHRS, which is not susceptible to internal flooding. Therefore, internal floods were not considered during POS6.
POS7	Similar to POS1 and POS6, the plant response in this POS is essentially the same as that when the NPM is at power, but the duration is much less. The electrical equipment modeled in the PRA are not susceptible to flooding damage. If the secondary system were affected by an internal flood, the DHRS, which is unaffected by flooding, would be available to remove decay heat and bring the NPM to safe shutdown. The ECCS, which is also not affected by flooding, would available as an additional decay heat means. Therefore, internal flooding impacts are not considered in POS7.

Table 19.1-53: External Flooding Susceptibility During Low Power and Shutdown Plant Operating States

Plant Operating State	External Flooding Susceptibility
POS1	The plant response in this POS is essentially the same as that when the NPM is at power, however, the duration is much shorter. Operators can also place the NPM in a safe condition given warning time. If the NPM cannot be cooled down to POS2 before equipment is susceptible to flood-induced failure, cooling can be provided by the passive DHRS, or ECCS if actuated. Further, the loss of power will result in an ECCS actuation; the loss of power will cause MPS actuation by removing power (i.e., MPS supplies power to maintain the solenoids in their nonactuated state), and cooling can be provided by passive natural circulation to cold conditions. Therefore, external flooding impacts are not considered in POS1.
POS2	There is no impact from external flooding during this POS; decay heat is passively conducted through the flooded CNV to the reactor pool. The NPM can be maintained in POS2 indefinitely without electric power or operator action, and SSC that support core cooling are not susceptible to flooding hazards.
POS3	There is some chance external flooding could result in a loss of power to the crane; however the crane is designed with redundant brakes that fail to a safe position on a loss of power. The NPM can be maintained in position suspended by the RBC until power is restored. Because of the limited duration in this POS, the low probability of external flooding, and the redundant fail-safe crane braking system, external floods are not considered during POS3.
POS4	In this POS, all decay heat is being removed by the ultimate heat sink. As such, there is no impact from external flooding during this POS. The NPM can be maintained in POS4 indefinitely without electric power or operator action, and SSC that support core cooling are not susceptible to flooding hazards.
POS5	Similar to POS2, there is no impact from external flooding during this POS; decay heat is passively conducted through the flooded CNV to the reactor pool. The NPM can be maintained in POS5 indefinitely without electric power or operation action, and SSC that support core cooling are not susceptible to flooding hazards.
POS6	Although the plant response in this POS is similar to that when the NPM is at power, with the control rods inserted, the impact from external flooding is limited to delaying heatup. Secondary cooling can also be provided by the passive DHRS. Therefore, external flooding impacts are not considered in POS6.
POS7	Similar to POS1, the plant response in this POS is essentially the same as that when the NPM is at power however, the duration is much shorter. Operators can also place the NPM in a safe condition given warning time. If the NPM cannot be cooled down to POS2 before equipment is susceptible to flood-induced failure, cooling can be provided by the passive DHRS, or ECCS if actuated. Further, the loss of power will result in an ECCS actuation; the loss of power will cause MPS actuation by removing power (i.e., MPS supplies power to maintain the solenoids in their nonactuated state), and cooling can be provided by passive natural circulation to cold conditions. Therefore, external flooding impacts are not considered in POS7.

Table 19.1-54: High-Wind Susceptibility during Low Power and Shutdown Plant Operating States

Plant Operating State	Tornado and Hurricane Susceptibility
POS1	The plant response in this POS is essentially the same as that when the NPM is at power, however, the duration is much shorter. Operators can also place the NPM in a safe condition given warning time. If the NPM cannot be cooled down to POS2 before equipment is susceptible to high-wind-induced failure, cooling can be provided by the passive DHRS, or ECCS if actuated. Further, if power is not recovered within 24 hours, ECCS will actuate; the loss of power will cause MPS actuation by removing power (i.e., MPS supplies power to maintain the solenoids in their nonactuated state), and cooling can be provided by passive natural circulation to cold conditions. Therefore, high-wind impacts are not considered in POS1.
POS2	There is no impact from high-wind events during this POS; the NPM can be maintained in POS2 indefinitely without electric power or operator action, and SSCs that support core cooling are not susceptible to high winds.
POS3	There is some chance high winds could result in a loss of power to the crane; however the crane is designed with redundant brakes that fail in a safe position on a loss of power. The NPM can be maintained in position suspended by the RBC until power is restored. Because of the limited duration in this POS, the low probability of a high-winds event, and the redundant fail-safe crane braking system, high-wind events are not considered during POS3.
POS4	In this POS, all decay heat is being removed by the UHS. As such, there is no impact from high winds during this POS. The NPM can be maintained in POS4 indefinitely without electric power or operator action, and SSCs that support core cooling are not susceptible to high winds.
POS5	Similar to POS2, there is no impact from high winds during this POS; the NPM can be maintained in POS5 indefinitely without electric power or operation action, and SSCs that support core cooling are not susceptible to high wind hazards.
POS6	Although the plant response in this POS is similar to that when the NPM is at power, with the control rods inserted, the impact from high winds is limited to delaying heatup. Secondary cooling can also be provided by the passive DHRS. Therefore, high-wind impacts are not considered in POS6.
POS7	Similar to POS1, the plant response in this POS is essentially the same as that when the NPM is at power, however, the duration is much shorter. Operators can also place the NPM in a safe condition given warning time. If the NPM cannot be cooled down to POS2 before equipment is susceptible to high-wind-induced failure, cooling can be provided by the passive DHRS, or ECCS if actuated. Further, if power is not recovered within 24 hours, ECCS will actuate; the loss of power will cause MPS actuation by removing power (i.e., MPS supplies power to maintain the solenoids in their nonactuated state), and cooling can be provided by passive natural circulation to cold conditions. Therefore, high-wind impacts are not considered in POS7.

Table 19.1-55: Shared System Hazard Analysis

System	Multiple Module Function	Accident Mitigation Implication	Included in Base Model for Single NPM
Boron addition system (BAS)	Described in Section 9.3	Reactivity control is provided by two independent systems, movable control rod assemblies and boron in the RCS. In the PRA, the module specific reactor trip system and control rods are considered for reactivity control. The BAS 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. The PRA models the boric acid storage tank as the short-term supply source to the CVCS until the operators can align additional inventory from the much larger demineralized water storage tank. BAS failures causing boration/dilution events are included in the general reactor trip initiator.	Yes
Control room habitability system (CHRS)	Described in Section 6.4	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 PPS when harsh conditions are detected in the control building. 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 be enacted.	No
Normal control room HVAC system (CRVS)	Described in Section 9.4	A loss of CRVS might require the MCR to be evacuated due to high temperature, but no operator actions are required to mitigate design basis accidents. Although the PRA includes a limited number of operator actions that are performed in the MCR during beyond design basis accidents, operators can also perform these actions locally (in the reactor building). Potential equipment failures due to high temperatures in the control building will not affect design basis accident mitigation because the design uses a combination of engineered safety features that actuate on loss of control power and passive cooling to the reactor pool. Failure of CRVS leading to high control room temperatures are included in the general reactor trip initiator.	Yes

Table 19.1-55: Shared System Hazard Analysis (Continued)

System	Multiple Module Function	Accident Mitigation Implication	Included in Base Model for Single NPM
Reactor building HVAC system (RBVS)	Described in Section 9.4	Loss of the RBVS would cause air temperatures in the reactor building to increase. Potential equipment failures due to high temperatures will not affect design basis accident mitigation because the design uses a combination of engineered safety features that actuate on loss of control power and provide passive cooling to the reactor pool. Potential high temperature failures of electrical systems would cause the ECCS, DHRS, and containment isolation valves to fail in their required positions for accident mitigation. The BAS pumps are located in the reactor building, and thus susceptible to high temperatures, but BAS is not required for design basis accident mitigation. BAS is included in the PRA for certain beyond design basis scenarios. In these scenarios, however, BAS is only credited in the short term while the operators align the long term makeup source, DWS. Since room heatup following loss of RBVS would be a slow process, the short term BAS makeup would not be affected. Failure of RBVS leading to high reactor building temperatures are bounded by the loss of support system initiator.	Yes
Liquid radioactive waste system (LRWS)	Described in Section 11.2	LRWS serves no safety-related functions and does not support the engineered safety features. The system is not designed to receive or process fluids resulting from reactor related accidents or emergency situations. The LWRS allows discharge of reactor coolant from CVCS for normal RCS inventory control, but this is not associated with accident mitigation.	No
Gaseous radioactive waste system	Described in Section 11.3	This system does not have a function associated with mitigation of an accident.	No
Solid radioactive waste system	Described in Section 11.4	This system does not have a function associated with mitigation of an accident.	No
Radioactive waste drain system	Described in Section 9.3	This system does not have a function associated with mitigation of an accident.	No
Radioactive waste building hvac system	Described in Section 9.4	This system does not have a function associated with mitigation of an accident.	No
Ultimate heat sink (UHS)	Described in Section 9.2	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 containment during an accident. The UHS inventory is large enough to provide cooling during a design basis accident without PCWS for at least 72 hours. Failure of post-accident heat transfer to the UHS is included in the PRA model.	Yes
Pool leakage detection system (PLDS)	Described in Section 9.1	The PLDS monitors for leakage in the UHS, but the failure of the leak detection will not affect the capacity of UHS for mitigating an accident. Monitoring of UHS water level required by technical specifications ensures the availability of the UHS.	No
Containment flooding and draining system (CFDS)	Described in Section 9.3	The CFDS is not required for design basis accident mitigation. It is included in the PRA as a means for reactor and containment makeup in certain beyond design basis events with failure of ECCS.	Yes

Table 19.1-55: Shared System Hazard Analysis (Continued)

System	Multiple Module Function	Accident Mitigation Implication	Included in Base Model for Single NPM
Reactor component cooling water system (RCCWS)	Described in Section 9.2	The RCCWS does not have an accident mitigation function. Loss of RCCWS cooling for the control rod drive mechanisms would be a potential cause of a reactor trip, and thus is included in the general reactor trip initiator. The loss of cooling for the CVCS non-regenerative heat exchanger would only affect reactor coolant cleanup, which is not required for accident mitigation.	Yes
Process sampling system	Described in Section 9.3	This system does not have a function associated with mitigation of an accident.	No
Feedwater treatment	Described in Section 10.4	This system does not have a function associated with mitigation of an accident.	No
Condensate polishing system	Described in Section 10.4	This system does not have a function associated with mitigation of an accident.	No
Chilled water system (CHWS)	Described in Section 9.2	Since the design basis accident mitigation systems (e.g., ECCS, DHRS) function by passive cooling processes and are actuated by valves that fail in their required positions on loss of power, potential failure of electrical power or control systems due to high building temperatures resulting from failure of chilled water would not affect design basis accident mitigation; high temperature failures of electrical systems would cause the ECCS and DHRS valves to fail in their required positions for accident mitigation. Similarly, containment isolation valves fail in their required positions on loss of power. Therefore, loss of chilled water will not affect design basis accident mitigation. Potential impact of CHWS failure on beyond design basis scenarios is bounded by the loss of support system initiator. High temperatures could lead to a plant shutdown, so loss of CHWS is included in the general reactor trip initiator.	Yes
Auxiliary boiler system	Described in Section 10.4	This system does not have a function associated with mitigation of an accident.	No
Site cooling water system (SCWS)	Described in Section 9.2	A loss of SCWS would inhibit cooling across numerous auxiliary systems, including the RCCWS, which cools the control rod drive mechanisms. Failure of SCWS could therefore cause a reactor trip and is included in the general reactor trip initiator. The system does not have a function associated with mitigation of an accident.	Yes
Potable water system	Described in Section 9.2	This system does not have a function associated with mitigation of an accident.	No
Utility water system	Described in Section 9.2	This system does not have a function associated with mitigation of an accident.	No
Demineralized water system (DWS)	Described in Section 9.2	The DWS is not required for design basis accident mitigation. In certain beyond design basis scenarios, the PRA models RCS injection using CVCS with long term inventory from the DWS.	Yes
Nitrogen distribution system	Described in Section 9.3	This system does not have a function associated with mitigation of an accident.	No

Table 19.1-55: Shared System Hazard Analysis (Continued)

System	Multiple Module Function	Accident Mitigation Implication	Included in Base Model for Single NPM
Service air system	Described in Section 9.3	This system does not have a function associated with mitigation of an accident.	No
Instrument and control air system (IAS)	Described in Section 9.3	The IAS is not required for accident mitigation. In certain beyond design basis scenarios, the PRA models RCS injection using CVCS with short term inventory from the BAS. Following a loss of instrument air, air operated valves in the CVCS makeup flow paths fail to the position required for makeup, so IAS is not modeled in the PRA. Loss of IAS is included in the general reactor trip initiator.	Yes
Turbine building hvac system (TBVS)	Described in Section 9.4	There is no accident mitigation equipment in the turbine building that would be failed by high turbine building temperatures. Loss of TBVS might lead to a plant scram or shutdown and is conservatively included in the general reactor trip initiator.	Yes
Fire protection system (FPS)	Described in Section 9.5	The FPS is the means for preventing fire propagation. A fire has the potential to affect key safety functions depending on where it occurs, but a fire coincident with an accident is extremely unlikely and is not considered in the internal events PRA. However, fire detection and suppression are included in the fire PRA.	No
Fire detection system	Described in Section 9.5	The FPS, including fire detection, is the means for preventing fire propagation. A fire has the potential to affect safety functions depending on where it occurs, but a fire coincident with an accident is extremely unlikely and is not considered in the internal events PRA base model. However, fire detection and suppression are included in the fire PRA.	No
Balance-of-plant drains system	Described in Section 9.3	This system does not have a function associated with mitigation of an accident.	No
High voltage AC electrical distribution system (EHVS)	Described in Section 8.3	Following a loss of EHVS, the BPSS will supply plant loads. Moreover, 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 provide passive cooling to the reactor pool. The BAS, CFDS, CVCS, and DWS, which are not required for design basis accident mitigation but are credited in the PRA for certain beyond design basis scenarios, receive power from EHVS via EMVS and ELVS buses; loss of EHVS therefore would cause failure of these beyond design basis mitigative systems. The 13.8 kV EHVS buses are included in the PRA model. Loss of EHVS is included in the loss of offsite power initiator.	Yes

Table 19.1-55: Shared System Hazard Analysis (Continued)

System	Multiple Module Function	Accident Mitigation Implication	Included in Base Model for Single NPM
Medium voltage AC electrical distribution system (EMVS)	Described in Section 8.3	A failure of the EMVS would be effectively a loss of all AC power (station blackout). The BPSS, even if available, would not be would be able to provide power, since it is connected to EMVS. The plant, however, is designed to cope with a loss of all AC power through a combination of engineered safety features that actuate on loss of control power and provide passive cooling to the reactor pool, so failure of EMVS would not affect design basis accident mitigation. The BAS, CFDS, CVCS, and DWS, which are not required for design basis accident mitigation but are credited in the PRA for certain beyond design basis scenarios, receive power from EMVS though ELVS buses; loss of EMVS therefore would cause failure of these beyond design basis mitigative systems. The common and module-specific EMVS buses are included in the PRA model. Loss of EMVS is included in the loss of support system initiator.	Yes
Low voltage AC electrical distribution system (ELVS)	Described in Section 8.3	A failure of the ELVS would have the same effect as a loss of all AC power (station blackout). The BPSS, even if available, would not be effective because power to loads would have to go through the ELVS. The plant, however, is designed to cope with a loss of all AC power through a combination of engineered safety features that actuate on loss of control power and provide passive cooling to the reactor pool, so failure of ELVS would not affect design basis accident mitigation. The BAS, CFDS, CVCS, and DWS, which are not required for design basis accident mitigation but are credited in the PRA for certain beyond design basis scenarios, receive power from ELVS; loss of ELVS therefore would cause failure of these beyond design basis mitigative systems. The common and module-specific ELVS buses that power systems modeled in the PRA are included in the PRA model. Loss of ELVS is implicitly included in the loss of support system initiator.	Yes
Augmented AC power system (EDAS)	Described in Section 8.3	Loss of the EDAS-C common loads could complicate emergency response efforts from the MCR in some situations, with the loss of emergency lighting (from PLS), loss of control room habitability supporting equipment (activated by PPS), and failure of post-accident monitoring (SDI). Emergency lighting would only be needed in a station blackout scenario, and control room action is not needed for a design basis accident. PPS initiates isolation of CRVS and actuates CRHS; this would only be needed in the case of a toxic chemical event or a beyond design basis accident causing a large radioactivity release. A toxic chemical event does not cause plant failures needing mitigation (PPS just protects the operators). A large radioactivity release during a beyond design basis event would mean that mitigation had already failed, so the loss of PPS would not affect mitigation. Finally, loss of SDI would only affect post-accident monitoring, which would not affect mitigation. Since EDAS-C does not power any equipment modeled in the PRA, EDAS-C is not modeled.	No

Table 19.1-55: Shared System Hazard Analysis (Continued)

System	Multiple Module Function	Accident Mitigation Implication	Included in Base Model for Single NPM
Normal DC power system (EDNS)	Described in Section 8.3	This system does not have a function associated with mitigation of an accident. Since EDNS provides the power to PCS and MCS, it is assumed that failure of EDNS will cause a plant transient that will lead to an automatic trip or manual shutdown and is thus included in the general reactor trip initiator.	Yes
Backup power supply system (BPSS)	Described in Section 8.3	The loss of the BPSS would reduce defense-in-depth of the station in response to a loss of 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. Therefore, the BPSS does not affect design basis accident mitigation. The backup diesel generators are included in the PRA as a power source for the EMVS buses in the case of loss of power from EHVS.	Yes
Plant lighting system	Described in Section 9.5	Loss of normal and emergency lighting would hinder operators' ability to respond to accidents using normal lighting, but no operator actions are required to design basis mitigate accidents. In beyond design basis accidents, the operators could perform PRA-modeled actions with the HSIS workstations and use flashlights for field actions.	No
Switchyard system	Described in Section 8.3	A loss of the switchyard is a loss of offsite power event. The BPSS will supply plant loads. Moreover, 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 provide passive cooling to the reactor pool. The switchyard is included in the PRA model as part of the loss of offsite power initiator.	Yes
Safety display and indication (SDI)	Described in Section 7.0	The SDI provides post-accident monitoring information to the control room, but does not have an accident mitigation function. No operator actions are required for design basis accident mitigation. Post-accident monitoring is not essential to beyond design basis accident mitigation.	No
Plant control system (PCS)	Described in Section 7.0	The PCS is not required for accident mitigation. None of the systems controlled by PCS is required for mitigating an accident. Loss of PCS is included in the general reactor trip initiator.	Yes
Plant protection system (PPS)	Described in Section 7.0	PPS isolation of control room envelop and actuation of control room habitability would only be needed in the case of a toxic chemical event or a beyond design basis accident causing a large radioactivity release. A toxic chemical event does not cause plant failures needing mitigation (PPS just protects the operators). A large radioactivity release during a beyond design basis event would mean that mitigation had already failed, so the loss of PPS would not affect mitigation.	No
Fixed area radiation monitoring system	Described in Section 7.0	This system does not have a function associated with mitigation of an accident.	No

Table 19.1-55: Shared System Hazard Analysis (Continued)

System	Multiple Module Function	Accident Mitigation Implication	Included in Base Model for Single NPM
Communication systems	Described in Section 9.5	This system does not have a function associated with mitigation of an accident. Design basis accidents do not require operator actions and operator actions outside the control room in a beyond design basis scenario could be coordinated using portable radios.	No
Seismic monitoring system	Described in Section 3.7	This system does not have a function associated with mitigation of an accident. It only provides information to the operators as to the magnitude of a seismic event. Operator response would be governed by any equipment failures.	No

Table 19.1-56: Multi-Module Adjustment Factors for Initiating Events

Initiating Event	MMAF Description	MMAF	Basis
CVCS-BREAK-IOC CVCS--BREAK-DOC CVCS--ALOCA-IIC MSS---ALOCA-SG- TGS---FMSLB-UD-	LOCA from a pipe break	0.01	These are initiating events associated with an LOCA occurring as a result of a pipe break. Potential coupling mechanisms include pipe age, manufacturing defects, similar phase transformations, environmental conditions, and water chemistry effects. An MMAF of one percent is assigned to each initiating event based on engineering judgment.
ECCS--ALOCA-RV1 RCS---ALOCA-IC-	LOCA not from a pipe break	0.1	These are initiating events associated with an LOCA that is not caused by a pipe break. Examples of events include spurious opening of valves or induced leaks. Potential coupling mechanisms (or items that reduce coupling) include environmental conditions, manufacturing errors, maintenance errors, and mechanical or electrical deficiencies for control or performance purposes. An MMAF of ten percent is assigned to each initiating event based on engineering judgment.
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 general transients, loss of feedwater, and loss of instrument air. Several modeled contributors are shared systems. Others, such as the feedwater system, are generally NPM-specific, but is shared outside of the reactor building and turbine generator building with a common water supply. The condenser heat sinks on each turbine are NPM-specific. General transients are deemed to primarily impact individual modules. Because the “general reactor trip” initiating event frequency is predominantly comprised of general transients, a factor of ten percent is assigned to the MMAF for this initiating event. The ten percent factor is a commonly used beta factor used to account for coupling mechanisms in CCF analysis.
TGS---TRAN--SS-	Loss of support system	0.1	This initiating event considers failures of equipment leading to unavailability of the CVCS or CFDS resulting from a loss of an EMVS bus. Failure of this support system will impact a single NPM and does not involve CCF (i.e., only a single bus failure is required). An MMAF of ten percent is assigned to each initiating event based on engineering judgment.
EHVS--LOOP-----	Site-wide initiating event	1.0	Initiating events impacting the site are grouped into this classification, (e.g., an 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). An MMAF of 100 percent is assigned based on engineering judgment.

Table 19.1-56: Multi-Module Adjustment Factors for Initiating Events (Continued)

Initiating Event	MMAF Description	MMAF	Basis
EDAS--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 buses 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 30 percent for the MMAF is applied as a conditional probability of CCF extension to two or more modules given a CCF in one module.

Table 19.1-57: Multi-Module Adjustment Factors and Multi-Module Performance Shaping Factors 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 NPMs; value based on commonly used beta factor.
CCF Basic Event	0.3	Potential coupling of failures in a short time period because of 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 probabilistic risk assessment, the failure event affects two or more NPMs simultaneously.
CCF Involving Shared Equipment Basic Event	1.0	The MMAF is used to model shared redundant SSC.
HFE Involving Shared Systems	1.0	The MMAF represents operator action affecting shared equipment.
Similar Plant Response Basic Events	1.0	Represents similar response of all NPMs. There is one event recovery of offsite power before depletion of backup battery power.
Physical Parameter Basic Events	1.0	Represents common deterministic design response, (e.g., actuation setpoint).
Passive Safety System Reliability ECCS events	1.0	Represents passive emergency core cooling system MMAF for multiple NPMs. The MMAF is determined based on engineering judgment.
Passive Safety System Reliability DHRS events	1.0	Represents passive decay heat removal system MMAF for multiple NPMs. The MMAF is determined 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.
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.
RSV Demand Probability Event	1.0	Represents common physical conditions and response. The MMAF is determined 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 NPM configuration.

Table 19.1-58: Dominant Cutsets (Multi-Module, Full-Power)

Cutset	Frequency	Contribution	Description
CDF Cutsets			
1	1.4E-10	12.0	
			Loss of Support System
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			NSSIE MMAF FOR BASIC EVENT- IE-TGS---TRAN--SS-
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
2	5.1E-11	4.5	
			Loss of Support System
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			CCF MMAF FOR BASIC EVENT- ECCS--POV-1CC22-FTO-S
			NSSIE MMAF FOR BASIC EVENT- IE-TGS---TRAN--SS-
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
3	5.1E-11	4.5	
			Loss of Support System
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			CCF MMAF FOR BASIC EVENT- ECCS--POV-2CC22-FTO-S
			NSSIE MMAF FOR BASIC EVENT- IE-TGS---TRAN--SS-
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
4	3.4E-11	3.0	
			LOCA Inside Containment
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			LOCA-NPBK MMAF FOR BASIC EVENT- IE-RCS---ALOCA-IC-
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS

Table 19.1-58: Dominant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Frequency	Contribution	Description
5	2.9E-11	2.6	
			Loss Of Offsite Power
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO OPEN ECCS VALVES
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			SHARED HFE MMAF FOR BASIC EVENT- BPSS--HFE-0001C-FTS-N
			PLANT RESPONSE MMAF FOR BASIC EVENT- EHVS--SYS-0001X-FOP-N
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			PARAMETER MMAF FOR BASIC EVENT- RCS---RSV-0003A-OPN-S
			CCF MMAF FOR BASIC EVENT- RCS---STL-3CC34-FOD-S
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
			CCF OF 3 OF 4 RCS RPV LEVEL SENSORS FAIL TO OPERATE ON DEMAND
6	2.9E-11	2.6	
			Loss Of Offsite Power
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO OPEN ECCS VALVES
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			SHARED HFE MMAF FOR BASIC EVENT- BPSS--HFE-0001C-FTS-N
			PLANT RESPONSE MMAF FOR BASIC EVENT- EHVS--SYS-0001X-FOP-N
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			CCF MMAF FOR BASIC EVENT- RCS---STL-3CC34-FOD-S
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			CCF OF 3 OF 4 RCS RPV LEVEL SENSORS FAIL TO OPERATE ON DEMAND
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-58: Dominant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Frequency	Contribution	Description
7	2.9E-11	2.6	
			General Reactor Trip
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET FOLLOWING ECCS SDM TIMER BYPASS HFE
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			TRANIE MMAF FOR BASIC EVENT- IE-TGS---TRAN--NPC
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			RCS Reactor Safety Valve Not Demanded to Open
8	2.9E-11	2.6	
			General Reactor Trip
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET FOLLOWING ECCS SDM TIMER BYPASS HFE
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			TRANIE MMAF FOR BASIC EVENT- IE-TGS---TRAN--NPC
			PARAMETER MMAF FOR BASIC EVENT- RCS---RSV-0003A-OPN-S
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
9	2.3E-11	2.0	
			Loss Of Offsite Power
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			SHARED HFE MMAF FOR BASIC EVENT- BPSS--HFE-0001C-FTS-N
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			PLANT RESPONSE MMAF FOR BASIC EVENT- EHVS--SYS-0001X-FOP-N
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			PARAMETER MMAF FOR BASIC EVENT- RCS---RSV-0003A-OPN-S
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN

Table 19.1-58: Dominant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Frequency	Contribution	Description
10	2.3E-11	2.0	
			Loss Of Offsite Power
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			SHARED HFE MMAF FOR BASIC EVENT- BPSS--HFE-0001C-FTS-N
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			PLANT RESPONSE MMAF FOR BASIC EVENT- EHVS--SYS-0001X-FOP-N
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			RCS Reactor Safety Valve Not Demanded to Open
11	2.2E-11	2.0	
			Loss Of Offsite Power
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO OPEN ECCS VALVES
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			SHARED HFE MMAF FOR BASIC EVENT- BPSS--HFE-0001C-FTS-N
			PLANT RESPONSE MMAF FOR BASIC EVENT- EHVS--SYS-0001X-FOP-N
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			CCF MMAF FOR BASIC EVENT- MPS---PLL-2CC34-FOD-S
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			CCF OF 3 OF 4 RPV LEVEL PROCESS LOGIC ELEMENTS
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-58: Dominant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Frequency	Contribution	Description
12	2.2E-11	2.0	
			Loss Of Offsite Power
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO OPEN ECCS VALVES
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			SHARED HFE MMAF FOR BASIC EVENT- BPSS--HFE-0001C-FTS-N
			PLANT RESPONSE MMAF FOR BASIC EVENT- EHVS--SYS-0001X-FOP-N
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			CCF MMAF FOR BASIC EVENT- MPS---PLL-2CC34-FOD-S
			PARAMETER MMAF FOR BASIC EVENT- RCS---RSV-0003A-OPN-S
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			CCF OF 3 OF 4 RPV LEVEL PROCESS LOGIC ELEMENTS
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
13	2.0E-11	1.8	
			Loss of DC Power
			OPERATOR FAILS TO LOCALLY UNISOLATE AND INITIATE CVCS INJECTION
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			CCFIE MMAF FOR BASIC EVENT- IE-EDAS--LODC-----
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
14	1.9E-11	1.7	
			Spurious Opening of an ECCS Valve
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			LOCA-NPBK MMAF FOR BASIC EVENT- IE-ECCS--ALOCA-RV1
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS

Table 19.1-58: Dominant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Frequency	Contribution	Description
15	1.7E-11	1.5	
			Loss of Support System
			OPERATOR FAILS TO OPEN ECCS VALVES
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			NSSIE MMAF FOR BASIC EVENT- IE-TGS---TRAN--SS-
			CCF MMAF FOR BASIC EVENT- RCS---STL-3CC34-FOD-S
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			CCF OF 3 OF 4 RCS RPV LEVEL SENSORS FAIL TO OPERATE ON DEMAND
16	1.6E-11	1.4	
			Loss Of Offsite Power
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS
			SHARED MMAF FOR BASIC EVENT- BPSS00DGN-6001X-FTR-N
			SHARED MMAF FOR BASIC EVENT- BPSS00DGN-6002X-FTR-N
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			PLANT RESPONSE MMAF FOR BASIC EVENT- EHVS--SYS-0001X-FOP-N
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			PARAMETER MMAF FOR BASIC EVENT- RCS---RSV-0003A-OPN-S
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN

Table 19.1-58: Dominant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Frequency	Contribution	Description
17	1.6E-11	1.4	
			Loss Of Offsite Power
			DGN 6001X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			DGN 6002X BPSS BACKUP DIESEL GENERATOR FAILS TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS
			SHARED MMAF FOR BASIC EVENT- BPSS00DGN-6001X-FTR-N
			SHARED MMAF FOR BASIC EVENT- BPSS00DGN-6002X-FTR-N
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			PLANT RESPONSE MMAF FOR BASIC EVENT- EHVS--SYS-0001X-FOP-N
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			RCS Reactor Safety Valve Not Demanded to Open
18	1.3E-11	1.2	
			Loss of Support System
			OPERATOR FAILS TO OPEN ECCS VALVES
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			NSSIE MMAF FOR BASIC EVENT- IE-TGS---TRAN--SS-
			CCF MMAF FOR BASIC EVENT- MPS---PLL-2CC34-FOD-S
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			CCF OF 3 OF 4 RPV LEVEL PROCESS LOGIC ELEMENTS
19	1.3E-11	1.1	
			LOCA Inside Containment
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			CCF OF 2 OF 2 ECCS REACTOR VENT VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			CCF MMAF FOR BASIC EVENT- ECCS--POV-2CC22-FTO-S
			LOCA-NPBK MMAF FOR BASIC EVENT- IE-RCS---ALOCA-IC-
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS

Table 19.1-58: Dominant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Frequency	Contribution	Description
20	1.3E-11	1.1	
			LOCA Inside Containment
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			CCF OF 2 OF 2 ECCS REACTOR RECIRCULATION VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			CCF MMAF FOR BASIC EVENT- ECCS--POV-1CC22-FTO-S
			LOCA-NPBK MMAF FOR BASIC EVENT- IE-RCS---ALOCA-IC-
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
21	1.3E-11	1.1	
			Loss Of Offsite Power
			CCF OF 2 OF 2 BPSS BACKUP DIESEL GENERATORS FAIL TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS
			SHARED CCF MMAF FOR BASIC EVENT- BPSS00DGN-1CC22-FTR-N
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			PLANT RESPONSE MMAF FOR BASIC EVENT- EHVS--SYS-0001X-FOP-N
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			PARAMETER MMAF FOR BASIC EVENT- RCS---RSV-0003A-OPN-S
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
22	1.3E-11	1.1	
			Loss Of Offsite Power
			CCF OF 2 OF 2 BPSS BACKUP DIESEL GENERATORS FAIL TO RUN (48 HOURS)
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OFF-SITE POWER NOT RESTORED WITHIN 24 HOURS
			SHARED CCF MMAF FOR BASIC EVENT- BPSS00DGN-1CC22-FTR-N
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			PLANT RESPONSE MMAF FOR BASIC EVENT- EHVS--SYS-0001X-FOP-N
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-58: Dominant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Frequency	Contribution	Description
23	1.3E-11	1.1	
			Loss of Support System
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			NSSIE MMAF FOR BASIC EVENT- IE-TGS---TRAN--SS-
			CCF MMAF FOR BASIC EVENT- MPS---APL-2CC22-FOP-S
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			CCF OF 2 OF 2 APL MODULES IN ECCS REACTOR VENT VALVES FAILS TO OPERATE
24	1.2E-11	1.1	
			Loss Of Offsite Power
			Backup Diesel Generators
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET FOLLOWING ECCS SDM TIMER BYPASS HFE
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			PARAMETER MMAF FOR BASIC EVENT- RCS---RSV-0003A-OPN-S
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			PROBABILITY THAT THE RSV IS DEMANDED TO OPEN
25	1.2E-11	1.1	
			Loss Of Offsite Power
			Backup Diesel Generators
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			OPERATOR FAILS TO BYPASS ECCS SHUTDOWN MARGIN TIMER
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET FOLLOWING ECCS SDM TIMER BYPASS HFE
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			RCS Reactor Safety Valve Not Demanded to Open

Table 19.1-58: Dominant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Frequency	Contribution	Description
			LRF Cutsets
1	4.2E-15	40.3	
			General Reactor Trip
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			OPERATOR FAILS TO OPEN ECCS VALVES
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR THIRD HFE IN CUTSET
			TRANIE MMAF FOR BASIC EVENT- IE-TGS---TRAN--NPC
			CCF MMAF FOR BASIC EVENT- MPS---SVM-1CC23-FOP-S
			CCF MMAF FOR BASIC EVENT- MPS---SVM-3CC23-FOP-S
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			CCF OF 2 OF 3 DIVISION I ESFAS SCHEDULING AND VOTING MODULES
			CCF OF 2 OF 3 DIVISION II ESFAS SCHEDULING AND VOTING MODULES
2	1.8E-15	17.4	
			Loss Of Offsite Power
			OPERATOR FAILS TO START/LOAD DGN 6001X AND 6002X BPSS BACKUP DIESEL GENERATORS
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			OPERATOR FAILS TO OPEN ECCS VALVES
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR THIRD HFE IN CUTSET
			SHARED HFE MMAF FOR BASIC EVENT- BPSS--HFE-0001C-FTS-N
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			CCF MMAF FOR BASIC EVENT- MPS---SVM-1CC23-FOP-S
			CCF MMAF FOR BASIC EVENT- MPS---SVM-3CC23-FOP-S
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			CCF OF 2 OF 3 DIVISION I ESFAS SCHEDULING AND VOTING MODULES
			CCF OF 2 OF 3 DIVISION II ESFAS SCHEDULING AND VOTING MODULES

Table 19.1-58: Dominant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Frequency	Contribution	Description
3	1.8E-15	17.1	
			Loss Of Offsite Power
			Backup Diesel Generators
			OPERATOR FAILS TO ISOLATE CONTAINMENT
			OPERATOR FAILS TO INITIATE CVCS INJECTION
			OPERATOR FAILS TO OPEN ECCS VALVES
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR SECOND HFE IN CUTSET
			HUMAN ERROR PROBABILITY FOR THIRD HFE IN CUTSET
			SITE-WIDE MMAF FOR BASIC EVENT- IE-EHVS--LOOP-----
			CCF MMAF FOR BASIC EVENT- MPS---SVM-1CC23-FOP-S
			CCF MMAF FOR BASIC EVENT- MPS---SVM-3CC23-FOP-S
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS
			CCF OF 2 OF 3 DIVISION I ESFAS SCHEDULING AND VOTING MODULES
			CCF OF 2 OF 3 DIVISION II ESFAS SCHEDULING AND VOTING MODULES
4	1.3E-15	12.6	
			Loss of Support System
			CCF OF 2 OF 2 CNTS CVCS DISCHARGE LINE CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			CCF MMAF FOR BASIC EVENT- CVCS--HOV-3CC22-FTC-S
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			NSSIE MMAF FOR BASIC EVENT- IE-TGS---TRAN--SS-
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS

Table 19.1-58: Dominant Cutsets (Multi-Module, Full-Power) (Continued)

Cutset	Frequency	Contribution	Description
5	1.3E-15	12.6	
			Loss of Support System
			CCF OF 2 OF 2 CNTS CES CONTAINMENT ISOLATION VALVES FAIL TO CLOSE
			CCF OF 2 OF 4 ECCS RVV TRIP VALVES FAIL TO OPEN
			OPERATOR FAILS TO ALIGN ALTERNATE POWER TO MODULE-SPECIFIC ELVS
			HUMAN ERROR PROBABILITY FOR FIRST HFE IN CUTSET
			CCF MMAF FOR BASIC EVENT- CES---HOV-1CC22-FTC-S
			CCF MMAF FOR BASIC EVENT- ECCS--SOV-2CC24-FTO-S
			NSSIE MMAF FOR BASIC EVENT- IE-TGS---TRAN--SS-
			HFE MMPSF FOR MODULE-DEPENDENT HUMAN ACTIONS

Table 19.1-59: Summary of Contribution to Internal Events Multi-Module Core Damage Frequency and Large Release Frequency by Initiator

Initiating Event Descriptions	Contribution to MM-CDF (Percentage)	Contribution to MM-LRF (Percentage)
Loss of support system (TGS---TRAN--SS)	25.4	25.2
Loss of offsite power (EHVS--LOOP)	50.7	34.5
General reactor trip (TGS---TRAN--NPC)	10.6	40.3
Reactor coolant system LOCA inside containment (RCS---ALOCA-IC)	6.4	<0.1
Chemical and volume control system LOCA injection line inside containment (CVCS--ALOCA-IIC)	0.2	<0.1
Spurious opening of an emergency core cooling system valve (ECCS--ALOCA-RV1)	2.9	<0.1
Loss of DC power (EDAS--LODC)	3.8	<0.1
CVCS injection line break outside containment (CVCS--BREAK-IOC)	<0.1	<0.1
CVCS discharge line break outside containment (CVCS--BREAK-DOC)	<0.1	<0.1
Steam generator tube failure (MSS---ALOCA-SG)	<0.1	<0.1
Secondary side line break (TGS---FMSLB-UD)	<0.1	<0.1

Table 19.1-60: Summary of Results

Full Power (per mcyr)						
Hazard	**CDF (mean values)**	**5th percentile**	**95th percentile**	**LRF (mean values)**	**5th percentile**	**95th percentile**
Internal Events	6.0E-09	2.2E-10	2.1E-08	6.6E-13	<1E-15	1.5E-12
Internal Fires	4.6E-09	9.7E-11	1.6E-08	1.3E-11	3.9E-15	3.0E-11
Internal Floods	1.6E-10	1.8E-12	5.5E-10	3.4E-14	<1E-15	2.8E-14
External Floods	9.5E-09	1.4E-10	3.5E-08	1.4E-13	5.9E-15	4.3E-12
High Winds (Tornado)	2.6E-09	2.6E-11	9.5E-09	1.6E-13	<1E-15	4.9E-13
High Winds (Hurricane)	1.9E-08	1.9E-10	7.0E-08	1.3E-12	<1E-15	4.3E-12
Seismic [1] (SMA)	0.92g					
Low Power and Shutdown (per year)						
Hazard	**CDF (mean values)**	**5th percentile**	**95th percentile**	**LRF (mean values)**	**5th percentile**	**95th percentile**
Internal Events	4.0E-11	9.8E-13	1.4E-10	3.5E-12	4.2E-14	1.2E-11
Module Drop	1.8E-08	2.5E-10	6.9E-08	NA [2]	NA [2]	NA [2]
Internal Fires	negligible[5]			negligible[5]		
Internal Floods	negligible[5]			negligible[5]		
External Floods	negligible[5]			negligible[5]		
High Winds (Tornado)	negligible[5]			negligible[5]		
High Winds (Hurricane)	negligible[5]			negligible[5]		
Seismic [1] (SMA)	NA					
Multi-Module						
Hazard	**Conditional Probability of Core Damage**			**Conditional Probability of Large Release**		
Multi-Module	0.21[3]			0.03[3]		
Composite CCFP < 0.1[4]						

Notes:

1. A seismic margins assessment is 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%).
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. Composite CCFP reflects contributions from all hazards.
5. Based on qualitative evaluation.

Table 19.1-61: Multi-Module Considerations for External Events

SSC	NPMs served	Seismic	Internal Flood	External Flood	High Winds
BAS	6	Note 1	Yes	Yes [2]	Yes [2]
BPSS	6	Note 1	None	Yes	Yes
RTS	1	Note 1	None	None	None
DHRS	1	Note 1	None	None	None
RSVs	1	Note 1	None	None	None
ECCS	1	Note 1	None	None	None
CVCS	1	Note 1	Yes	Yes [2]	Yes [2]
CFDS	6	Note 1	Yes	Yes [2]	Yes [2]
CIVs	1	Note 1	None	None	None
UHS	6	None	None	None	None

1. Seismic events have the potential to produce correlated SSC failures in multiple NPM.
2. If hazard results in a loss of all AC power, system is unavailable (e.g., pump motive power).

Figure 19.1-1: Master Logic Diagram for Initiating Events

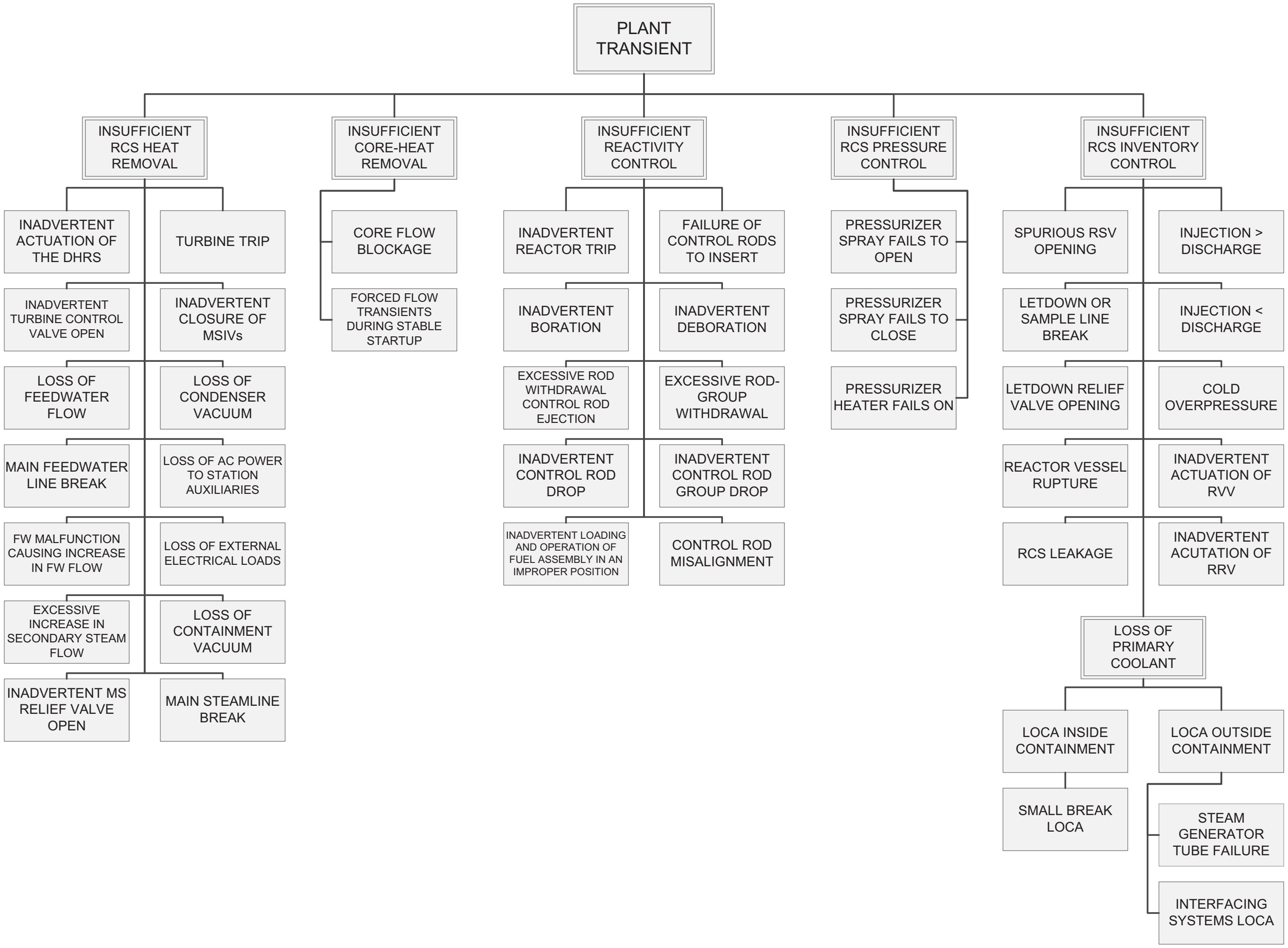
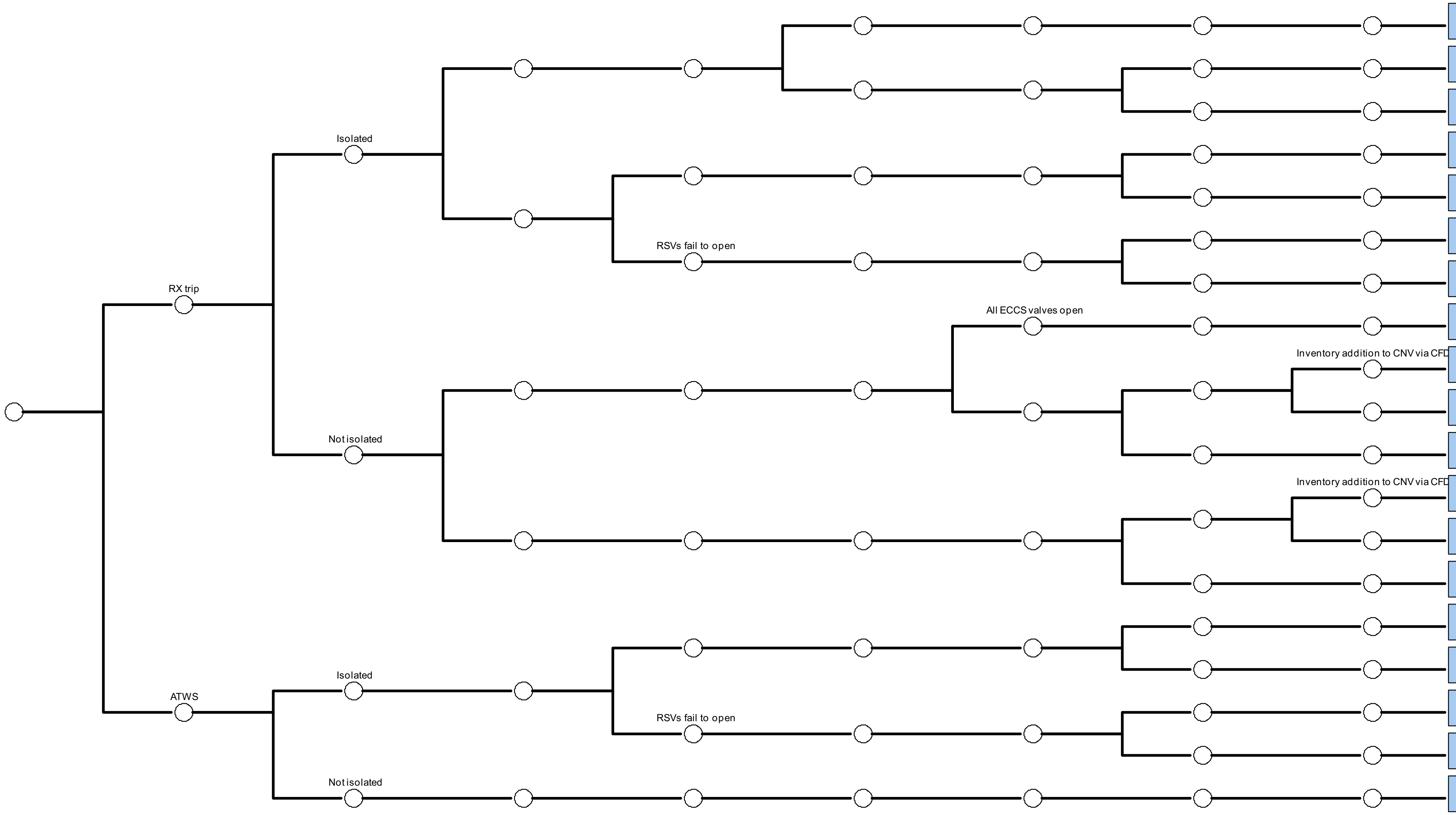

PLANT TRANSIENT
INSUFFICIENT RCS HEAT REMOVAL
INSUFFICIENT CORE-HEAT REMOVAL
INSUFFICIENT REACTIVITY CONTROL
INSUFFICIENT RCS PRESSURE CONTROL
INSUFFICIENT RCS INVENTORY CONTROL
INADVERTENT ACTUATION OF THE DHRS
TURBINE TRIP
INADVERTENT TURBINE CONTROL VALVE OPEN
INADVERTENT CLOSURE OF MSIVs
LOSS OF FEEDWATER FLOW
LOSS OF CONDENSER VACUUM
MAIN FEEDWATER LINE BREAK
LOSS OF AC POWER TO STATION AUXILIARIES
FW MALFUNCTION CAUSING INCREASE IN FW FLOW
LOSS OF EXTERNAL ELECTRICAL LOADS
EXCESSIVE INCREASE IN SECONDARY STEAM FLOW
LOSS OF CONTAINMENT VACUUM
INADVERTENT MS RELIEF VALVE OPEN
MAIN STEAMLINE BREAK
CORE FLOW BLOCKAGE
FORCED FLOW TRANSIENTS DURING STABLE STARTUP
INADVERTENT REACTOR TRIP
FAILURE OF CONTROL RODS TO INSERT
INADVERTENT BORATION
INADVERTENT DEBORATION
EXCESSIVE ROD WITHDRAWAL CONTROL ROD EJECTION
EXCESSIVE ROD-GROUP WITHDRAWAL
INADVERTENT CONTROL ROD DROP
INADVERTENT CONTROL ROD GROUP DROP
INADVERTENT LOADING AND OPERATION OF FUEL ASSEMBLY IN AN IMPROPER POSITION
CONTROL ROD MISALIGNMENT
PRESSURIZER SPRAY FAILS TO OPEN
PRESSURIZER SPRAY FAILS TO CLOSE
PRESSURIZER HEATER FAILS ON
SPURIOUS RSV OPENING
INJECTION > DISCHARGE
LETDOWN OR SAMPLE LINE BREAK
INJECTION < DISCHARGE
LETDOWN RELIEF VALVE OPENING
COLD OVERPRESSURE
REACTOR VESSEL RUPTURE
INADVERTENT ACTUATION OF RVV
RCS LEAKAGE
INADVERTENT ACUTATION OF RRV
LOSS OF PRIMARY COOLANT
LOCA INSIDE CONTAINMENT
LOCA OUTSIDE CONTAINMENT
SMALL BREAK LOCA
STEAM GENERATOR TUBE FAILURE
INTERFACING SYSTEMS LOCA

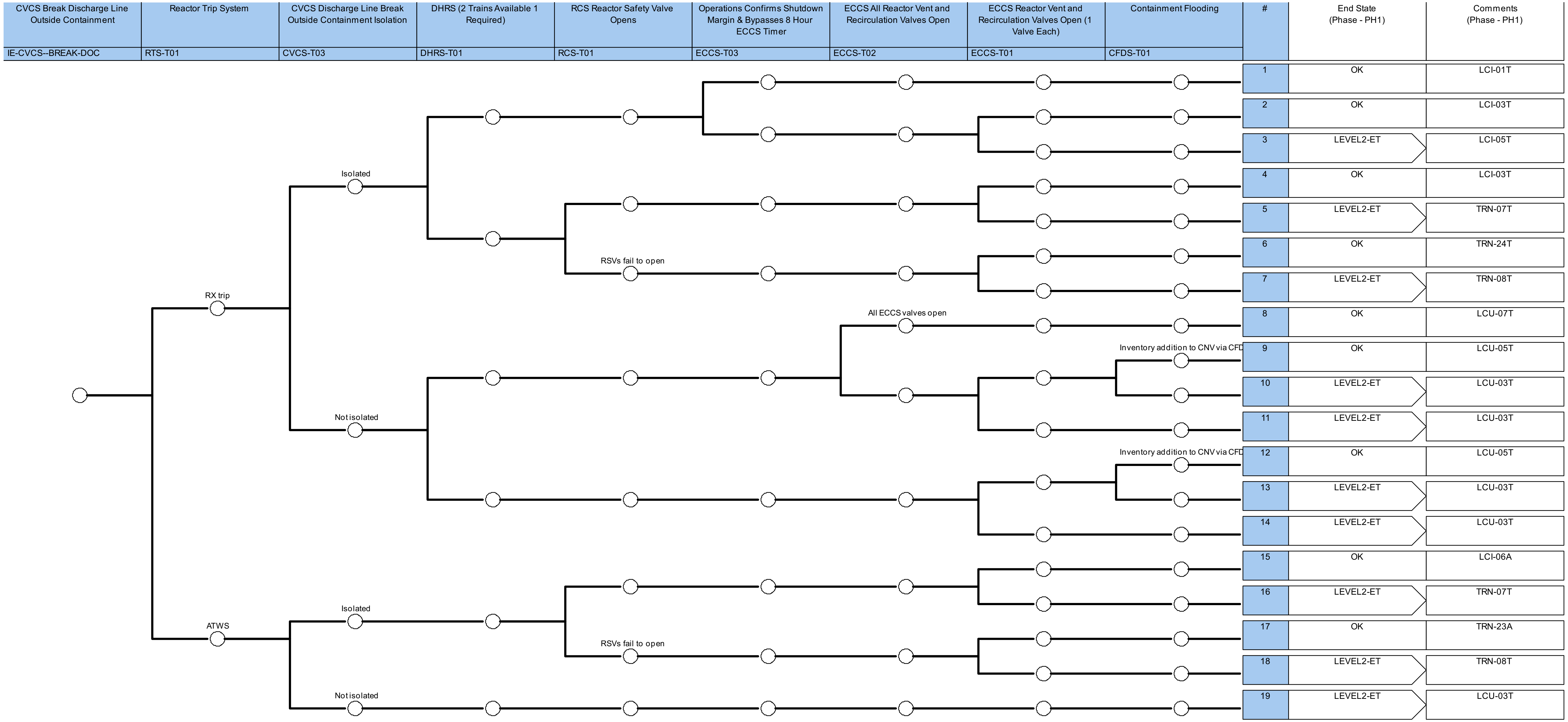
Figure 19.1-2: Event Tree for Chemical and Volume Control System Injection Line Pipe Break Outside Containment

CVCS Break Injection Line Outside Containment	Reactor Trip System	CVCS Injection Line Break Outside Containment Isolation	DHRS (2 Trains Available 1 Required)	RCS Reactor Safety Valve Opens	Operations Confirms Shutdown Margin & Bypasses 8 Hour ECCS Timer	ECCS All Reactor Vent and Recirculation Valves Open	ECCS Reactor Vent and Recirculation Valves Open (1 Valve Each)	Containment Flooding
IE-CVCS--BREAK-IOC	RTS-T01	CVCS-T02	DHRS-T01	RCS-T01	ECCS-T03	ECCS-T02	ECCS-T01	CFDS-T01



#	End State (Phase - PH1)	Comments (Phase - PH1)
1	OK	LCI-01T
2	OK	LCI-03T
3	LEVEL2-ET	LCI-05T
4	OK	LCI-03T
5	LEVEL2-ET	TRN-07T
6	OK	TRN-24T
7	LEVEL2-ET	TRN-08T
8	OK	LCU-07T
9	OK	LCU-05T
10	LEVEL2-ET	LCU-03T
11	LEVEL2-ET	LCU-03T
12	OK	LCU-05T
13	LEVEL2-ET	LCU-03T
14	LEVEL2-ET	LCU-03T
15	OK	LCI-06A
16	LEVEL2-ET	TRN-07T
17	OK	TRN-23A
18	LEVEL2-ET	TRN-08T
19	LEVEL2-ET	LCU-03T

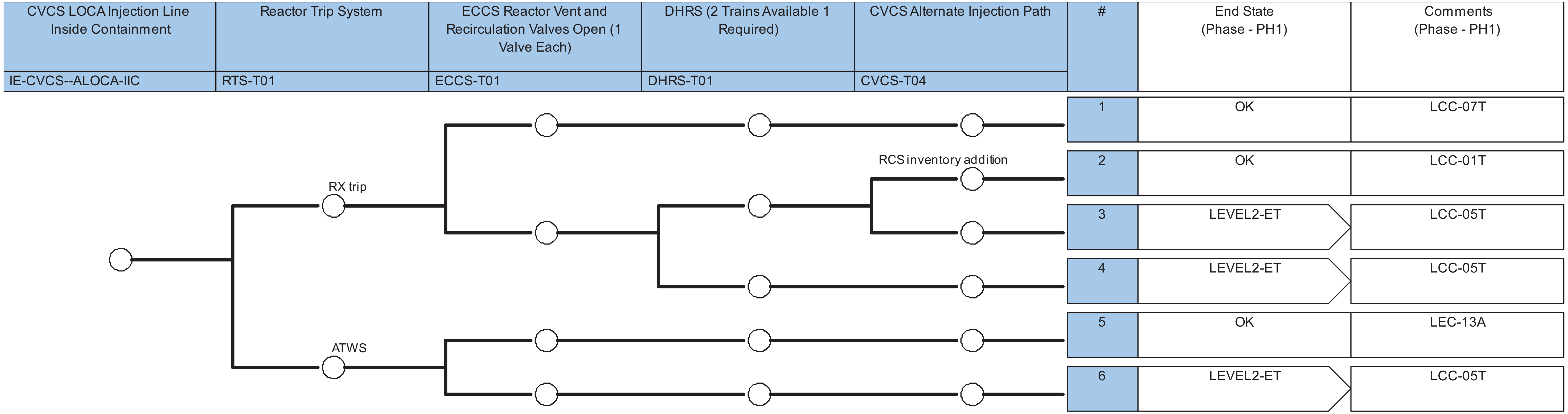
Figure 19.1-3: Event Tree for Chemical and Volume Control System Discharge Line Pipe Break Outside Containment



CVCS Break Discharge Line Outside Containment	Reactor Trip System	CVCS Discharge Line Break Outside Containment Isolation	DHRS (2 Trains Available 1 Required)	RCS Reactor Safety Valve Opens	Operations Confirms Shutdown Margin & Bypasses 8 Hour ECCS Timer	ECCS All Reactor Vent and Recirculation Valves Open	ECCS Reactor Vent and Recirculation Valves Open (1 Valve Each)	Containment Flooding
IE-CVCS--BREAK-DOC	RTS-T01	CVCS-T03	DHRS-T01	RCS-T01	ECCS-T03	ECCS-T02	ECCS-T01	CFDS-T01

#	End State (Phase - PH1)	Comments (Phase - PH1)
1	OK	LCI-01T
2	OK	LCI-03T
3	LEVEL2-ET	LCI-05T
4	OK	LCI-03T
5	LEVEL2-ET	TRN-07T
6	OK	TRN-24T
7	LEVEL2-ET	TRN-08T
8	OK	LCU-07T
9	OK	LCU-05T
10	LEVEL2-ET	LCU-03T
11	LEVEL2-ET	LCU-03T
12	OK	LCU-05T
13	LEVEL2-ET	LCU-03T
14	LEVEL2-ET	LCU-03T
15	OK	LCI-06A
16	LEVEL2-ET	TRN-07T
17	OK	TRN-23A
18	LEVEL2-ET	TRN-08T
19	LEVEL2-ET	LCU-03T

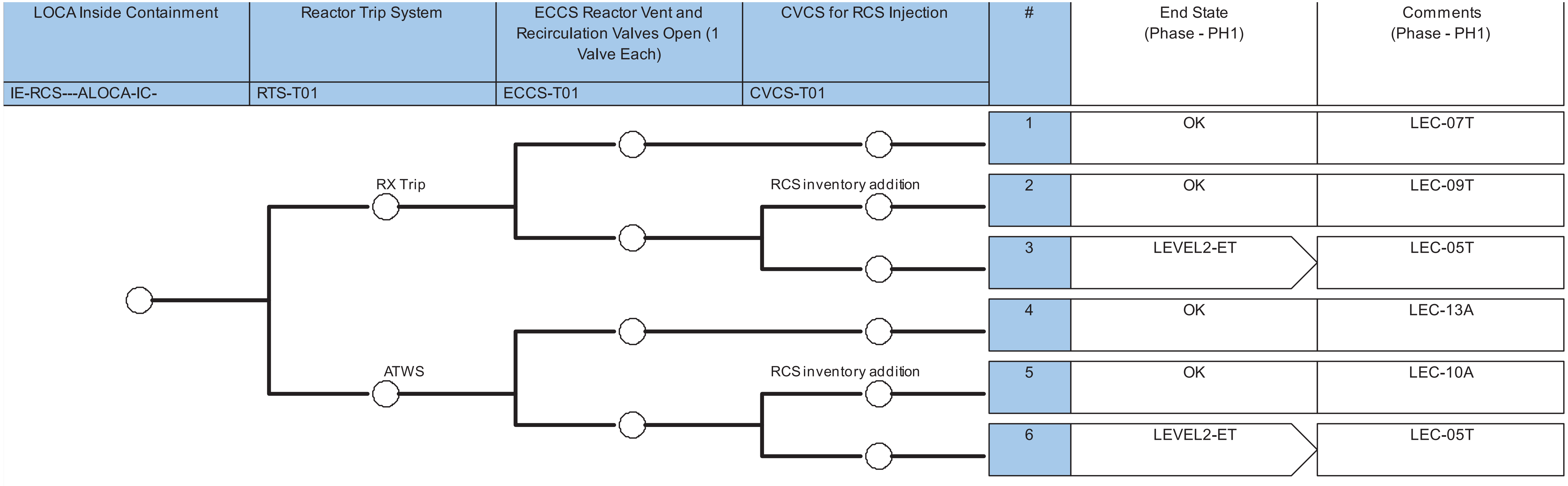
Figure 19.1-4: Event Tree for Chemical and Volume Control System Injection Line Loss-of-Coolant Accident Inside Containment



CVCS LOCA Injection Line Inside Containment	Reactor Trip System	ECCS Reactor Vent and Recirculation Valves Open (1 Valve Each)	DHRS (2 Trains Available 1 Required)	CVCS Alternate Injection Path
IE-CVCS--ALOCA-IIC	RTS-T01	ECCS-T01	DHRS-T01	CVCS-T04

#	End State (Phase - PH1)	Comments (Phase - PH1)
1	OK	LCC-07T
2	OK	LCC-01T
3	LEVEL2-ET	LCC-05T
4	LEVEL2-ET	LCC-05T
5	OK	LEC-13A
6	LEVEL2-ET	LCC-05T

Figure 19.1-5: Event Tree for Reactor Coolant System Loss-of-Coolant Accident Inside Containment



#	End State (Phase - PH1)	Comments (Phase - PH1)
1	OK	LEC-07T
2	OK	LEC-09T
3	LEVEL2-ET	LEC-05T
4	OK	LEC-13A
5	OK	LEC-10A
6	LEVEL2-ET	LEC-05T

Figure 19.1-6: Event Tree for Spurious Opening of an Emergency Core Cooling System Valve

Spurious Opening of an ECCS Valve	Reactor Trip System	ECCS Reactor Vent and Recirculation Valves Open (1 Valve Each)	CVCS for RCS Injection	#	End State (Phase - PH1)	Comments (Phase - PH1)
IE-ECCS--ALOCA-RV1	RTS-T01	ECCS-T01	CVCS-T01			
				1	OK	LEC-07T
				2	OK	LEC-09T
				3	LEVEL2-ET	LEC-05T
				4	OK	LEC-13A
				5	OK	LEC-10A
				6	LEVEL2-ET	LEC-05T

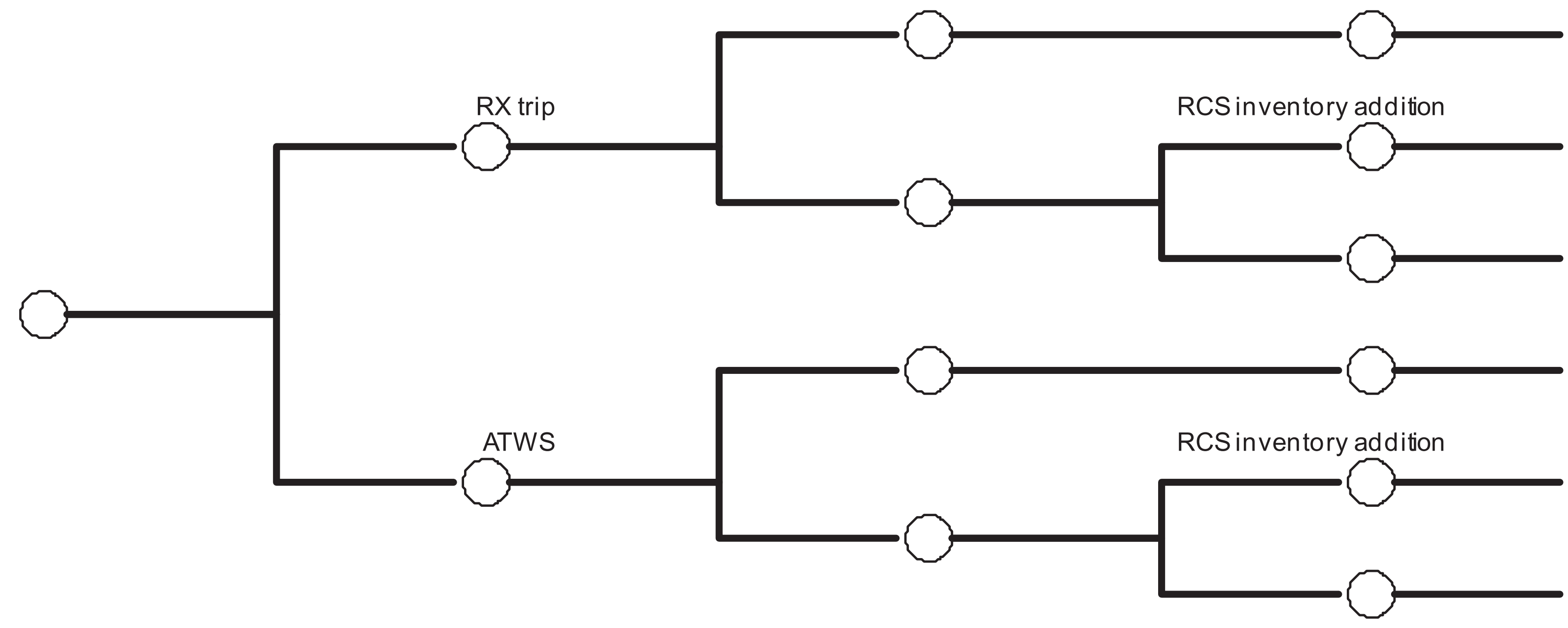
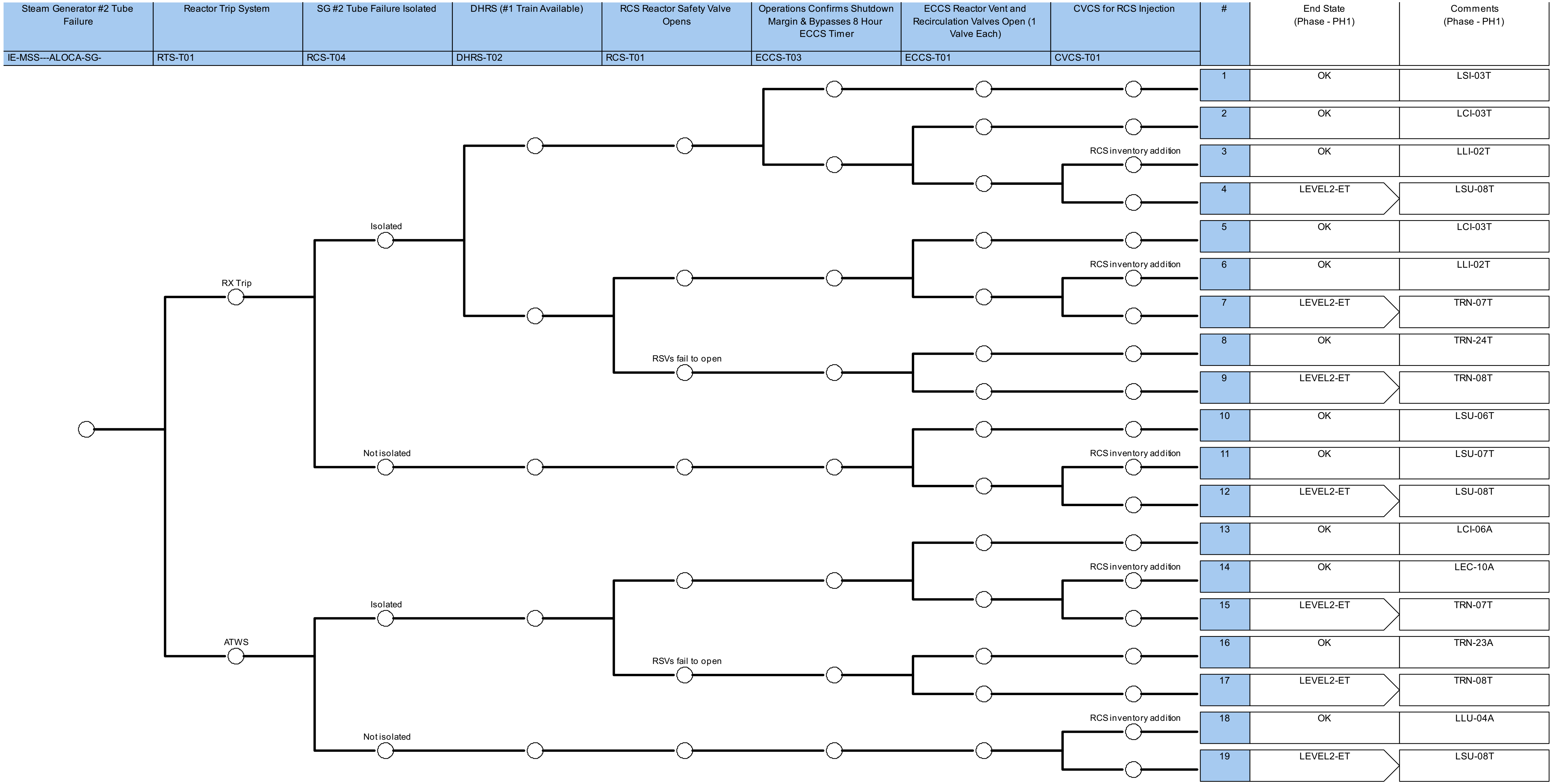


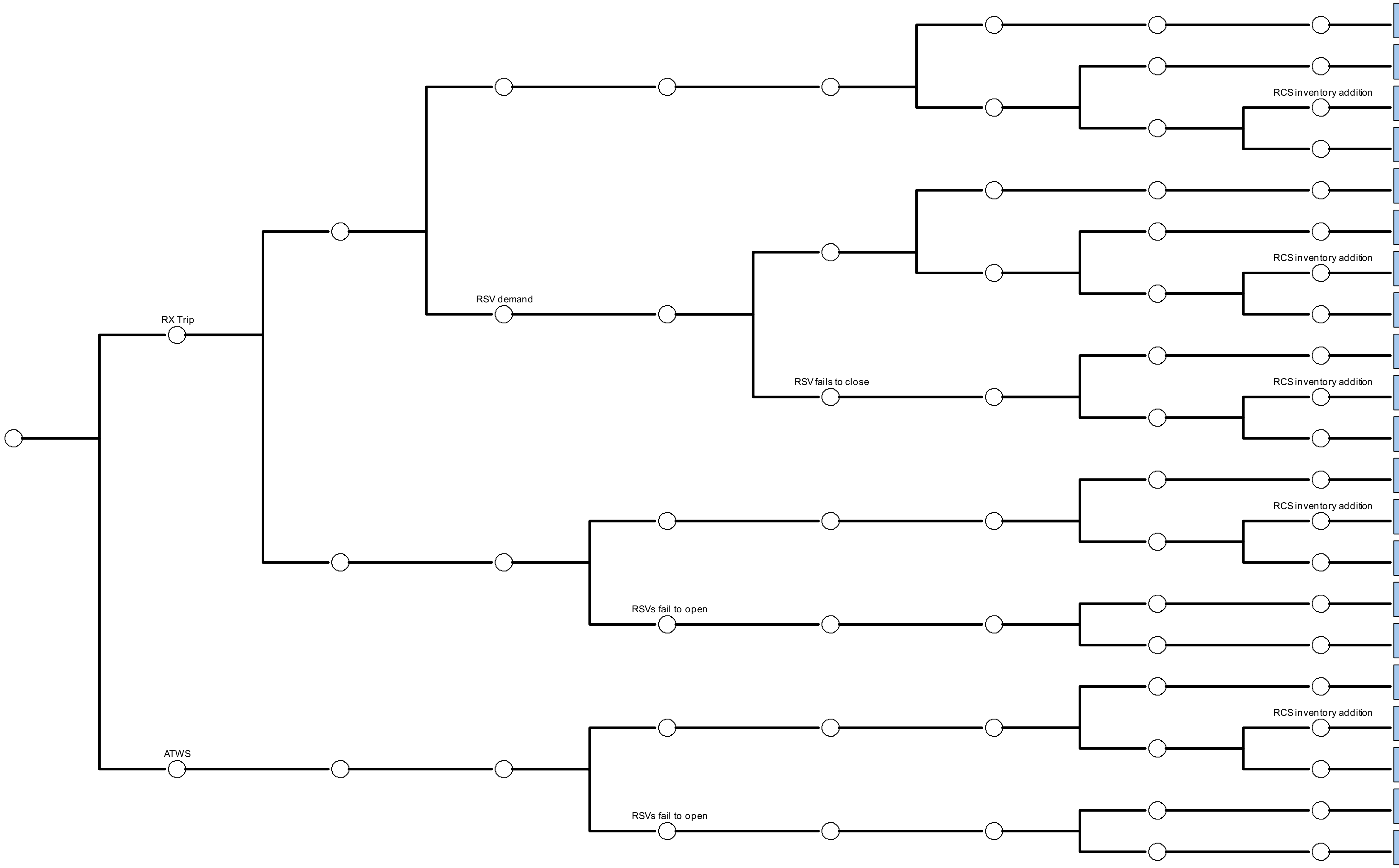
Figure 19.1-7: Event Tree for Steam Generator Tube Failure



#	End State (Phase - PH1)	Comments (Phase - PH1)
1	OK	LSI-03T
2	OK	LCI-03T
3	OK	LLI-02T
4	LEVEL2-ET	LSU-08T
5	OK	LCI-03T
6	OK	LLI-02T
7	LEVEL2-ET	TRN-07T
8	OK	TRN-24T
9	LEVEL2-ET	TRN-08T
10	OK	LSU-06T
11	OK	LSU-07T
12	LEVEL2-ET	LSU-08T
13	OK	LCI-06A
14	OK	LEC-10A
15	LEVEL2-ET	TRN-07T
16	OK	TRN-23A
17	LEVEL2-ET	TRN-08T
18	OK	LLU-04A
19	LEVEL2-ET	LSU-08T

Figure 19.1-8: Event Tree for Secondary Line Break

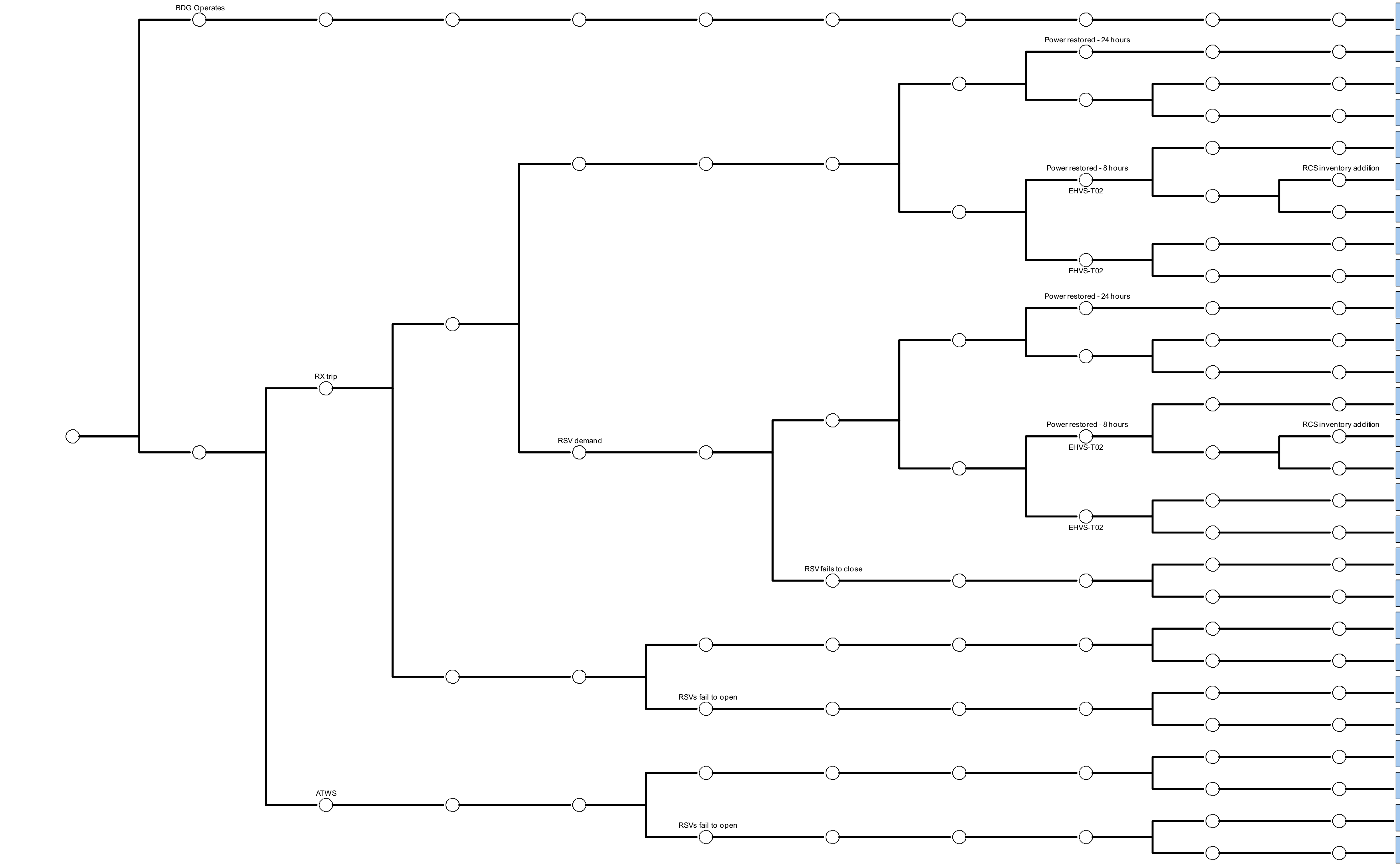
Secondary Side Line Break	Reactor Trip System	DHRS (#1 Train Available)	RCS Reactor Safety Valve Not Demanded to Open	RCS Reactor Safety Valve Opens	RCS Reactor Safety Valve Closes (1 Cycle)	Operations Confirms Shutdown Margin & Bypasses 8 Hour ECCS Timer	ECCS Reactor Vent and Recirculation Valves Open (1 Valve Each)	CVCS for RCS Injection
IE-TGS---FMSLB-UD-	RTS-T01	DHRS-T02	RCS-T05	RCS-T01	RCS-T06	ECCS-T03	ECCS-T01	CVCS-T01



#	End State (Phase - PH1)	Comments (Phase - PH1)
1	OK	TRN-18T
2	OK	LCI-03T
3	OK	LEC-09T
4	LEVEL2-ET	TRN-17T
5	OK	TRN-18T
6	OK	LCI-03T
7	OK	LEC-09T
8	LEVEL2-ET	TRN-17T
9	OK	LCI-03T
10	OK	LMU-02T
11	LEVEL2-ET	TRN-07T
12	OK	LCI-03T
13	OK	LMU-02T
14	LEVEL2-ET	TRN-07T
15	OK	TRN-24T
16	LEVEL2-ET	TRN-08T
17	OK	LCI-06A
18	OK	LEC-10A
19	LEVEL2-ET	TRN-07T
20	OK	TRN-23A
21	LEVEL2-ET	TRN-08T

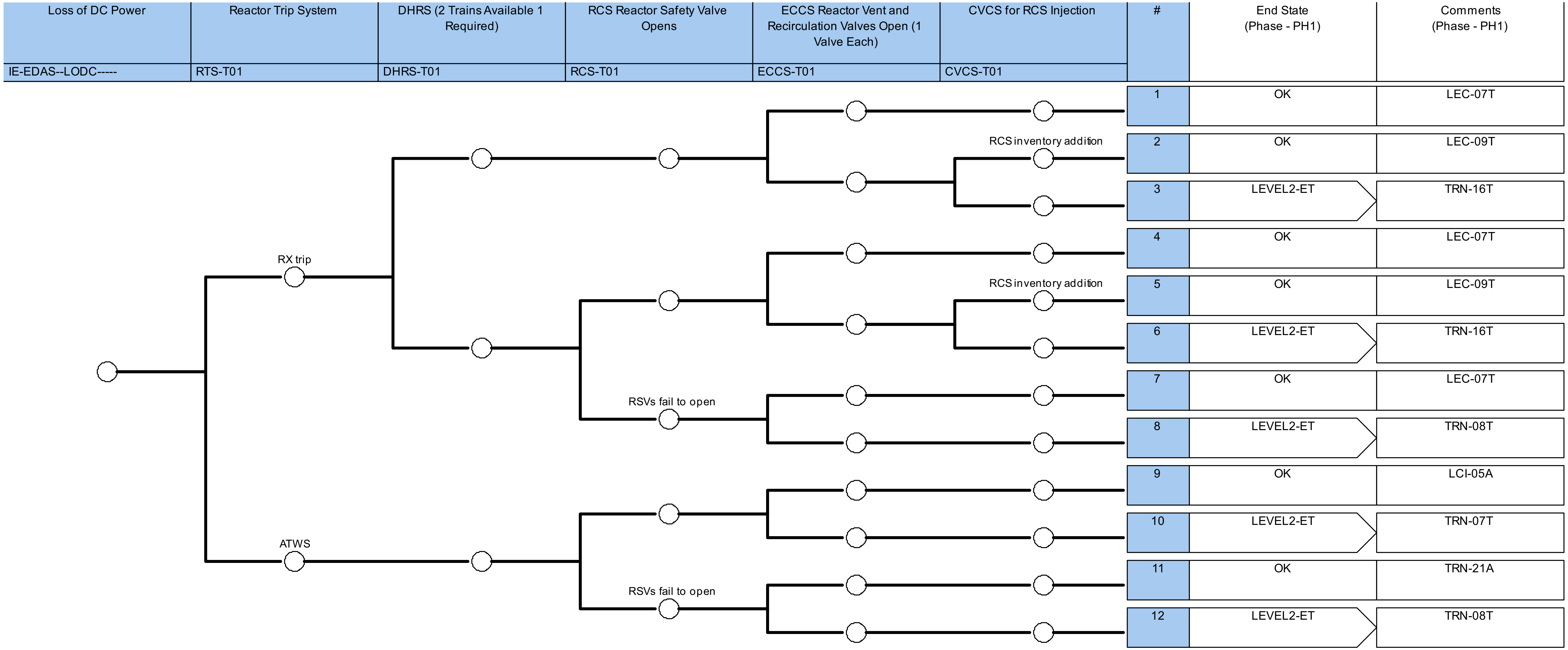
Figure 19.1-9: Event Tree for Loss of Offsite Power

Loss Of Offsite Power	Backup Diesel Generators	Reactor Trip System	DHRS (2 Trains Available 1 Required)	RCS Reactor Safety Valve Not Demanded to Open	RCS Reactor Safety Valve Opens	RCS Reactor Safety Valve Closes (1 Cycle)	Operations Confirms Shutdown Margin & Bypasses 8 Hour ECCS Timer	Offsite Power Recovered (24 Hours)	ECCS Reactor Vent and Recirculation Valves Open (1 Valve Each)	CVCS for RCS Injection
IE-EHVS--LOOP-----	BPSS-T01	RTS-T01	DHRS-T01	RCS-T05	RCS-T01	RCS-T06	ECCS-T03	EHVS-T01	ECCS-T01	CVCS-T01



#	End State (Phase - PH1)	Comments (Phase - PH1)
1	TGS---TRAN--NPC-ET	transfer
2	OK	TRN-18T
3	OK	LEC-07T
4	LEVEL2-ET	TRN-17T
5	OK	TRN-18T
6	OK	LEC-09T
7	LEVEL2-ET	TRN-17T
8	OK	LEC-07T
9	LEVEL2-ET	TRN-17T
10	OK	TRN-18T
11	OK	LEC-07T
12	LEVEL2-ET	TRN-17T
13	OK	TRN-18T
14	OK	LEC-09T
15	LEVEL2-ET	TRN-17T
16	OK	LEC-07T
17	LEVEL2-ET	TRN-17T
18	OK	LCI-03T
19	LEVEL2-ET	TRN-07T
20	OK	LEC-07T
21	LEVEL2-ET	TRN-07T
22	OK	TRN-24T
23	LEVEL2-ET	TRN-08T
24	OK	LCI-06A
25	LEVEL2-ET	TRN-07T
26	OK	TRN-23A
27	LEVEL2-ET	TRN-08T

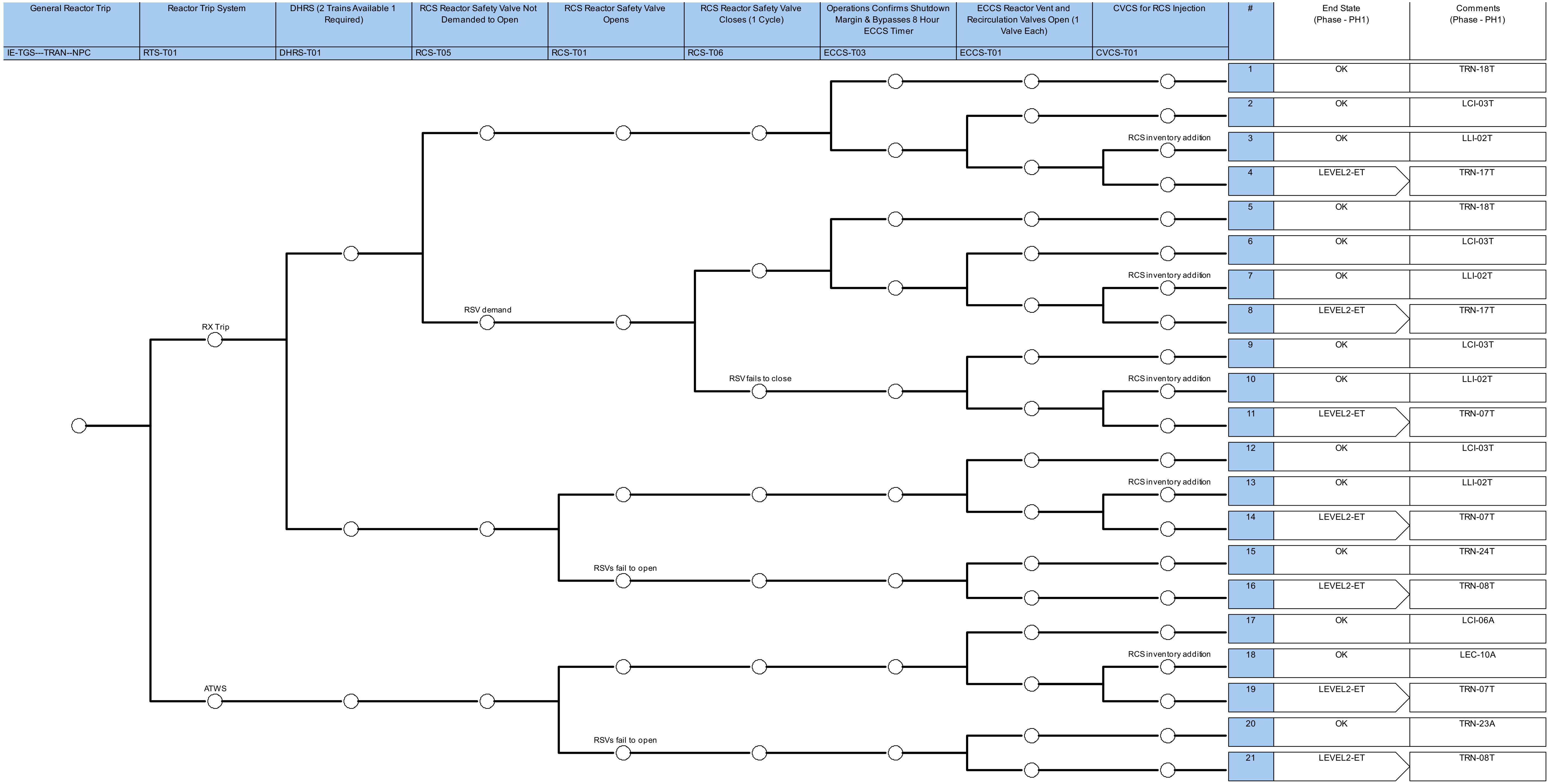
Figure 19.1-10: Event Tree for Loss of Direct Current Power



Loss of DC Power	Reactor Trip System	DHRS (2 Trains Available 1 Required)	RCS Reactor Safety Valve Opens	ECCS Reactor Vent and Recirculation Valves Open (1 Valve Each)	CVCS for RCS Injection
IE-EDAS--LODC-----	RTS-T01	DHRS-T01	RCS-T01	ECCS-T01	CVCS-T01

#	End State (Phase - PH1)	Comments (Phase - PH1)
1	OK	LEC-07T
2	OK	LEC-09T
3	LEVEL2-ET	TRN-16T
4	OK	LEC-07T
5	OK	LEC-09T
6	LEVEL2-ET	TRN-16T
7	OK	LEC-07T
8	LEVEL2-ET	TRN-08T
9	OK	LCI-05A
10	LEVEL2-ET	TRN-07T
11	OK	TRN-21A
12	LEVEL2-ET	TRN-08T

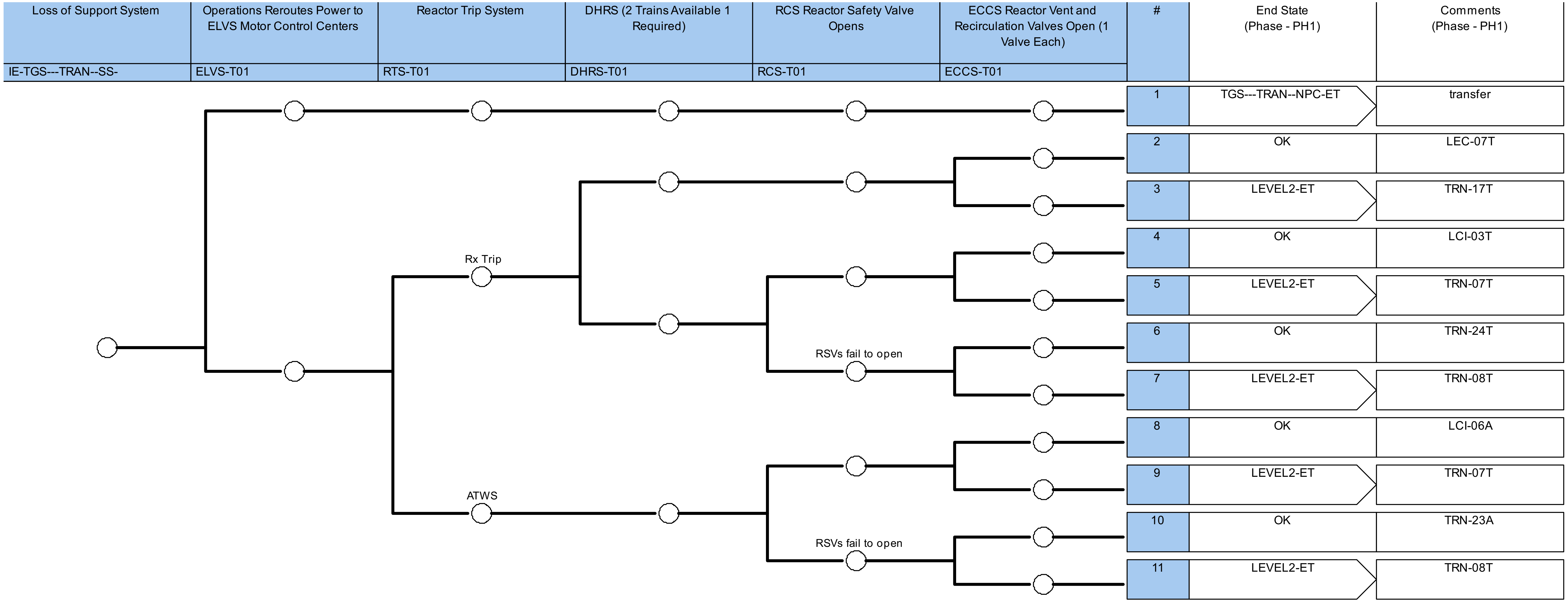
Figure 19.1-11: Event Tree for General Reactor Trip



General Reactor Trip	Reactor Trip System	DHRS (2 Trains Available 1 Required)	RCS Reactor Safety Valve Not Demanded to Open	RCS Reactor Safety Valve Opens	RCS Reactor Safety Valve Closes (1 Cycle)	Operations Confirms Shutdown Margin & Bypasses 8 Hour ECCS Timer	ECCS Reactor Vent and Recirculation Valves Open (1 Valve Each)	CVCS for RCS Injection
IE-TGS---TRAN--NPC	RTS-T01	DHRS-T01	RCS-T05	RCS-T01	RCS-T06	ECCS-T03	ECCS-T01	CVCS-T01

#	End State (Phase - PH1)	Comments (Phase - PH1)
1	OK	TRN-18T
2	OK	LCI-03T
3	OK	LLI-02T
4	LEVEL2-ET	TRN-17T
5	OK	TRN-18T
6	OK	LCI-03T
7	OK	LLI-02T
8	LEVEL2-ET	TRN-17T
9	OK	LCI-03T
10	OK	LLI-02T
11	LEVEL2-ET	TRN-07T
12	OK	LCI-03T
13	OK	LLI-02T
14	LEVEL2-ET	TRN-07T
15	OK	TRN-24T
16	LEVEL2-ET	TRN-08T
17	OK	LCI-06A
18	OK	LEC-10A
19	LEVEL2-ET	TRN-07T
20	OK	TRN-23A
21	LEVEL2-ET	TRN-08T

Figure 19.1-12: Event Tree for Loss of Support System



Loss of Support System	Operations Reroutes Power to ELVS Motor Control Centers	Reactor Trip System	DHRS (2 Trains Available 1 Required)	RCS Reactor Safety Valve Opens	ECCS Reactor Vent and Recirculation Valves Open (1 Valve Each)
IE-TGS---TRAN--SS-	ELVS-T01	RTS-T01	DHRS-T01	RCS-T01	ECCS-T01

#	End State (Phase - PH1)	Comments (Phase - PH1)
1	TGS---TRAN--NPC-ET	transfer
2	OK	LEC-07T
3	LEVEL2-ET	TRN-17T
4	OK	LCI-03T
5	LEVEL2-ET	TRN-07T
6	OK	TRN-24T
7	LEVEL2-ET	TRN-08T
8	OK	LCI-06A
9	LEVEL2-ET	TRN-07T
10	OK	TRN-23A
11	LEVEL2-ET	TRN-08T

Figure 19.1-13: Containment Event Tree

Core Damage Sequences	Core Damage Cutset Mapped to Release Size	Containment Isolation Fails	#	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

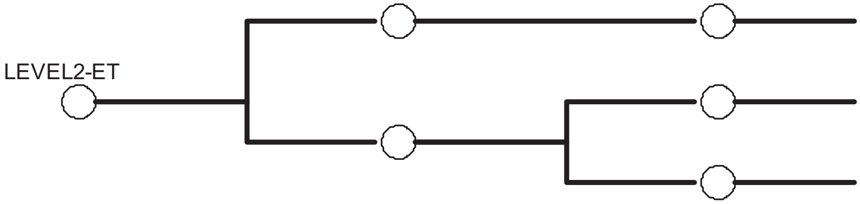


Figure 19.1-14: Representative Seismic Event Tree

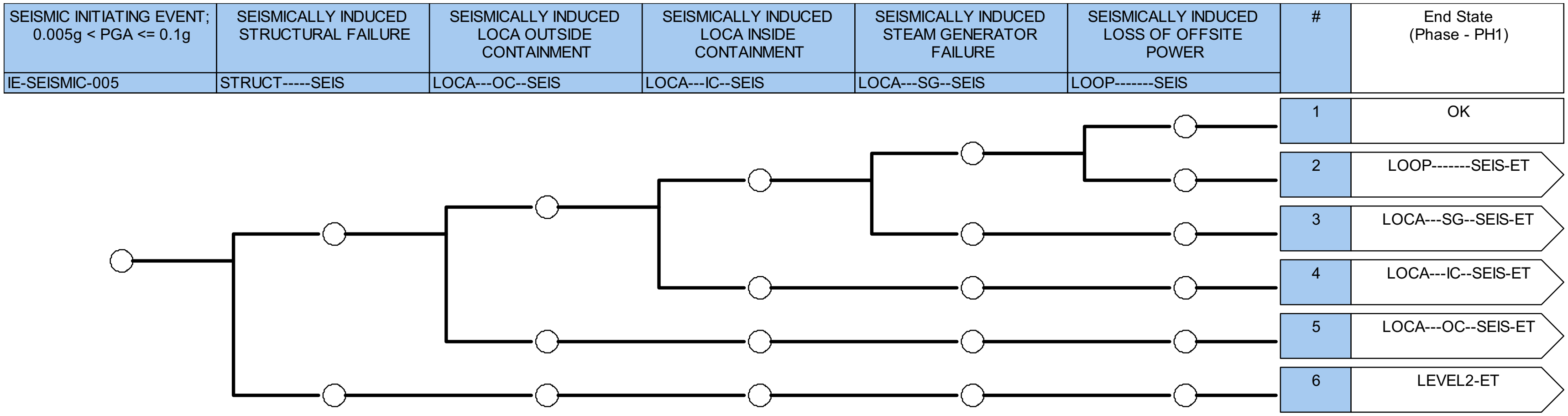
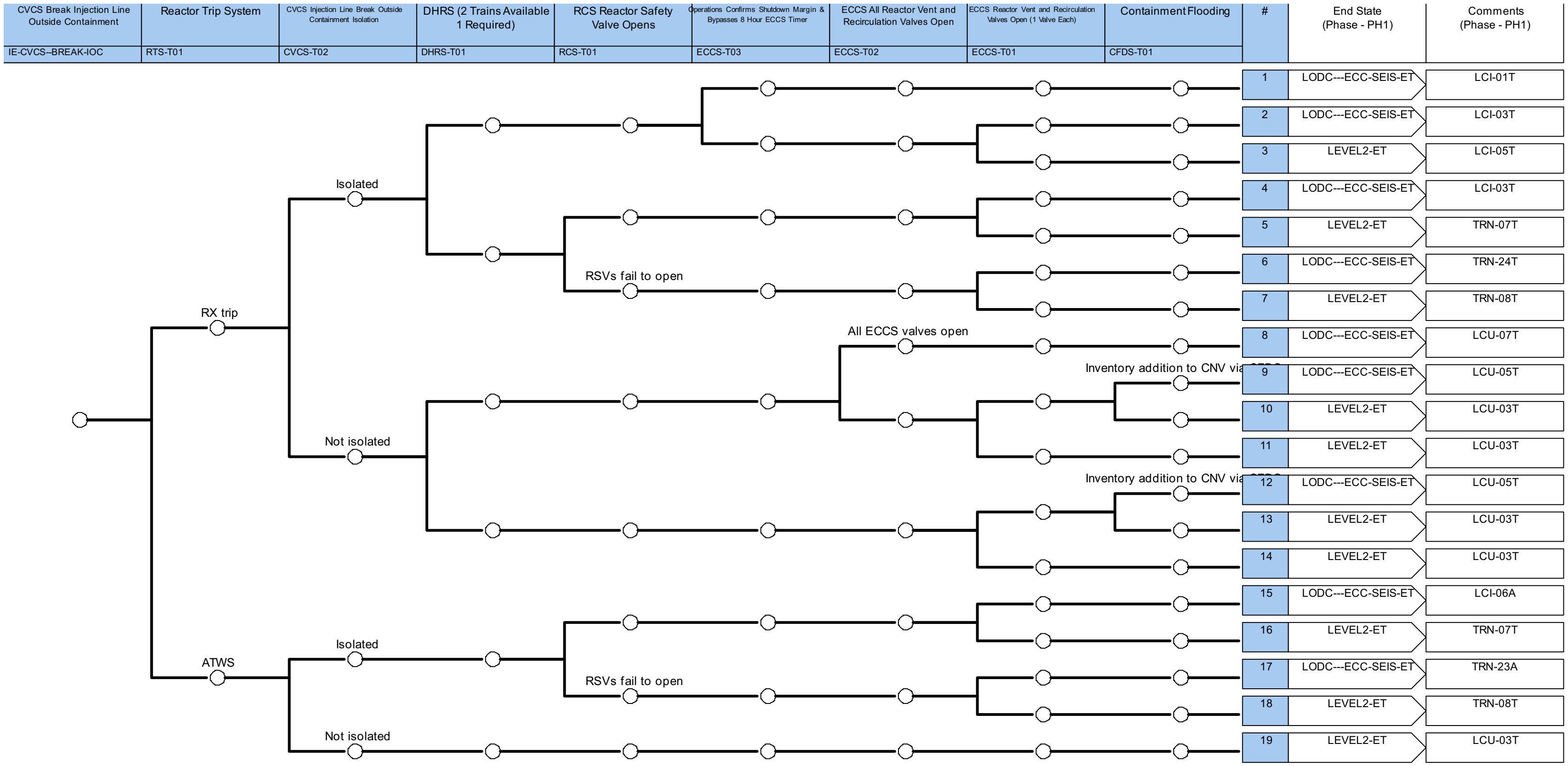

SEISMIC INITIATING EVENT; 0.005g < PGA <= 0.1g
SEISMICALLY INDUCED STRUCTURAL FAILURE
SEISMICALLY INDUCED LOCA OUTSIDE CONTAINMENT
SEISMICALLY INDUCED LOCA INSIDE CONTAINMENT
SEISMICALLY INDUCED STEAM GENERATOR FAILURE
SEISMICALLY INDUCED LOSS OF OFFSITE POWER
#
End State (Phase - PH1)
IE-SEISMIC-005
STRUCT-----SEIS
LOCA---OC--SEIS
LOCA---IC--SEIS
LOCA---SG--SEIS
LOOP-------SEIS
1
OK
2
LOOP-------SEIS-ET
3
LOCA---SG--SEIS-ET
4
LOCA---IC--SEIS-ET
5
LOCA---OC--SEIS-ET
6
LEVEL2-ET

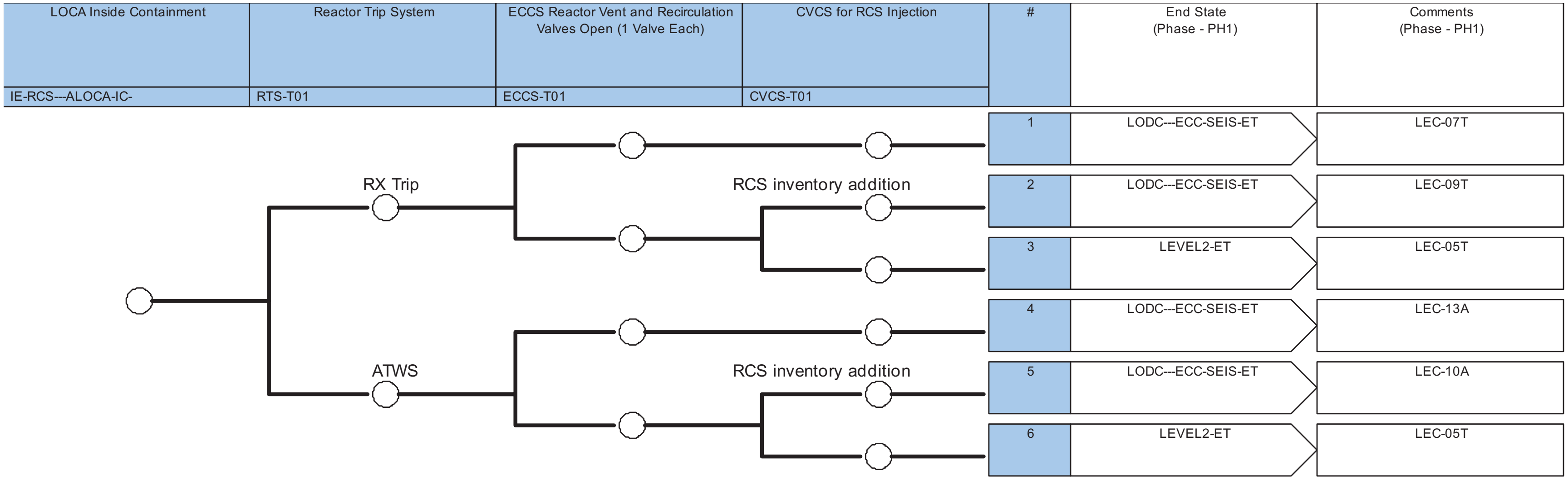
Figure 19.1-15: Seismically Induced Break Outside Containment Event Tree



CVCS Break Injection Line Outside Containment	Reactor Trip System	CVCS Injection Line Break Outside Containment Isolation	DHRS (2 Trains Available 1 Required)	RCS Reactor Safety Valve Opens	Operations Confirms Shutdown Margin & Bypasses 8 Hour ECCS Timer	ECCS All Reactor Vent and Recirculation Valves Open	ECCS Reactor Vent and Recirculation Valves Open (1 Valve Each)	Containment Flooding
IE-CVCS–BREAK-IOC	RTS-T01	CVCS-T02	DHRS-T01	RCS-T01	ECCS-T03	ECCS-T02	ECCS-T01	CFDS-T01

#	End State (Phase - PH1)	Comments (Phase - PH1)
1	LODC---ECC-SEIS-ET	LCI-01T
2	LODC---ECC-SEIS-ET	LCI-03T
3	LEVEL2-ET	LCI-05T
4	LODC---ECC-SEIS-ET	LCI-03T
5	LEVEL2-ET	TRN-07T
6	LODC---ECC-SEIS-ET	TRN-24T
7	LEVEL2-ET	TRN-08T
8	LODC---ECC-SEIS-ET	LCU-07T
9	LODC---ECC-SEIS-ET	LCU-05T
10	LEVEL2-ET	LCU-03T
11	LEVEL2-ET	LCU-03T
12	LODC---ECC-SEIS-ET	LCU-05T
13	LEVEL2-ET	LCU-03T
14	LEVEL2-ET	LCU-03T
15	LODC---ECC-SEIS-ET	LCI-06A
16	LEVEL2-ET	TRN-07T
17	LODC---ECC-SEIS-ET	TRN-23A
18	LEVEL2-ET	TRN-08T
19	LEVEL2-ET	LCU-03T

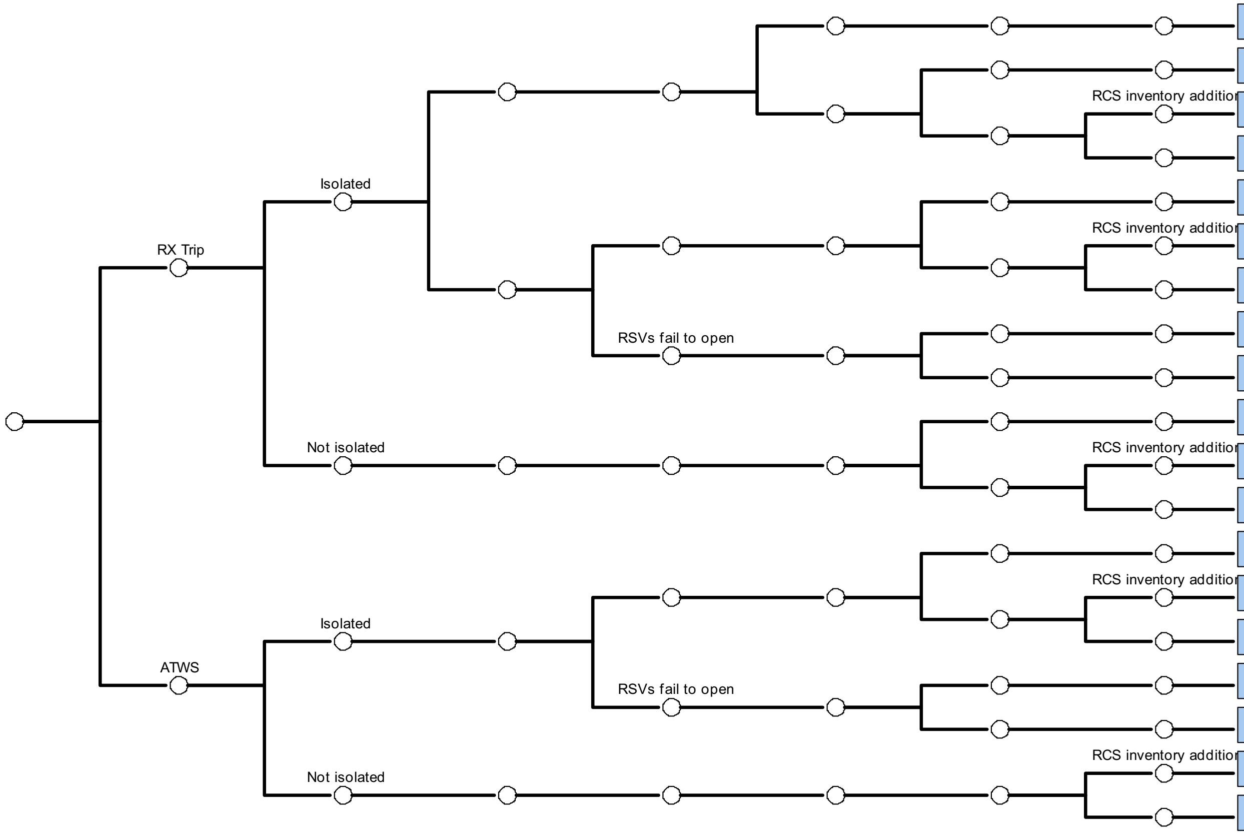
Figure 19.1-16: Seismically Induced Loss-of-Coolant Accident Inside Containment Event Tree



#	End State (Phase - PH1)	Comments (Phase - PH1)
1	LODC---ECC-SEIS-ET	LEC-07T
2	LODC---ECC-SEIS-ET	LEC-09T
3	LEVEL2-ET	LEC-05T
4	LODC---ECC-SEIS-ET	LEC-13A
5	LODC---ECC-SEIS-ET	LEC-10A
6	LEVEL2-ET	LEC-05T

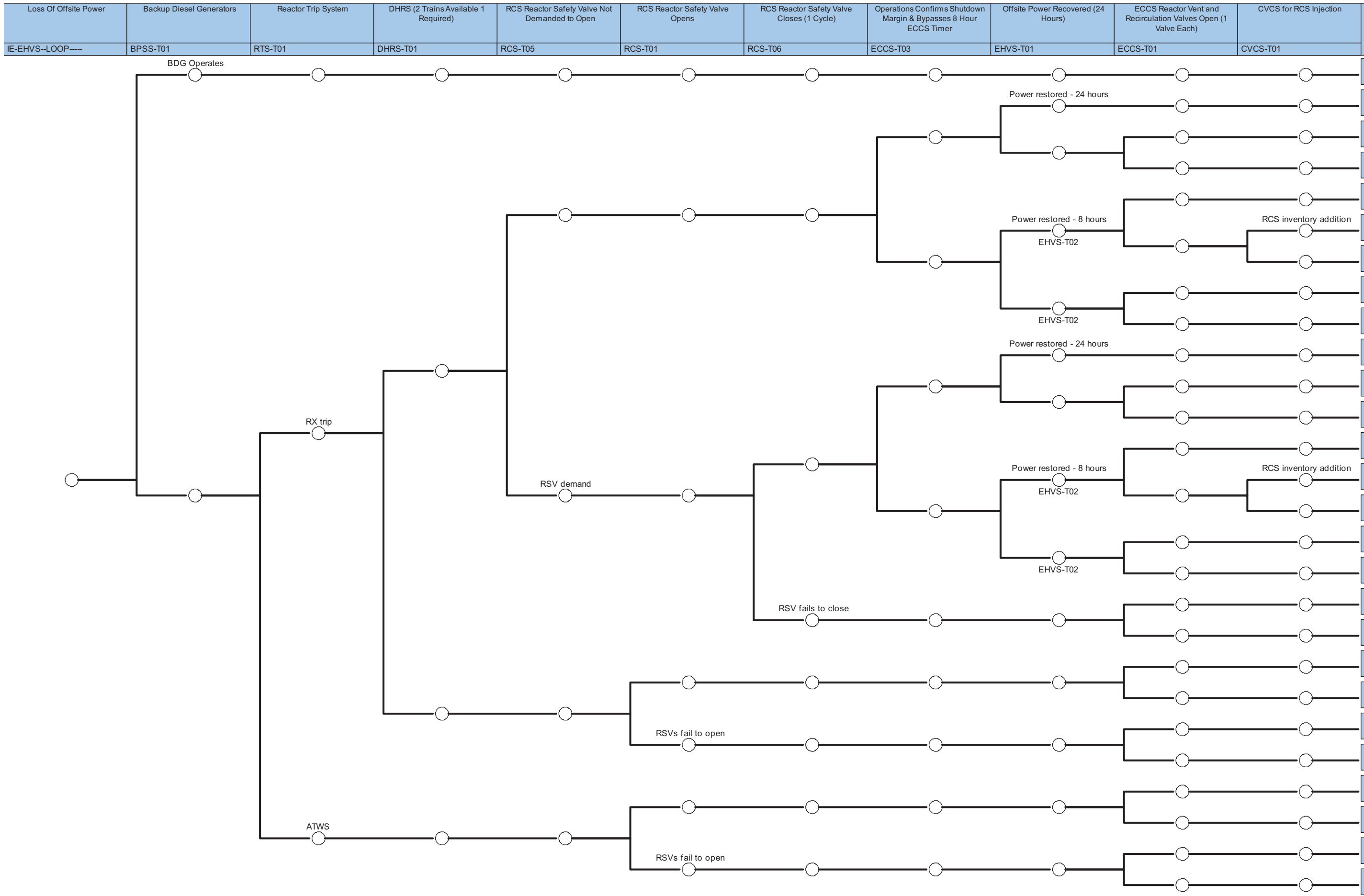
Figure 19.1-17: Seismically Induced Steam Generator Tube Failure Event Tree

Steam Generator #2 Tube Failure	Reactor Trip System	SG #2 Tube Failure Isolated	DHRS (#1 Train Available)	RCS Reactor Safety Valve Opens	Operations Confirms Shutdown Margin & Bypasses 8 Hour ECCS Timer	ECCS Reactor Vent and Recirculation Valves Open (1 Valve Each)	CVCS for RCS Injection
IE-MSS--ALOCA-SG-	RTS-T01	RCS-T04	DHRS-T02	RCS-T01	ECCS-T03	ECCS-T01	CVCS-T01



#	End State (Phase - PH1)	Comments (Phase - PH1)
1	LODC---ECC-SEIS-ET	LSI-03T
2	LODC---ECC-SEIS-ET	LCI-03T
3	LODC---ECC-SEIS-ET	LLI-02T
4	LEVEL2-ET	LSU-08T
5	LODC---ECC-SEIS-ET	LCI-03T
6	LODC---ECC-SEIS-ET	LLI-02T
7	LEVEL2-ET	TRN-07T
8	LODC---ECC-SEIS-ET	TRN-24T
9	LEVEL2-ET	TRN-08T
10	LODC---ECC-SEIS-ET	LSU-06T
11	LODC---ECC-SEIS-ET	LSU-07T
12	LEVEL2-ET	LSU-08T
13	LODC---ECC-SEIS-ET	LCI-06A
14	LODC---ECC-SEIS-ET	LEC-10A
15	LEVEL2-ET	TRN-07T
16	LODC---ECC-SEIS-ET	TRN-23A
17	LEVEL2-ET	TRN-08T
18	LODC---ECC-SEIS-ET	LLU-04A
19	LEVEL2-ET	LSU-08T

Figure 19.1-18: Seismically Induced Loss of Offsite Power Event Tree



#	End State (Phase - PH1)	Comments (Phase - PH1)
1	TGS---TRAN--NPC-ET	transfer
2	OK	TRN-18T
3	OK	LEC-07T
4	LEVEL2-ET	TRN-17T
5	OK	TRN-18T
6	OK	LEC-09T
7	LEVEL2-ET	TRN-17T
8	OK	LEC-07T
9	LEVEL2-ET	TRN-17T
10	OK	TRN-18T
11	OK	LEC-07T
12	LEVEL2-ET	TRN-17T
13	OK	TRN-18T
14	OK	LEC-09T
15	LEVEL2-ET	TRN-17T
16	OK	LEC-07T
17	LEVEL2-ET	TRN-17T
18	OK	LCI-03T
19	LEVEL2-ET	TRN-07T
20	OK	LEC-07T
21	LEVEL2-ET	TRN-07T
22	OK	TRN-24T
23	LEVEL2-ET	TRN-08T
24	OK	LCI-06A
25	LEVEL2-ET	TRN-07T
26	OK	TRN-23A
27	LEVEL2-ET	TRN-08T

Figure 19.1-19: Seismically Induced Loss of DC Power Event Tree

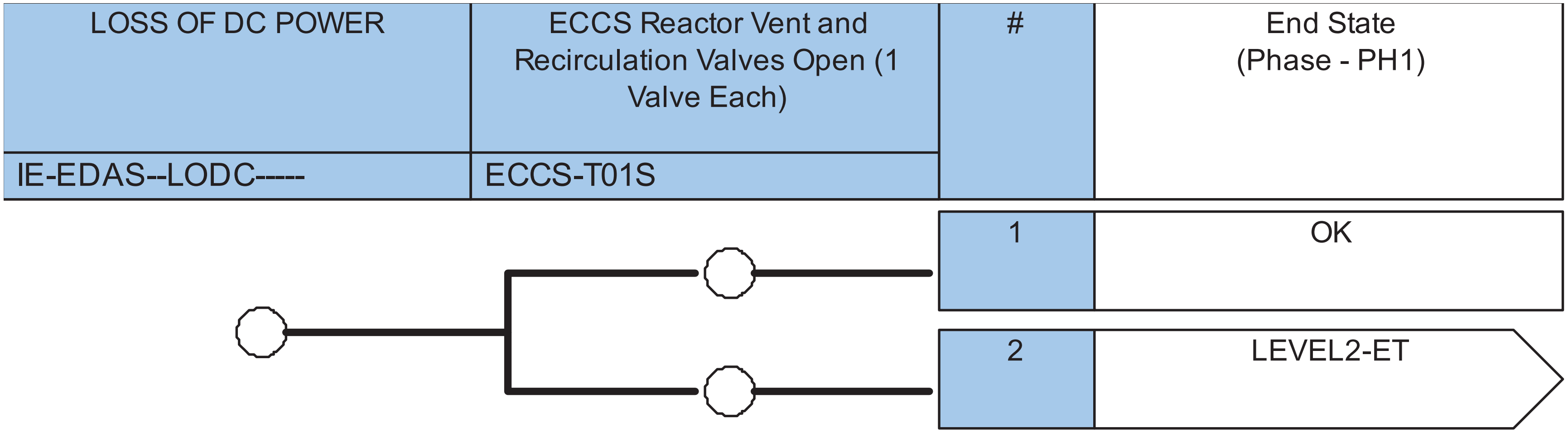


Figure 19.1-20: Fire Probabilistic Risk Assessment Event Tree FIRE-4-ECCS

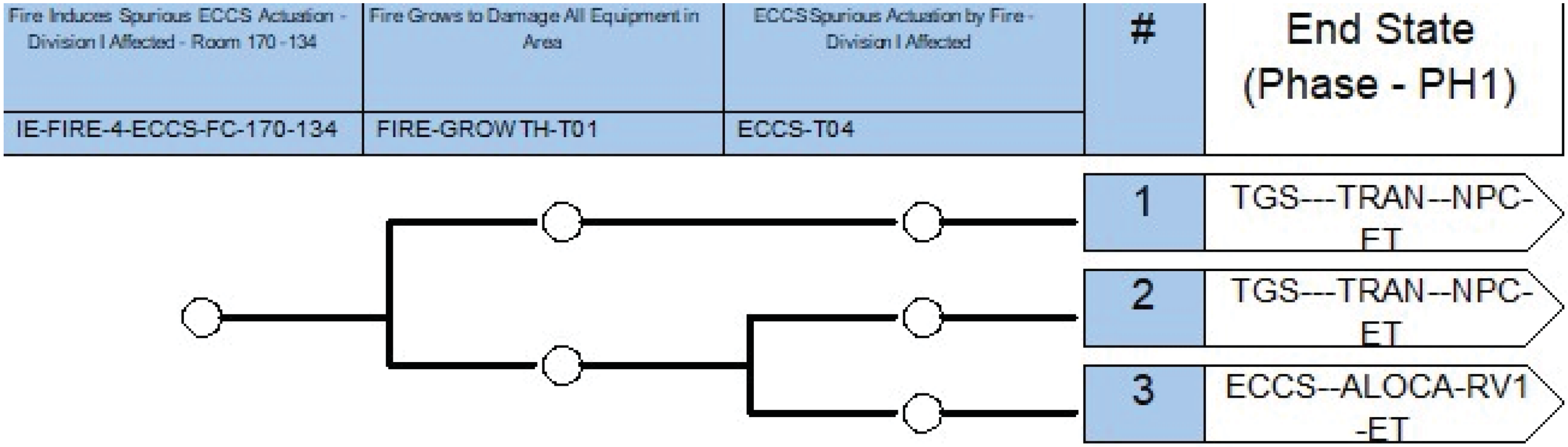

Fire Induces Spurious ECCS Actuation - Division I Affected - Room 170 -134
IE-FIRE-4-ECCS-FC-170-134
Fire Grows to Damage All Equipment in Area
FIRE-GROWTH-T01
ECCS Spurious Actuation by Fire - Division I Affected
ECCS-T04
#
End State (Phase - PH1)
1
TGS---TRAN--NPC-ET
2
TGS---TRAN--NPC-ET
3
ECCS--ALOCA-RV1-ET

Figure 19.1-21: Internal Flooding in Reactor Building

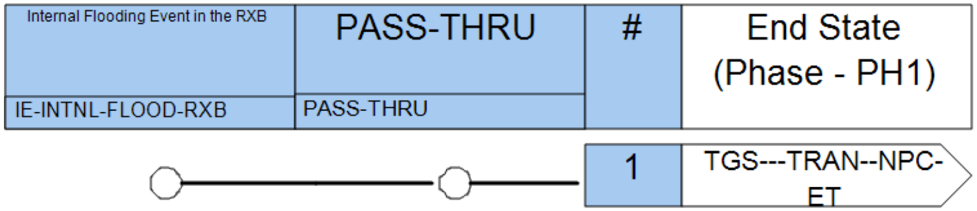


Figure 19.1-22: Internal Flooding Outside Reactor Building

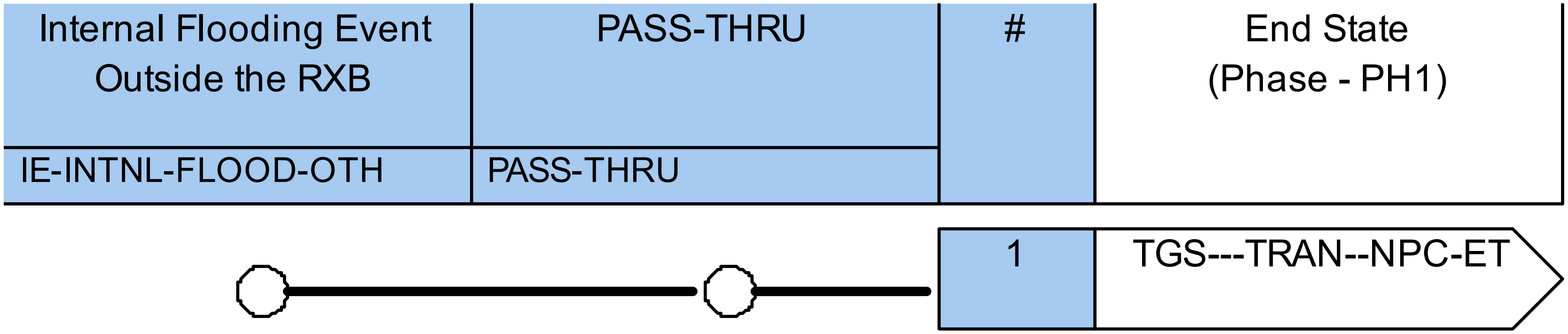


Figure 19.1-23: External Flooding Event Tree

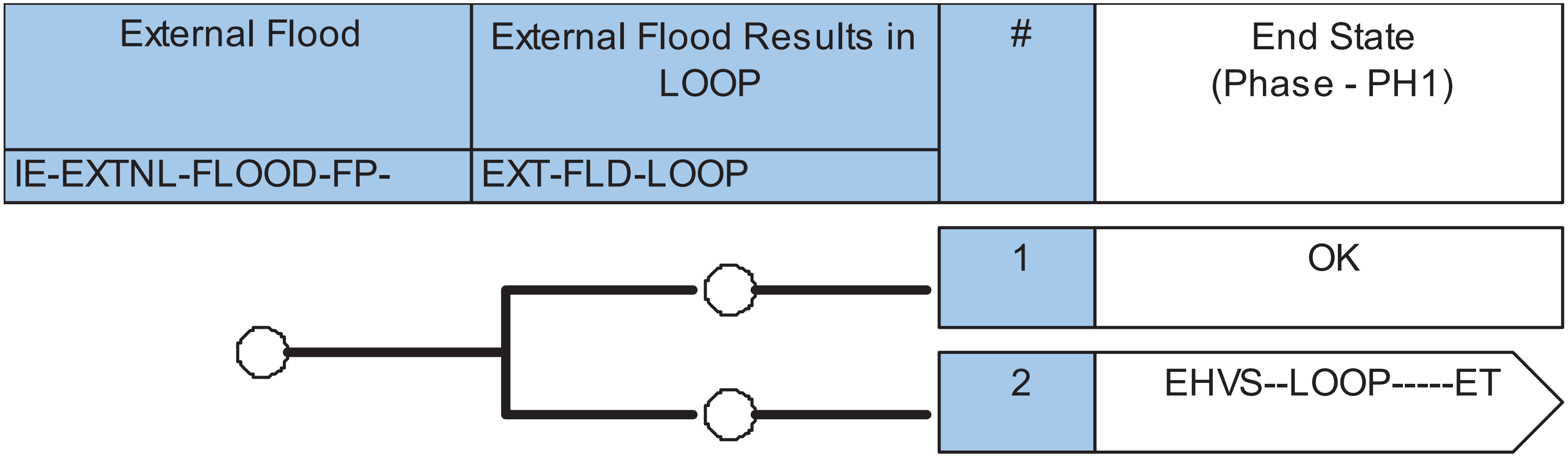


Figure 19.1-24: High-Winds (Tornado) Event Tree

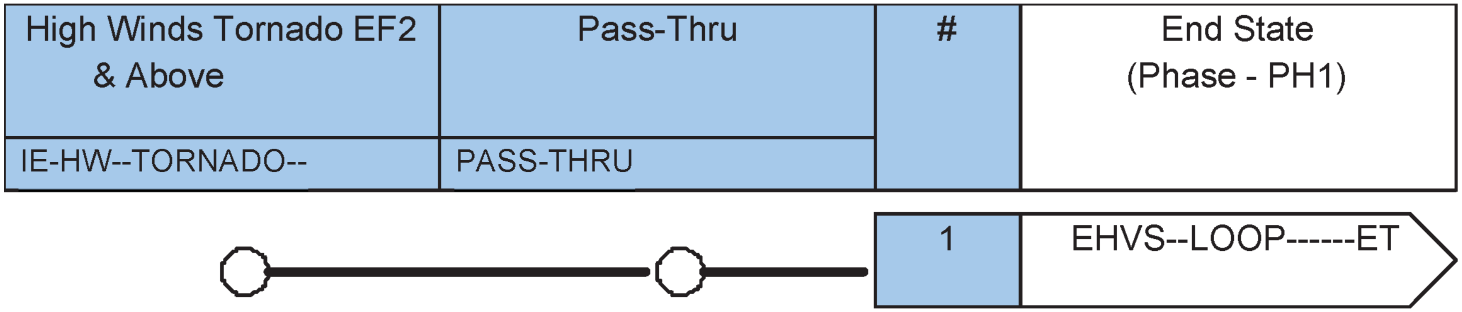


Figure 19.1-25: High-Winds (Hurricane) Event Tree

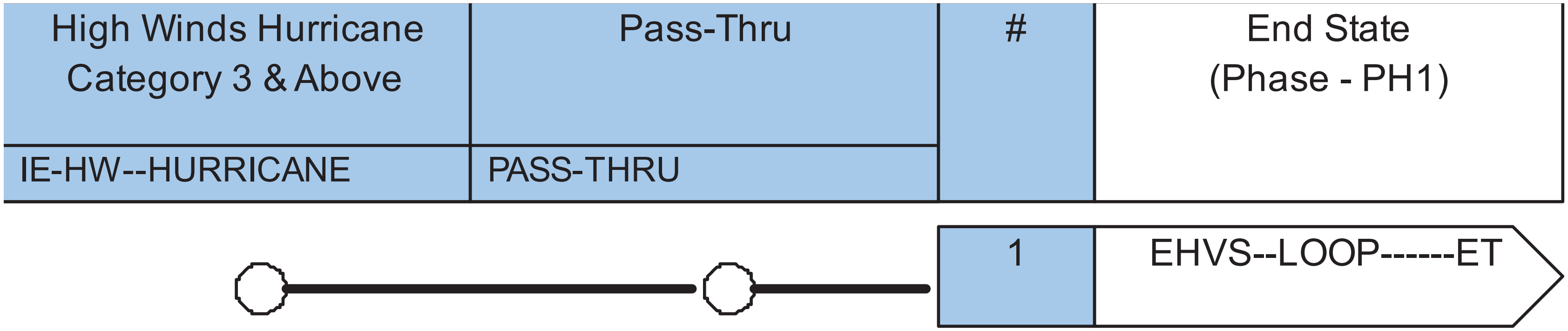


Figure 19.1-26: POS1 Transfer to Spurious Opening of an ECCS Valve (Representative)

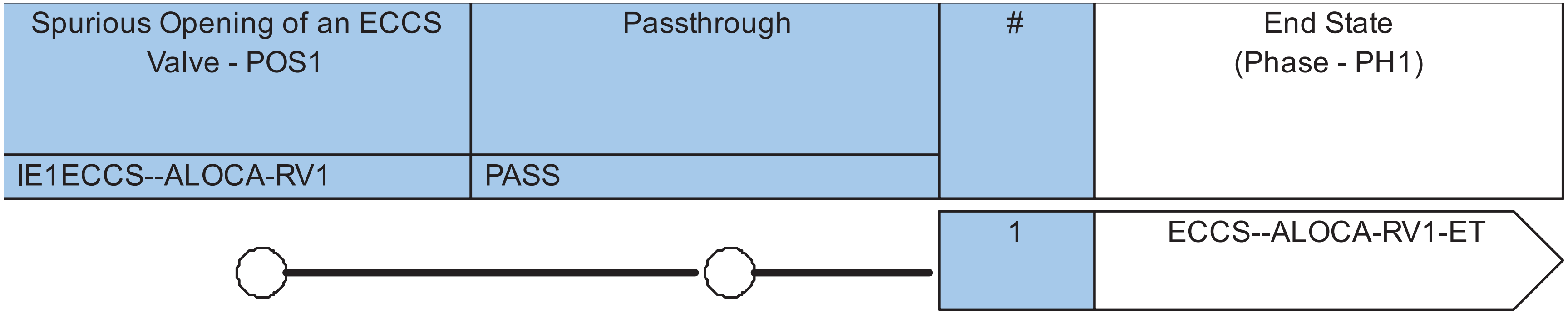


Figure 19.1-27: Event Tree for Module Drop

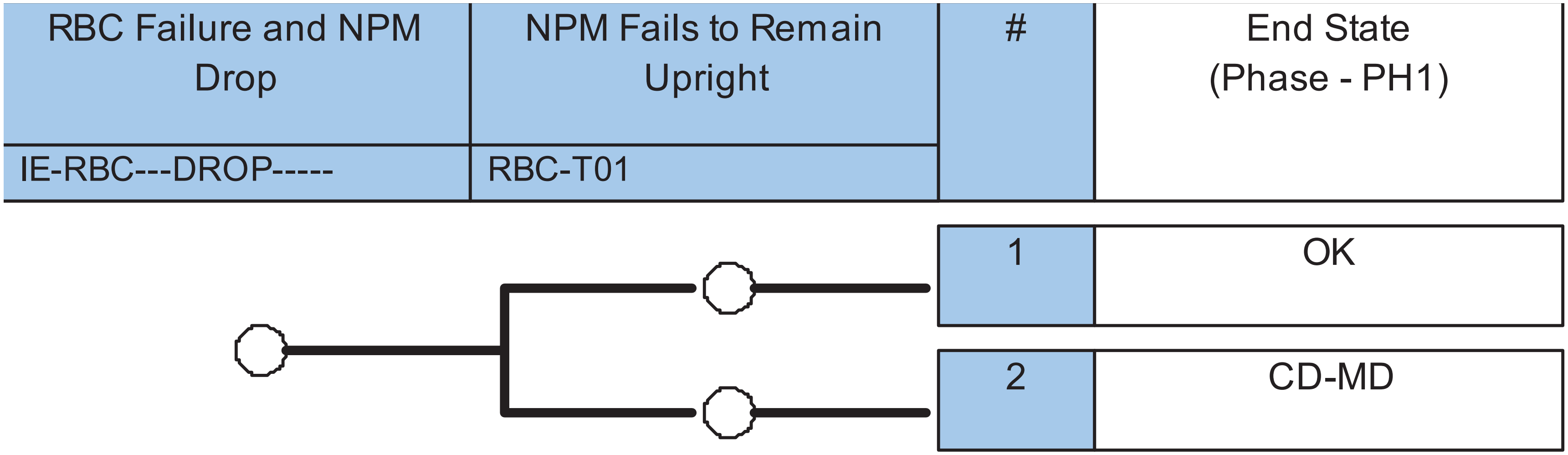
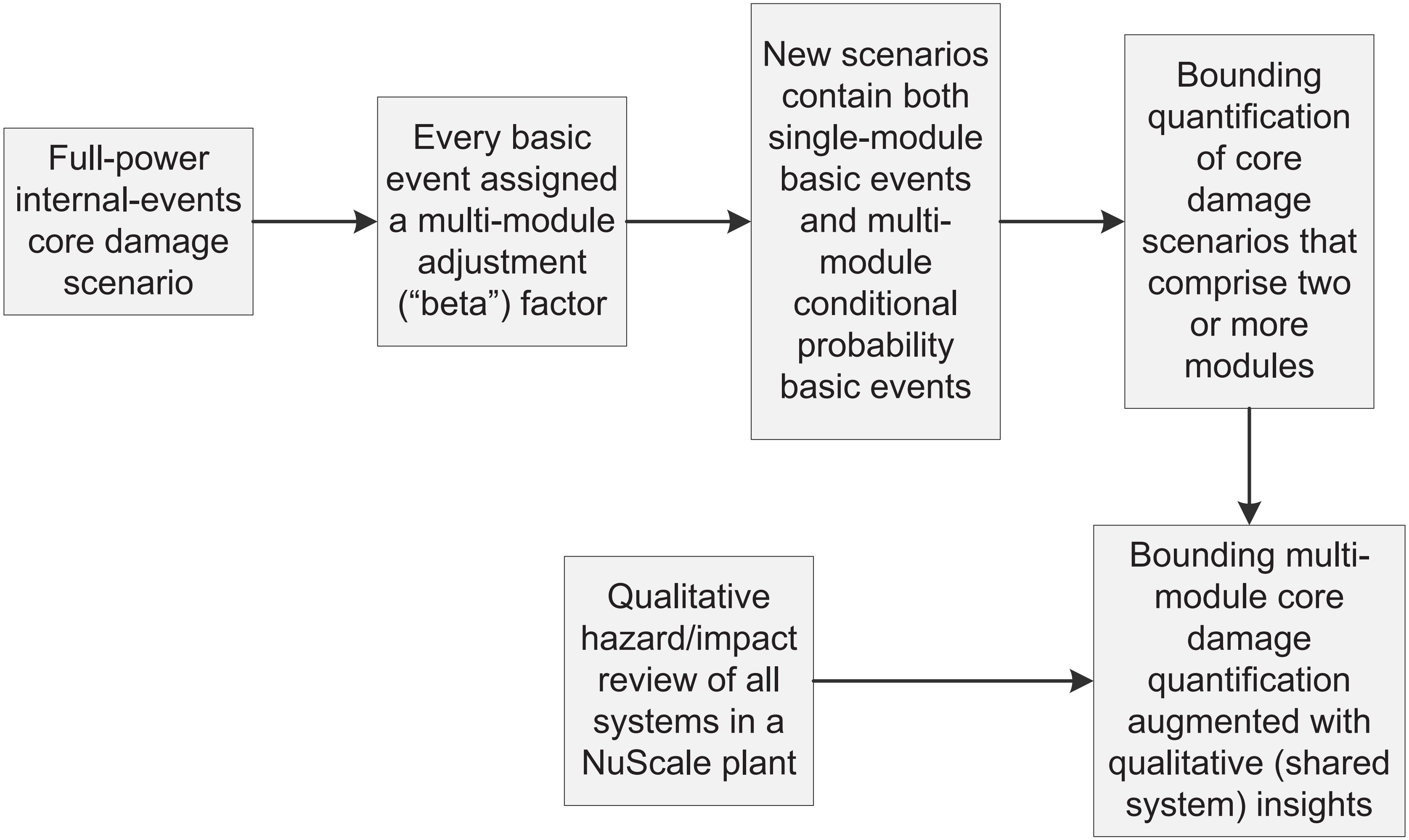


Figure 19.1-28: Multi-Module Assessment Approach



Full-power internal-events core damage scenario

Every basic event assigned a multi-module adjustment (“beta”) factor

New scenarios contain both single-module basic events and multi-module conditional probability basic events

Bounding quantification of core damage scenarios that comprise two or more modules

Bounding multi-module core damage quantification augmented with qualitative (shared system) insights

Qualitative hazard/impact review of all systems in a NuScale plant

19.2 Severe Accident Evaluation

This section describes NuScale Power Plant US460 standard design features to prevent and mitigate potential severe accidents in accordance with the requirements in 10 CFR 52.137(a)(23). This section also addresses specific severe accident issues identified in SECY-90-016 (1990) and SECY-93-087 (1993). 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 NPM configurations do not introduce unique severe accident progression phenomena within each CNV.

19.2.1 Introduction

As discussed in Section 19.1, the Level 2 probabilistic risk assessment (PRA) evaluates severe accident sequences that result in core damage for the likelihood of challenging containment and resulting in a large radionuclide release. The following sections discuss potential severe accident phenomena that could challenge containment. The Level 2 PRA evaluates phenomena using fundamental physics modeling with conservative assumptions. Potential challenges to containment integrity are identified from

- Section 19.0 of the Standard Review Plan (NUREG-0800, Rev. 3).
- SECY-90-016.
- SECY-93-087.
- The American Society of Mechanical Engineers (ASME)/ANS PRA Standard (Reference 19.2-1).
- NUREG/CR-2300 (1983).
- NUREG/CR-6595 (2004).

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 an NPM with regard to these selected beyond-design-basis events. If the event is applicable to the design, it is addressed from a probabilistic perspective, as described in each discussion.

Section 19.2.2.6 summarizes additional design capability for severe accident prevention.

19.2.2.1 Anticipated Transient Without Scram

The requirements of 10 CFR 50.62 are addressed in Section 15.8. From a probabilistic perspective, the probability of an ATWS event is several orders of magnitude below the SECY-83-293 safety goal of 1 E-5/year. To provide insights into the NPM response to postulated ATWS events, NRELAP5 modeling is performed. For ATWS sequences that do not result in core damage:

- 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 prevent core damage.
- the peak containment pressure does not exceed the ultimate CNV failure pressure.
- return to power may occur, but core damage, as defined in Section 19.1.4, does not occur.

Event trees identify potential ATWS sequences, 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. In the design, the RCS is internal to the RPV and, because it relies on natural circulation, does not include reactor coolant pumps. There is no NPM configuration that requires the RCS coolant inventory to be reduced to support maintenance. Thus, mid-loop operation is not applicable to the design and there is not an analogous configuration.

19.2.2.3 Station Blackout

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 a station blackout (SBO) with no reliance on emergency on-site or off-site AC power.

The accident sequence discussions for the loss of direct current (DC) power initiating event, EDAS--LODC, and the loss of off-site power initiating event, EHVS--LOOP, provided in Section 19.1.4, illustrate the unique capability of the design with respect to loss of DC power and to loss of all AC power (i.e., on-site and off-site sources), respectively.

19.2.2.4 Fire Protection

The design includes the following features to cope with potential fires that could affect NPM 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 that 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
- no electrical power requirement for mitigating design-basis events as safety systems are fail-safe on loss of power

Section 9.5.1 addresses conformance with applicable codes and standards. The risk associated with internal fires is evaluated 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 design does not have low-pressure systems connected to the RCS. Hence, the PRA does not use the term “interfacing systems LOCA.” The term "piping breaks outside containment" is applicable to the design. The 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 discussed in 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). 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.

19.2.2.6 Other Severe Accident Preventive Features

The 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) because of the reduction of potential accidents, such as LOCAs initiated by pipe breaks, due to the reduced number of components and limited external piping connections.
- The response to LOCAs and pipe breaks is simplified because inventory makeup from external sources is not required to prevent core uncovery (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 because of its simplified, fail-safe, electric power-independent design.
- The passive ECCS contributes to low CDF because of its simplified, fail-safe, electric power-independent design.
- The below-grade reactor pool contributes to low CDF by serving as the ultimate heat sink (UHS). With the NPMs partially 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 for mitigation of a severe accident resulting in core damage. The sections discuss 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.

19.2.3.1 Overview of the Containment Design

Section 6.2 describes the design of the CNV that encapsulates each RPV. The CNV provides for the retention of reactor coolant inventory to support ECCS function. The reactor coolant that collects in the CNV returns to the RPV by natural circulation through open reactor vent valves (RVVs) and reactor recirculation valves (RRVs). 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 needed.

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 limits the capability for combustion in the event of hydrogen generation due to a severe accident.

Following an ECCS actuation, boron in the CNV is recirculated into the reactor core to ensure shutdown margin under cold conditions. The CNV is also 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) are evaluated to provide insights into the potential for RPV failure and resultant containment challenges, such as hydrogen generation, high-pressure melt ejection (HPME), and fuel-coolant interaction (FCI). Additionally, very low-probability containment bypass scenarios are evaluated to provide insights into the CNV lower-head performance and potential for mitigation. The thermal-hydraulic simulations, using the MELCOR code, model potential severe accident sequences and identify the limiting challenges to the RPV and the CNV. In some situations, the sequence simulated for severe-accident considerations differs from the representative core damage sequence in the Level 1 event trees. This difference 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 that ECCS may fail because of recirculation valve or vent valve failure. Both failure modes are considered, but the NPM response differs depending on which failure occurs. Failure of the RVVs to open results in a shorter time to core damage, whereas failure of the RRVs to open results in a longer time to core damage, but more severe core damage.

The set of sequences selected for simulation represents the spectrum of conditions 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 19.2-1 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 both RVVs opening while both 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. 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 that 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 19.2-2 provides key events and associated timing. A total of 191.5 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. In this case the failure mode of the ECCS is all four valves failing to open. This failure mode is the least credible mode. The two cases are otherwise identical. This case results in the shortest time for core damage for cases involving an intact containment with total fuel relocation.

Table 19.2-3 provides key events and associated timing. A total of 202.9 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 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 RVV 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). 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 19.2-4 provides key events and associated timing. The timing of key events indicates that a vapor-space LOCA progresses slower than a liquid-space LOCA. A total of 183.4 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 LEC-05T-00

Case LEC-05T-00 is a variation of LEC-06T-00, however, it is initiated by the spurious actuation of a single RRV. With both RRVs open and both RVVs closed, this case accelerates the time to core damage and the onset of fuel relocation. Table 19.2-5 provides key events and associated timing. 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. This case bounds the most rapid time to core damage for a liquid-space LOCA in containment.

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 fails to reclose, creating a LOCA into the containment. Upon demand, all four ECCS valves fail to open.

Table 19.2-6 provides key events and associated timing. A total of 230.7 lbm of hydrogen is generated. The RPV pressurizes to the RSV setpoint, but does not exceed design pressure, nor does the CNV; 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 break 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. Although improbable and artificial (in the sense that the CNV is already bypassed and, hence, the containment function is already failed), this case is included to evaluate the CNV performance when subjected to thermal attack from core debris upon a postulated RPV lower-head failure.

Table 19.2-7 provides key events and associated timing. A total of 126.4 lbm of hydrogen is produced. Failure of the RPV lower head transports 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.

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 is postulated to penetrate 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. In an unmitigated severe accident with complete core uncovery, core materials heat up, degrade, and eventually relocate to the lower RPV plenum. Relocation occurs when the internal structures supporting the core materials yield at high temperature. However, if heat removal on the outside of the lower RPV head is effective, the lower head remains sufficiently cool to remain intact and achieve in-vessel retention (IVR) of the core debris in the RPV.

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 classified as large release sequences. Core relocation is illustrated in Figure 19.2-1. Under these circumstances,

- Heat generating core materials relocated to the RPV lower plenum impose a heat load on the inner surface of the lower head.
- The external surface of the lower head is cooled by water in the CNV.

- The water pool in the CNV is cooled by the reactor pool through the CNV shell.
- The RPV is depressurized (i.e., same pressure as the CNV).
- The gas space in the NPM is composed of hydrogen at elevated pressure, causing the CNV water pool to be subcooled.

From the perspective of retaining a damaged core in the RPV, the concern is that structural failure may occur at a temperature lower than the melting temperature of steel because of loss of strength of the steel wall. Thus, the in-vessel retention-RPV analysis considers the coolability of the relocated core material. The heat flux to the RPV lower head from the relocated core debris is a primary consideration in this regard. The distribution of the heat flux over the RPV lower head depends on the physical state (molten or solid) and the configuration of the relocated debris in the RPV lower plenum. Reactor pressure vessel integrity is evaluated by comparing the local heat flux to the flux needed to produce a departure from nucleate boiling, which is the critical heat flux (CHF).

The major elements of the evaluation are

- identification of potential core debris configurations.
- evaluation of heat fluxes from the relocated core debris to the RPV wall inner surface.
- determination of appropriate CHF values for the RPV wall outer surface.

Evaluation of Potential Core Debris Configurations in the Reactor Pressure Vessel

The profile of the heat flux associated with the core debris bed is dependent on the physical state and configuration of the relocated core materials. The physical state may be molten, solid, or a solid-liquid slurry. If the relocated core debris forms a molten pool in the lower plenum, the heat flux imposed on the inside surface of the RPV lower head depends on the flow characteristics of the molten pool. If the debris bed forms a solid block, the heat flux to the RPV lower head would be maximum at the RPV bottom-center and minimum at the edge, where the top of the debris meets the RPV lower head. A solid-liquid slurry transfers heat from the solid oxides to the surface of the lower head, maintaining sufficiently low temperatures for the oxides to remain solid. This configuration is similar to the molten pool configuration in that heat transfer to the lower head is driven by convective flows that result in peak heat fluxes at the edge of the debris that decrease towards the bottom of the lower head. The physical state and configuration also determine the metallic “focusing” effect. This effect results from oxidic and metallic materials segregating in a molten pool, forming a lower oxide pool and an upper metallic layer. Although the metal layer does not generate significant quantities of heat, it can thermally challenge the section of RPV wall that it is in contact with because the convective forces and high thermal conductivity of the molten metallic layer can efficiently transfer heat from the top of the oxide layer onto a relatively small surface area along the RPV wall.

Theofanous (Reference 19.2-3) and Rempe (Reference 19.2-4) provide a range of potential debris bed configurations, based on an assumed molten core, for which reference data are available:

- Configuration 1 is a layered configuration that is reached after considerable evolution of the core melt and core debris has relocated to the RPV lower head. A layered configuration is established with a molten oxide layer at the bottom and a molten metal layer on top. The oxides consist primarily of uranium dioxide, which is denser than the metals that consist primarily of unoxidized steel and zirconium. The heat is generated in the UO_2 layer because of 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.
- Configuration 2 is an intermediate configuration that is postulated to occur upon failure of a core-internal crucible, which 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. Upon rupture of this crucible, a molten jet penetrates the core peripheral structures and impinges on the RPV surface, imposing a localized dynamic heat flux that is enhanced due to forced convection and agitation by the jet.
- Configuration 3 is an intermediate state that is similar to Configuration 1 except that it is considered earlier in the core melt progression. The relevant characteristic is that it has a comparatively thin metal layer because this state is postulated to occur prior to large quantities of steel components melting and contributing to the molten pool. The thin metallic layer could result in a more challenging focusing effect. This configuration develops as a result of localized relocations through the reflector sidewalls (i.e., a consequence of the dynamic melt ejection characterized by Configuration 2).
- Configuration 4 represents an end state that develops from Configuration 3. At a time after Configuration 3 develops, a second relocation occurs due to failure of the bottom crust of the in-core pool. The phased relocation results in four distinct layers (from the bottom: oxide, metal, oxide, metal). The lower metal layer is sealed in place by frozen oxide crusts. The unique challenge presented by this configuration is that the lower metal layer is heated by the overlying and underlying oxide layers and focuses the heat load on a small area of the RPV wall.
- Configuration 5 represents a configuration in which uranium dioxide is dissolved by unoxidized (metal) zirconium, dissociating the uranium and oxygen. A uranium-zirconium metal mixture is formed that is denser than the oxides and therefore sinks to the bottom in this configuration. The unique challenge of this configuration is that the heavy metal layer generates heat internally and is also heated from above by the oxide layer;

this action focuses the heat load on the bottom of the head where the heat removal capacity on the outside of the lower head is minimized.

Given the uncertainty in potential core debris condition, IVR is evaluated by considering two bounding configurations. The first is termed “edge-peaked” and considers a convecting molten pool with a floating metallic layer that imposes a high heat flux onto the side walls of the RPV (metallic focusing effect dominates). The second, termed “downward-peaked”, considers a solid debris block in which heat transfer through the debris and onto the surface of the lower head is controlled by conduction.

The analytical model used to evaluate the edge-peaked heat flux is based on the two-layer model, with a molten oxide pool and molten metallic layer floating on top. Heat is generated in the oxide layer and heat transfer is governed by internal natural convection. The oxide layer imposes a heat flux distribution down onto the lower head and also transfers heat up into the metallic layer where the focusing effect imposes a high heat flux on the RPV side walls. The analytical model used to evaluate the downward-peaked heat flux is based on a homogenous solid block. In this case, core materials are modeled as a solid, nonporous block, where heat transfer through the debris is governed by conduction. This unrealistic configuration is used to bound the downward-peaked heat flux.

Evaluation of Heat Flux in RPV

The water in the CNV cools the outside surface of the RPV lower head. 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 compared to 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. However, remaining in the nucleate boiling regime ensures RPV integrity as the excess surface temperature is small.

The evaluations of the edge-peaked heat flux and downward-peaked heat flux are performed with steady-state thermal analyses using ANSYS. For both evaluations, a bounding heat load is imposed on the inside surface of the lower head and the heat flux distribution on the outside of the lower head is calculated, assuming that heat transfer occurs in the nucleate boiling regime.

The heat balance for the two-layer model used for the bounding edge-peaked heat flux evaluation is illustrated in Figure 19.2-2. The debris is assumed to be molten, with a dense oxide pool on the bottom and a floating metallic layer. The heat source in the system is the radioactive decay of fission products in the oxide pool. A portion of the decay heat is transferred down through the lower head to the water in the containment (Q_{down}). The remaining portion is transferred to the metallic layer on top of the debris (Q_{up}), which in turn transfers 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 generation increases the temperature of the core debris (and melts additional structural materials into the debris field). An increase in the core debris temperature enhances the heat transfer out of the core debris and eventually the system reaches steady state. The limiting condition is a result of a high heat transfer rate into the metallic layer that is then transferred onto a small surface area on the side of the RPV. The heat flux from the focusing effect is maximized when the total heat generation rate is maximized and the metallic layer height is minimized. For a bounding evaluation, it is assumed that a quasi-steady intermediate condition is established in which the only metals in the core debris field are those associated with the fuel assemblies (e.g., unoxidized cladding, fuel assembly nozzles) as well as the steel structures initially in the lower plenum (flow diverter and core support blocks). Additionally, a high oxidation fraction of 75 percent for zirconium components is assumed to minimize the quantity of unoxidized metal. Radiative heat losses and heat lost to melting steel are also conservatively neglected.

Two cases are considered for the edge-peaked heat flux evaluation. One case considers that the entirety of the fuel in the core is relocated along with a proportional amount of core components, which maximizes the heat flux from the focusing effect. Another case is a partial relocation of 30 percent of the fuel. The latter case imposes a maximum heat flux at a location where the CHF on the outside surface is minimized; specifically, at the transition from the curved lower head surface to the flat refueling ledge. The resultant heat fluxes are compared to applicable CHF values to assess RPV integrity.

The bounding evaluation for a downward-peaked heat flux models the core debris as a solid nonporous block. Because the focusing effect from an upper metallic layer reduces the downward-peaked heat flux, the debris volume is assumed to be homogenous with heat transfer governed by conduction to maximize the downward heat flux. The limiting condition is a result of a high decay heat rate generated in a relatively small volume of debris, which maximizes the average heat flux imposed on the RPV wall.

For the bounding evaluation, it is conservatively assumed that a quasi-steady intermediate condition is established where the only materials in the core debris are those directly associated with the fuel assemblies (e.g., unoxidized cladding, fuel assembly nozzles) as well as the steel structures initially in the lower plenum (flow diverter and core support blocks). Additionally, metals are assumed to remain unoxidized, which minimizes their contribution to the volume of the debris. Conductivity of the debris block is conservatively assumed to be the minimum conductivity of uranium dioxide (temperature distribution is more uniform in a highly conductive material). Radiative heat losses and heat lost to melting steel are also conservatively neglected.

Three cases are considered for the downward-peaked heat flux evaluation; each case includes the entirety of the fuel in the core along with a proportional relocation of core components, which maximizes the total heat generation rate, the volumetric heat generation rate, and the average heat flux imposed on the RPV lower head surface. The cases differ in consideration of a heavy metal layer at the bottom of the debris volume. The cases indicate that the thickness of a heavy metal layer does not significantly increase the downward peaking of the heat flux compared to the postulate of a solid block for the core debris.

Determination of CHF Values

Experimental studies related to in-vessel retention (IVR) are reviewed to support development of CHF values applicable to the NuScale design. The studies demonstrate that the CHF value fundamentally varies with the effectiveness of generated steam escaping from the RPV source; as such, the studies provide insights for the underside of the RPV as well as the vertical portion of the RPV wall:

- Guo and El-Genk (Reference 19.2-5) performed an experimental study of saturated pool boiling from the downward facing and inclined heated surface.
- Theofanous et al (Reference 19.2-6, Reference 19.2-7) performed experiments for both saturated and subcooled conditions.
- The Subscale Boundary Layer Boiling (SBLB) experiment (NUREG/CR-6507, 1997) correlated critical heat flux data obtained for downward facing boiling on the exterior surface of a heated hemispherical vessel, taking into account the effect of subcooling.

The experimental studies for CHF on downward facing surfaces that most apply to an IVR scenario have been performed at atmospheric pressure and saturated conditions or a relatively modest level of subcooling. However, in a severe accident, hydrogen gas is produced, which pressurizes the NPM. Coupled with effective heat transfer to the UHS, the water in the CNV becomes subcooled. Other studies indicate that increased pressure and subcooling enhance the CHF. Increased pressure causes increased steam density, which results in smaller bubbles and a more easily wetted surface. Increased subcooling enhances CHF because of the sensible heat transfer required to bring the liquid to the boiling point as well as the interfacial condensation of steam by subcooled liquid, which reduces the size of bubbles and facilitates wetting of the heated surface. Theoretical and experimental studies considered in the evaluation to account for CHF enhancement include:

- Effect of increased pressure on CHF (Kutateladze, Reference 19.2-8)

- Effect of increased subcooling on CHF (Kutateladze, Reference 19.2-9)
- Effect of increased pressure and subcooling on CHF (NUREG/CR-6507)
- Effect of increased subcooling on CHF (Jun, Reference 19.2-10)
- Effect of increased pressure and subcooling on CHF (Inoue, Reference 19.2-11)
- Effect of increased pressure and subcooling on CHF (Sakurai, Reference 19.2-12)

Success Criterion for Retention of Core Debris in the Reactor Pressure Vessel

To evaluate the structural capability of the RPV to retain a core debris bed, the concept of heat flux limited wall thickness is relevant. From Theofanous (Reference 19.2-3), 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 because of 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 heat flux limited wall thickness is inversely proportional to the slope of the linear temperature profile. Accordingly, the heat flux limited wall thickness decreases as the imposed heat flux increases.

The minimum thickness of the wall necessary for supporting the lower head is determined by calculating the weight of the lower head and its contents and subtracting the opposing buoyancy force due to the water in the CNV that is displaced by the RPV. The net weight acting on the lower head is divided by the yield stress to determine the cross sectional area of material necessary for supporting the load. From that, the required vessel thickness is calculated.

The bounding heat flux limited wall thickness is calculated for the RPV lower head assuming that the imposed heat flux is equal to the maximum CHF. The resulting heat flux limited wall thickness is shown to be greater than the minimum thickness required to support the weight of the lower head and its contents with a large margin. It is therefore concluded that the RPV lower head remains sufficiently strong to retain the core debris as long as the heat flux does not exceed the CHF.

ANSYS Modeling

Evaluations of the edge-peaked heat flux and downward-peaked heat flux are performed with steady-state thermal analyses using ANSYS (Reference 19.2-2). For both evaluations, a bounding heat load is imposed on the inside surface of the lower head and the heat flux distribution on the outside of the lower head is calculated, assuming that heat transfer occurs in the nucleate boiling regime. The RPV lower head is a torisphere with two external protrusions: the lower seismic restraint at the central pole and the shoulder ledge on the periphery. The model uses three materials: SA-965 FXM-19 for the RPV, a simplified uranium dioxide material, and a generic highly thermally conductive material. For steady-state thermal analysis, thermal conductivity is the relevant material property. The intent of the model is to evaluate the external surface heat fluxes given various thermal loadings imposed on the inside surface.

Conservatisms in ANSYS simulation include:

- a bounding decay heat load. The entire core relocates at a conservatively early relocation time and the heat balance immediately reaches a steady-state condition.
- no credit for heat removal from the top of the debris.
- massive quantities of non-heat generating structural materials (including upper plate, core barrel, reflector) are omitted from the relocated debris field, thereby increasing core debris power density and the focusing effect challenge.
- various bounding core debris configurations considered to maximize heat flux at locations where heat removal is most challenging.

The results of the simulations illustrate that heat fluxes on the RPV lower head remain below the CHF for each case. This result implies that the RPV lower head does not fail structurally under the thermal attack from the relocated core debris.

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 is performed using conservative ANSYS modeling. 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. The analysis demonstrates that heat transfer on the surface of the lower head remains in the nucleate boiling regime with significant margin between the heat flux and the CHF; thus, structural integrity of the lower head is maintained in the event of in-vessel core relocation.

The design characteristics of the NPM that support the in-vessel retention-RPV capability include

- In a scenario in which the CNV is isolated, it is flooded with reactor coolant, which provides effective external cooling of the RPV. There is no reliance on active or passive systems (except for containment isolation) to ensure that the external surface of the RPV is cooled.
- The CNV is submerged in the reactor pool. The reactor pool passively cools the water inside the CNV, which in turn cools the RPV lower head.

- Severe accident progression generates large quantities of hydrogen gas, which pressurizes the closed system and causes the water pool in the CNV to become subcooled. The increased system pressure and CNV water subcooling increases the CHF and heat removal capacity on the outside of the RPV lower head.
- The fuel used in the NPM has a lower power density than typical large light water reactors. The lower power density results in a lower volumetric heat generation rate, which reduces the heat load imposed on the lower head.
- The core is smaller than typical large light water reactors, resulting in a smaller volume of relocated core debris. A small volume has a greater surface area per unit volume. Accordingly, the core debris in the NPM has a greater relative heat transfer surface area and a lower heat flux for a given volumetric heat generation rate.

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 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 the RPV would retain a damaged core 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 to demonstrate defense-in-depth with respect to the severe accident mitigating capabilities of the design, the IVR capability of the CNV lower head is considered.

Drawing on similarities with the evaluation of core relocation in the RPV, the possibility of arresting core damage progression in the CNV is evaluated using an approach similar to that used for RPV retention. In both situations, as illustrated in Figure 19.2-3, core debris relocates to the lower head of a concave vessel with the potential to thermally challenge the lower head. Because the debris is fully submerged in the water retained in the CNV, heat removal from the top surface of the relocated core debris in the CNV is greater than in the RPV situation. Additionally, the debris mass will have a greater surface area and less depth in the CNV due to the smaller curvature of the CNV lower head (i.e., larger radius). These factors reduce the steady-state heat flux imposed on the lower head and thus improve the coolability of the core debris in the lower head of the CNV when compared to the same debris mass in the lower head of the RPV. Flow holes are included in the CNV skirt to vent the steam generated in the skirted region and recirculate liquid water to cool the lower head.

Because of considerably lower heat fluxes in the CNV case, the only credible way that the lower head could fail is if steam generated under the lower head could not be vented effectively. Based on the design similarities with the NuScale US600 Plant Design (Docket No. 52-048), steam accumulation in the skirted region is judged to be minimal and does not lead to significant dryout of the CNV lower head. Thus, the CNV would remain intact and retain core debris in the event of RPV failure. To further consider defense-in-depth, 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

This section summarizes design capabilities with regard to potential severe accident challenges and the survivability of equipment needed for post-accident monitoring.

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 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 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

As stated in Section 6.2 and Section 19.2.3.1, the potential for hydrogen combustion is minimized in the design because of factors such as the near vacuum condition during normal power operation. During a severe accident, when the core becomes uncovered, cladding oxidation can result in the release of hydrogen; however, the only source of oxygen with an intact containment is the radiolysis of water, which is relatively slow. The design includes a passive autocatalytic recombiner (PAR). The main function of the PAR is to maintain the concentration of oxygen in the CNV atmosphere below the combustible limit. Because oxygen production is possible only after long-term radiolysis, the use of a PAR eliminates the potential for long-term hydrogen combustion.

In the event that the PAR is unavailable, severe accident simulations show that the oxygen concentration does not exceed flammability limits within 72 hours for intact containment scenarios. In terms of hydrogen generation, the severe accident cases bound a 100 percent fuel-clad coolant reaction. Although the oxygen concentration can be higher in containment bypass scenarios, the high steam concentration precludes the possibility of hydrogen deflagration in the CNV.

Table 19.2-1 identifies the simulations that are evaluated for potential hydrogen combustion. Figure 19.2-4 illustrates the hydrogen mass versus time; Figure 19.2-5 illustrates the oxygen concentration in the CNV versus time for the evaluated severe accident cases.

To provide insight into the potential challenge to containment for a hydrogen deflagration after 72 hours, an evaluation of adiabatic isochoric complete combustion is performed using the MELCOR code and results of the severe accident simulations specified in Section 19.2.3.2. This analysis does not credit the PAR as a mitigation feature for combustible gas control. 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 possible only following an extended period of radiolysis causing the oxygen concentration to increase to the minimum combustible limits. The adiabatic isochoric complete combustion analysis uses 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 challenging as it increases the total available moles of oxygen for combustion. It is estimated that radiolysis would have to proceed uninhibited for 37 days to produce such an oxygen concentration. The adiabatic isochoric complete combustion calculation results show that the post-deflagration pressure remains 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 CNV.

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 design does not include concrete inside the CNV. Thus, molten core-concrete interaction is not applicable to the 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. As discussed in Section 19.2.3.2.1, core debris is retained in the RPV after a core damage accident involving an intact CNV; thus, HPME is evaluated as not a threat to containment integrity. However, from the perspective of defense-in-depth, the RPV is postulated to fail and the potential for HPME to challenge containment integrity is evaluated.

Literature sources such as NUREG-1150 (1990) indicate that a significant pressure differential between the RPV and containment is required to cause HPME from the RPV. Although there is not an accepted technical basis for a differential pressure below which HPME is not possible, NuScale severe accident simulations show a lack of driving pressure at the time the RPV lower head temperature begins to increase substantially (which indicates the potential for lower head failure), as illustrated in Figure 19.2-6. The pressure differential is caused by a momentary increase in steam generation from relocated debris interacting with the liquid water in the RPV lower head. The differential pressure decreases substantially within an hour because the RPV is effectively cooled. After water in the lower head boils off, the differential pressure between the RPV and CNV rapidly drops until there is no driving pressure for HPME. The RCS inventory transferred to the CNV cools the core debris in the lower head by heat transfer to the UHS.

In summary, the passive DHRS and ECCS are designed to provide efficient heat removal and 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 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.

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"), is evaluated. Fuel-coolant interaction can result in an energetic and rapid phase transition from liquid water to steam, referred to as a "steam explosion." The potential for an in-vessel steam explosion is minimized in the design because of the small size of the NPM core, physical dimensions of the RPV, and thermal-hydraulic conditions within the RPV, including:

- The amount of core melt available for a steam explosion is small and 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 molten corium 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. There is a small vertical distance between the core and the pool in the lower plenum, and the depth of the pool in lower plenum is shallow.

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, as described in NUREG-1524 (1996) and NUREG/CR-5030 (1989), is considered with respect to its potential in the design. The analysis evaluates the likelihood of CNV failure using a probabilistic framework that applies uncertainty distributions to the various physical phenomena involved in an FCI. This framework models the alpha-mode sequence as a series of causal relationships that are used to evaluate the likelihood of CNV failure.

A bounding quantitative assessment of the frequency of alpha-mode failure is conducted based on the probabilistic model provided in NUREG/CR-5030; the assessment accounts for advances in the study of FCI and for the unique design of the NPM. The probabilistic model represents the sequence of events leading to alpha-mode failure as a series of causal relationships, depicting specific phenomena, derived from initial conditions.

Input distributions of the probabilistic modeling include the molten core fraction at the time of lower core plate failure, failure area of the lower core plate, the mass of corium in the premixture, conversion ratio for thermal to mechanical energy, the ratio of mechanical energy resulting in upward slug energy, the energy dissipation in the RPV prior to RPV head failure, and the energy required to fail the CNV.

The probabilistic analysis for the evaluation of alpha-mode neglects multiple characteristics of the NPM that would limit steam explosion severity. Results of the analysis are that the conditional probability of alpha-mode failure of the CNV is less than 1.0E-5 given a core damage event. As a result of this conservative evaluation, in-vessel steam explosion is not considered further.

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 is not performed.

However, from the perspective of demonstrating defense-in-depth, several aspects of the design minimize the possibility of an ex-vessel FCI.

- The distance between the RPV lower head and the CNV is small and occupied by a water pool. Because the molten jet will originate underwater, there is no available space between a failed RPV lower head and the water pool to foster the material breakup needed to promote an energetic transfer of heat to the water pool in the CNV.
- The CNV lower head region below the RPV is not large enough to allow for 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. This backfilling prevents the majority of fuel material from interacting with a water pool in the CNV. Coupled with the small size of the NPM core, a relocation of fuel materials from the RPV to the CNV will involve less material than a similar fuel coolant interaction within the RPV, further limiting the potential energy transfer necessary for an energetic ex-vessel steam explosion.
- Due to the large water pool predicted to reside in the CNV, the resultant energy conversion ratio for an ex-vessel FCI is significantly less than the predicted ratio using the thermodynamic model of an in-vessel FCI (which is 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 and ex-vessel steam explosion is not considered further.

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 (RXB), bypassing containment. Core damage sequences that include containment bypass 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 failure of containment isolation or steam generator tube failure (SGTF) concurrent with failure of secondary-side isolation on the failed steam generator (SG).

As stated in Section 6.2.4, the containment system design provides for isolation of systems that penetrate the CNV. Modeling of containment isolation is discussed in Section 19.1.4.2.

The SG bundles are integrated within the RPV and 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; thus the 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 of the lack of data on thermal-induced SGTFs for the NuScale design, an evaluation of creep rupture is performed based on historical data for conventional SG tube flaws and time-history temperature and pressure conditions representative of severe accident sequences as modeled by MELCOR.

The SG tubes under severe accident conditions typically have a much higher probability of failure due to 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 (1998). Although the formulations employed for predicting creep rupture are based on internally pressurized tubes, the NuScale SG 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, the CNV is bypassed and a large release is assumed.

19.2.3.3.7 Other Severe Accident Mitigation Features

The 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 RXB.

19.2.3.3.8 Equipment Survivability

Consistent with SECY-90-016, SECY-93-087, and SECY-94-302 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 survives 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 occurs, the functions that must be maintained are containment integrity, the capability to control combustible gas, and post-accident monitoring. 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 that survivability is reasonably assured is specific to the equipment and its function. Equipment that is necessary to maintain containment integrity is reasonably assured to survive for at least 48 hours after core damage. Equipment necessary for combustible gas control is reasonably assured to survive for at least 48 hours. Equipment used for post-accident 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 48 hours after core damage.

Equipment is qualified to 100-percent humidity. In terms of post-accident dose, the design uses a methodology for assuring equipment survivability based, in part, on environments predicted for severe accidents as modeled in the PRA. This approach provides confidence that the equipment needed for severe accident mitigation and monitoring survives over the time span 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 where the environmental qualification dose is larger, survivability is assured. For cases where the severe accident dose is larger, qualitative assessments, testing, or additional analyses are performed to assure survivability.

Table 19.2-8 summarizes the evaluation of equipment for survivability; the table identifies each component or variable, its function, and the duration over which it is needed. Post-accident temperature and pressure conditions are discussed with regard to containment integrity, combustible gas control, and post-accident monitoring capabilities as follows.

Containment Integrity

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 CNV temperatures are highest early in an accident progression following coolant transfer from the RPV to the CNV and continue to decrease following this initial maximum due to UHS cooling of containment, remaining well below the CNV temperature limit in all sequences. The most challenging accident sequence with respect to containment pressure results from a general reactor trip with failure of the RSVs to open and a successful automatic ECCS actuation at high RCS energy to protect the RPV from over pressurization. In this sequence, containment pressure remains below the ultimate failure pressure.

Given CNV isolation, the design eliminates severe accident phenomena that result in containment challenges for current generation plants.
Section 19.2.3.3 discusses NPM capability with respect to such challenges.

Combustible Gas Control

The design includes a passive autocatalytic recombiner (PAR) that operates within the CNV. The PAR is used to control the generation of combustible gas passively. The PAR is designed to recombine hydrogen and oxygen in the CNV into water vapor, precluding a combustible mixture in the CNV over the duration of a severe accident. Therefore, the PAR functions to preclude a combustion event and protect containment integrity, precluding the need for combustible gas monitoring. The design for combustible gas control in the CNV is described in Section 6.2.5.

Due to proximity to the core, the PAR is in a high radioactivity environment during normal operation and must withstand neutron and gamma flux. Of the radiation types, neutron flux is the greater threat, as neutrons can cause displacements in the atomic matrix, potentially reducing the efficacy of the PAR. Although the gamma flux is high due to the severe accident radiological environment, there is no significant neutron flux during a severe accident as the fission reaction is either stopped by successful control rod insertion, or by loss of coolant moderation prior to core damage if reactor trip is not successful. Gamma radiation is judged not to influence PAR performance as the PAR does not contain organic materials and therefore there is reasonable assurance the PAR would survive with minimal depreciation in performance.

The CNV pressures are not a concern for the PAR, because the PAR is open to the CNV atmosphere. Since the severe accident simulations show the CNV pressure and temperature do not exceed the equipment pressure and temperature qualification for the PAR, there is reasonable assurance the PAR equipment will be maintained during a severe accident.

Post-Accident Monitoring

Monitoring is not required to support mitigation of a severe accident. However, each Type B, C, D, and F post-accident monitoring variable is included in the equipment survivability assessment. 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 that 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 occurs.

As shown in Figure 19.2-7, the simulation results from the intact CNV severe accident cases exhibit RPV shell temperatures that do not increase above the RPV design temperature, even after core damage and relocation. Figure 19.2-7 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 CNV pressures due to decay heat do not approach design-basis pressure, and are therefore not challenging to the equipment located within the CNV. 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 is 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 experiences conditions much less severe than those on the RPV and are reasonably assured to survive severe accident temperature and pressure conditions.

19.2.4 Containment Performance Capability

As discussed in SECY 90-016, SECY 93-087, and associated staff requirements memoranda, containment performance with regard to severe accidents is evaluated using deterministic and probabilistic approaches.

Section 3.8 provides an evaluation of the ultimate pressure capacity of the CNV. The evaluation demonstrates that the ultimate pressure capacity 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 50.44. 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. The design has no safety-related low-pressure injection that requires venting to atmosphere. Thus, a containment vent is unnecessary in the NuScale design.

Using a probabilistic approach, the conditional containment failure probability (CCFP) is not to exceed 0.1. This criterion is applied to the NPM in the following manner.

- The criterion is applied to internal and external event scenarios when a NPM 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 NPM is calculated to be less than 0.1, which meets the safety goal, as discussed in Section 19.1.

Containment performance is ensured also by achieving combustible gas control as discussed in Section 19.2.3.3.2. A list of structures, systems and components (SSC) that are required to survive following a hydrogen combustion event to support containment integrity, combustible gas control, and post-accident monitoring is included in Section 19.2.3.3.8.

In summary, 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 off site releases.

The inherent design characteristics (e.g., fail-safe equipment position and design simplicity) and thermal-hydraulic characteristics (e.g., passive cooling) of the 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 NPM or providing backup in the event of multiple component failures. Section 19.2.5.1 summarizes the capability of the 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.

<u>Prevention of Core Damage</u>

The Level 1 PRA discussed in Section 19.1 demonstrates the very low CDF is primarily the result of beyond-design-basis accidents involving incomplete actuation of the ECCS. In such sequences, establishing coolant flow to the RPV is required to prevent core damage. Potential actions to provide the necessary coolant flow, 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.

<u>Terminate Core Damage Progression and Retain the Core within the RPV</u>

The actions identified for preventing core damage are also taken to arrest the progression of core damage once begun and retain the core within the RPV.

<u>Maintaining Containment Integrity</u>

The analyses supporting the Level 2 PRA 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 Off-site 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 because of 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 RXB.

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, specifically:

- 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. Section 13.5 addresses EOPs and other operating procedures.
- The response to an ATWS defined by 10 CFR 50.62 is addressed in SAMGs or other administrative controls. Section 19.2.2.1 summarizes the NPM capability to accommodate an ATWS event.
- The response to an SBO defined by 10 CFR 50.63 is addressed in SAMGs or other administrative controls. Section 19.2.2.3 summarizes the NPM capability to accommodate an SBO and related events.
- The response to an aircraft impact event defined in 10 CFR 50.150 is addressed in SAMGs or other administrative controls. Section 19.5 addresses key design features associated with the design capability to survive an aircraft impact.
- Strategies and guidelines for mitigation of beyond-design-basis events, as required by 10 CFR 50.155, are addressed in Section 19.4.

COL Item 19.2-1: An applicant that references the NuScale Power Plant US460 standard design 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, the design-specific PRA performed is 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 following sections summarize the method for identifying and evaluating these design improvements and the conclusions of the evaluation.

19.2.6.1 Introduction

The design improvement 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.

19.2.6.2 Estimate of Risk for Design

The estimate of the risk that provides the basis for the design improvement evaluation is developed from the PRA performed for the standard design and an estimate of the characteristics of a potential site. Key points of the evaluation include.

- The PRA provides Level 1 and Level 2 information for all modes of operation. In addition to full power, low power, and shutdown internal events, the PRA addresses internal flood, internal fire, high winds, external flooding, and seismic hazard.
- Site characteristics are based on the State-of-the-Art Reactor Consequence Analysis Project Surry Nuclear Power Station off-site consequence model in NUREG/CR-7110 (2013), updated with 2022 economic information and 2060 population estimates, which are considered representative for the purposes of the design improvement evaluation for standard design.
- To determine the offsite 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 three release categories to more realistically estimate the offsite consequences of severe accidents. Radionuclide source terms corresponding to each release category are determined with MELCOR severe accident simulations.
- The MACCS code in NUREG/CR-6613 (1998) is used to evaluate the population dose and off-site economic consequences.
- Onsite operational dose estimates and cleanup and decontamination cost estimates are used from NUREG/BR-0184 (1997).
- Multiple-module events are addressed by applying multipliers (corresponding to the maximum number of NPMs 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 improvement.

Following the guidance in NEI 05-01 (Reference 19.2-13), the maximum benefit associated with eliminating all risk in the design (which can be viewed as an estimate of the severe accident risk for the design) is conservatively calculated to be $110,000 for a 6-NPM configuration. This maximum benefit is bounding for a configuration with a smaller number of NPMs.

19.2.6.3 Identification of Potential Design Improvements

The design improvement evaluation is performed using the guidance in NEI 05-01 and NUREG/BR-0184. Design improvements include those typically considered for currently operating pressurized water reactor plants and those that may be beneficial to the design. Design improvements specific to the NuScale design are identified to improve the reliability of the SSC determined to be candidates for risk-significance; in some cases a generic design improvement is applicable to the risk-significant candidate component, but in most cases, a design-specific design improvement is identified and evaluated. The design improvement candidates are considered based on the generic list provided in NEI 05-01 and NuScale-specific design considerations.

NuScale design-specific design improvement candidates are postulated for a variety of plant 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
- augmented DC power system (EDAS)
- 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 design improvements 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 design that warrant a detailed cost-benefit evaluation. The categories and the screening process itself are based on the "Phase I" analysis screening criteria in NEI 05-01; the categories are:

- Not applicable: Design improvement candidates that are not considered applicable to the design are those with specific pressurized water reactor equipment that is not in the design.
- Already implemented: Candidate design improvements that are already included in the design or whose intent is already fulfilled by a different design feature are considered "already implemented" in the design. If a particular design improvement is already implemented in the design, it is not retained for further analysis.

- Combined: The design improvement candidates that are similar to one another are combined and evaluated in conjunction with each other. This combination of design improvement candidates leads to a more comprehensive or plant-specific candidate set. The combined candidate set would then be assessed against the remaining six screening categories.
- Excessive implementation cost: If a design improvement requires extensive changes that exceed the value shown in Section 19.2.6.2 even without an implementation cost estimate, it is not retained for further analysis.
- Very low benefit: If a proposed design improvement is related to a system for which improved reliability would have a negligible impact on overall plant risk, it is judged to have a very low benefit and is not retained for further analysis.
- Not required for standard design: Design improvement 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.
- Considered for further evaluation: Any design improvement candidate that did not screen into any of the previous six screening categories is subject to a more in-depth cost-benefit analysis.

19.2.6.5 Cost Impacts of Candidate Design Improvements

A total of 22 design improvements are screened into the "excessive implementation cost" or "considered for further evaluation" categories. Of the 22 design improvements, one is screened in Phase I as exceeding the maximum benefit value shown in Section 19.2.6.2 for the design. The remaining Phase I candidates considered to be potentially cost beneficial are evaluated further in Phase II.

19.2.6.6 Cost-Benefit Comparison

The contribution to the maximum benefit for each design improvement evaluated in Phase II is below the estimated cost of implementation of greater than $100,000 for each design improvement candidate. Therefore, none of the candidates are considered to be potentially cost beneficial in the Phase II screening.

Maximum benefit sensitivity analyses are performed using different assumptions of on-site dose, dollar per person-rem conversion factor, discount rate, and off-site consequence modeling assumptions for the release characteristics, site characteristics, and emergency planning characteristics.

19.2.6.7 Conclusions of Design Improvement Evaluation

Design improvements that are considered in the evaluation include those typically considered for currently operating plants and those that may be beneficial to the design. There are no design improvements determined to be cost-beneficial for severe accident mitigation.

COL Item 19.2-2: An applicant that references the NuScale Power Plant US460 standard design 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).

COL Item 19.2-3: Not used.

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 ANSYS (Release 19.2) [Computer Program]. (2019). Canonsburg, PA, ANSYS Incorporated.

19.2-3 Theofanous, T.G., et al., "In-vessel Coolability and Retention of a Core Melt," DOE/ID-10460, Vol. I, October 1996.

19.2-4 Rempe, J.L., "Potential for AP600 In-Vessel Retention through Ex-Vessel Flooding," INEEL/EXT-97-00779, December 1997.

19.2-5 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.

19.2-6 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.

19.2-7 Theofanous, T.G., et al., "Critical heat flux through curved, downward facing, thick walls," *Nuclear Engineering and Design*, (1994): 151: 1:247-258.

19.2-8 Kutateladze, S. "On the transition to film boiling under natural convection", Kotloturbostronie, no. 3, p. 10, 1948.

19.2-9 Kutateladze, S. "Heat Transfer in Condensation and Boiling," Tech. Rep., State Scientific and Technical Publishers of Literature on Machinery, 1952.

19.2-10 Seongchul Jun et. al. "Effect of Subcooling on Pool Boiling of Water from Sintered Copper Microporous Coating at Different Orientations", Science and Technology of Nuclear Installations, 2018

19.2-11 Inoue, T., et al. "Effect of Subcooling on Critical Heat Flux during Pool Boiling on a Horizontal Heated Wire." Heat and Mass Transfer, vol. 33, no. 5-6, 1998, pp. 481-488.

19.2-12 Sakurai, A. "Mechanisms of Transitions to Film Boiling at CHFs in Subcooled and Pressurized Liquids Due to Steady and Increasing Heat Inputs." Nuclear Engineering and Design, vol. 197, no. 3, 2000, pp. 301-356.

19.2-13 Nuclear Energy Institute, "Severe Accident Mitigation Alternatives (SAMA) Analysis Guidance Document," NEI 05-01, Revision A, Washington, DC, November 2005.

Table 19.2-1: Core Damage Simulations for Severe Accident Evaluation

Simulation ID	Description	Mitigating Systems[1,2]			Severe Accident Applicability
		RSV	ECCS	CI	
LCC-05T-01	CVCS LOCA inside CNV (vapor space break)	ND	IA	CI	RPV IVR, H2, HPME, FCI, ES
LCC-05T-02	CVCS LOCA inside CNV (liquid space break)	ND	NA	CI	RPV IVR, H2, HPME, FCI, ES
LEC-06T-00	RVV LOCA (fast vapor space break)	ND	IA	CI	RPV IVR, H2, HPME, FCI, ES
LEC-05T-00	RRV LOCA (fast liquid space break)	ND	IA	CI	RPV IVR, H2, HPME, FCI, ES
TRN-07T-01	General transient (slow vapor space break)	SO	NA	CI	RPV IVR, H2, HPME, FCI, ES
LCU-03T-01	CVCS break outside CNV (bounding release)	ND	NA	NA	CNV IVR, HPME, ES

Abbreviations:

CI- containment isolation
NA- not available

ND- not demanded
IA- incomplete actuation

SO- stuck open

ES- equipment survivability
FCI- fuel-coolant interaction

H2- hydrogen combustion
IVR- in-vessel retention (RPV, CNV)

Notes:

1. Scenarios include success of the reactor trip system.
2. Feedwater, main steam, and CVCS are not credited in any simulation. Base case simulations also do not credit DHRS.

Table 19.2-2: Sequence LCC-05T-01 Key Events

Time (seconds)	Event
0	CVCS injection line LOCA inside containment
4	High CNV pressure
6	Reactor trip (successful), containment isolation (successful), pressurizer heater isolation (successful)
140	Low-low pressurizer level
285	ECCS actuation signal on low RPV level - incomplete ECCS actuation
325	Maximum CNV pressure (711.7 psia) measured at the top of the CNV
11340 (3.2 hr)	RPV collapsed liquid level below TAF
13860 (3.9 hr)	High core outlet temperature
14940 (4.2 hr)	Onset of cladding oxidation (timing approximate)
15250 (4.2 hr)	First gap release (group 3)
15724 (4.4 hr)	Core damage (> 2200 F)
28440 (7.9 hr)	Maximum cladding temperature (4001.9 F)
33856 (9.4 hr)	Failure of core support plates in rings 1 & 2 - begins debris relocation to RPV lower plenum
34503 (9.6 hr)	Failure of core support plates in ring 3 due to yielding
48938 (13.6 hr)	Failure of core support plates in ring 4 due to yielding
61200 (17 hr)	End of cladding oxidation (timing approximate)
259200 (72 hr)	Simulation terminates

Table 19.2-3: Sequence LCC-05T-02 Key Events

Time (seconds)	Event
0	CVCS injection line LOCA inside containment
3	High CNV pressure
5	Reactor trip (successful), containment isolation (successful), pressurizer heater isolation (successful)
140	Low-low pressurizer level
285	ECCS actuation signal on low RPV level - ECCS fails completely
3060	Maximum CNV pressure (373.1 psia) measured at the top of the CNV
4620 (1.3 hr)	RPV collapsed level below TAF (timing approximate)
5580 (1.6 hr)	High core outlet temperature
6900 (1.9 hr)	Onset of cladding oxidation (timing approximate)
7097 (2 hr)	First gap release (group 1)
7497 (2.1 hr)	Core damage (> 2200 F)
10620 (3 hr)	Maximum cladding temperature (4002.4 F)
15323 (4.3 hr)	Failure of core support plates in rings 1 & 2 - begins debris relocation to RPV lower plenum
16519 (4.6 hr)	Failure of core support plates in ring 3 due to yielding
42481 (11.8 hr)	Failure of core support plates in ring 4 due to yielding
90000 (25 hr)	End of cladding oxidation (timing approximate)
259200 (72 hr)	Simulation terminates

Table 19.2-4: Sequence LEC-06T-00 Key Events

Time (seconds)	Event
0	Spurious single RVV LOCA
1	High CNV pressure
3	Reactor trip (successful), containment isolation (successful), pressurizer heater isolation (successful)
90	Low-low RPV level
135	ECCS actuation signal on low RPV level - incomplete ECCS actuation
140	Maximum CNV pressure (570.1 psia) measured at the top of the CNV
340	Low-low pressurizer level
14760 (4.1 hr)	RPV collapsed level below TAF (timing approximate)
18360 (5.1 hr)	High core outlet temperature
19900 (5.5 hr)	First gap release (group 3)
19620 (5.5 hr)	Onset of cladding oxidation (timing approximate)
20376 (5.7 hr)	Core damage (> 2200 F)
33120 (9.2 hr)	Maximum cladding temperature (4002.5 F)
40093 (11.1 hr)	Failure of core support plate in ring 1 by yielding - begins debris relocation to RPV lower plenum
40363 (11.2 hr)	Failure of core support plate in ring 2 by yielding
40938 (11.4 hr)	Failure of core support plate in ring 3 by yielding
52212 (14.5 hr)	Failure of core support plate in ring 4 by yielding
130320 (36.2 hr)	End of cladding oxidation (timing approximate)
259200 (72 hr)	Simulation terminates

Table 19.2-5: Sequence LEC-05T-00 Key Events

Time (seconds)	Event
0	Spurious single RRV LOCA
3	High CNV pressure
5	Reactor trip (successful), containment isolation (successful), pressurizer heater isolation (successful)
105	Low-low pressurizer level
230	ECCS actuation signal on low RPV level - incomplete ECCS actuation
390	Low-low RPV level
2340	Maximum CNV pressure (356.6 psia) measured at the top of the CNV
2400	RPV collapsed level below TAF (timing approximate)
3180	High core outlet temperature
4200 (1.2 hr)	Onset of cladding oxidation (timing approximate)
4390 (1.2 hr)	First gap release (group 3)
4761 (1.3 hr)	Core damage (> 2200 F)
5640 (1.6 hr)	Maximum cladding temperature (4002.4 F)
9997 (2.8 hr)	Failure of core support plate in ring 1 by yielding - begins debris relocation to RPV lower plenum
10164 (2.8 hr)	Failure of core support plate in ring 2 by yielding
10478 (2.9 hr)	Failure of core support plate in ring 3 by yielding
32320 (9 hr)	End of cladding oxidation (timing approximate)
259200 (72 hr)	Simulation terminates

Table 19.2-6: Sequence TRN-07T-01 Key Events

Time (seconds)	Event
0	General transient - reactor trip (successful), containment isolation (successful), pressurizer heater isolation (successful)
415	High CNV pressure
1710	Low-low pressurizer level
2400	ECCS actuation signal on low RPV level - ECCS fails completely
3960 (1.1 hr)	Low-low RPV level
25560 (7.1 hr)	RPV collapsed level below TAF (timing approximate)
28800 (8 hr)	High core outlet temperature
30960 (8.6 hr)	Onset of cladding oxidation (timing approximate)
31400 (8.7 hr)	First gap release (group 3)
32077 (8.9 hr)	Core damage (> 2200 F)
40320 (11.2 hr)	Maximum cladding temperature (4002.5 F)
59661 (16.6 hr)	Failure of core support plate in rings 1 and 2 - begins debris relocation to the RPV lower plenum
60387 (16.8 hr)	Failure of core support plate in ring 3 by yielding
61200 (17 hr)	Maximum CNV pressure (221.9 psia) measured at the top of the CNV
63577 (17.7 hr)	Failure of core support plate in ring 4 by yielding
204120 (56.7 hr)	End of cladding oxidation (timing approximate)
259200 (72 hr)	Simulation terminates

Table 19.2-7: Sequence LCU-03T-01 Key Events

Time (seconds)	Event
0	CVCS injection line pipe break outside containment
85	Reactor trip (successful), secondary system isolation (successful)
105	containment isolation (failed), pressurizer heater isolation (successful)
200	Low-low pressurizer level
455	ECCS actuation signal on low RPV level - ECCS fails completely
930	Low-low RPV level
5220 (1.5 hr)	RPV collapsed level below TAF (timing approximate)
6000 (1.7 hr)	High core outlet temperature
7380 (2.1 hr)	Onset of cladding oxidation (timing approximate)
7720 (2.1 hr)	First gap release (group 1)
8167 (2.3 hr)	Core damage (> 2200 F)
11160 (3.1 hr)	Maximum cladding temperature (4002.5 F)
12686 (3.5 hr)	Failure of core support plates in rings 1 & 2 by yielding - begins debris relocation to RPV lower plenum
12739 (3.5 hr)	Failure of core support plate in ring 3 by yielding
20700 (5.8 hr)	Failure of RPV lower head (segment 3 of ring 3) by thru-wall yielding
30942 (8.6 hr)	High CNV pressure
30942 (8.6 hr)	Maximum CNV pressure (10.5 psia) measured at the top of the CNV
36766 (10.2 hr)	Failure of core support plate in ring 4 by yielding
51480 (14.3 hr)	End of cladding oxidation (timing approximate)
259200 (72 hr)	Simulation terminates

Table 19.2-8: Equipment Survivability List

Component/Variable	Function	Duration
CNV (including closure flanges and bolting)	Maintain containment integrity	48 hours after core damage
Electrical penetration assemblies	Maintain containment integrity	48 hours after core damage
ECCS trip and reset valves	Maintain containment integrity	48 hours after core damage
Containment isolation valves	Close to maintain containment integrity	1 hour after transient
PAR	Combustible gas control	48 hours after core damage
Neutron flux	PAM variable	Until core damage
Core exit temperatures	PAM variable	Until core damage
Wide range RCS pressure	PAM variable	Until core damage
Wide range RCS THOT	PAM variable	Until core damage
RPV riser level	PAM variable	Until core damage
Wide range containment pressure	PAM variable	Until core damage
Containment isolation valve positions	PAM variable	1 hour after transient
Inside bioshield area radiation monitor	PAM variable	48 hours after core damage
ECCS valve position (including trip valve)	PAM variable	Until core damage
Spent fuel pool water level	PAM variable	48 hours after core damage
DHRS valve position	PAM variable	Until core damage
Secondary main steam isolation valve position	PAM variable	Until core damage
Secondary main steam isolation valve bypass valve position	PAM variable	Until core damage
Feedwater regulating valve position	PAM variable	Until core damage
RCS flow	PAM variable	Until core damage
Reactor trip breaker position feedback	PAM variable	1 hour after transient
Pressurizer heater trip breaker position feedback	PAM variable	1 hour after transient
Demineralized water supply isolation valve position	PAM variable	Until core damage
Under-the-bioshield temperature	PAM variable	1 hour after transient
Neutron monitoring system detector position	PAM variable	Until core damage
Control room habitability system air supply isolation valve position	PAM variable	Until core damage
Control room habitability system pressure relief isolation valve position	PAM variable	Until core damage
Control room HVAC system supply air damper position	PAM variable	Until core damage
Control room HVAC system general exhaust damper position	PAM variable	Until core damage
Control room HVAC system return air damper position	PAM variable	Until core damage

Figure 19.2-1: Illustration of Reactor Pressure Vessel In-Vessel Retention

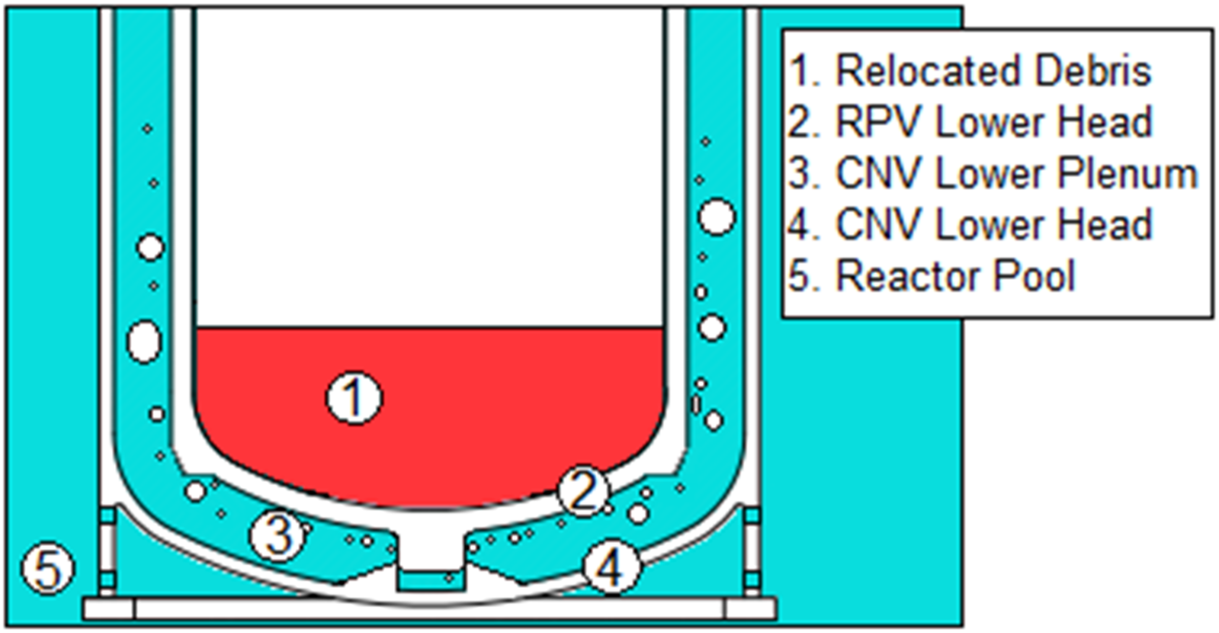


Figure 19.2-2: Heat Transfer Model for Retention of Core Debris in the Reactor Pressure Vessel

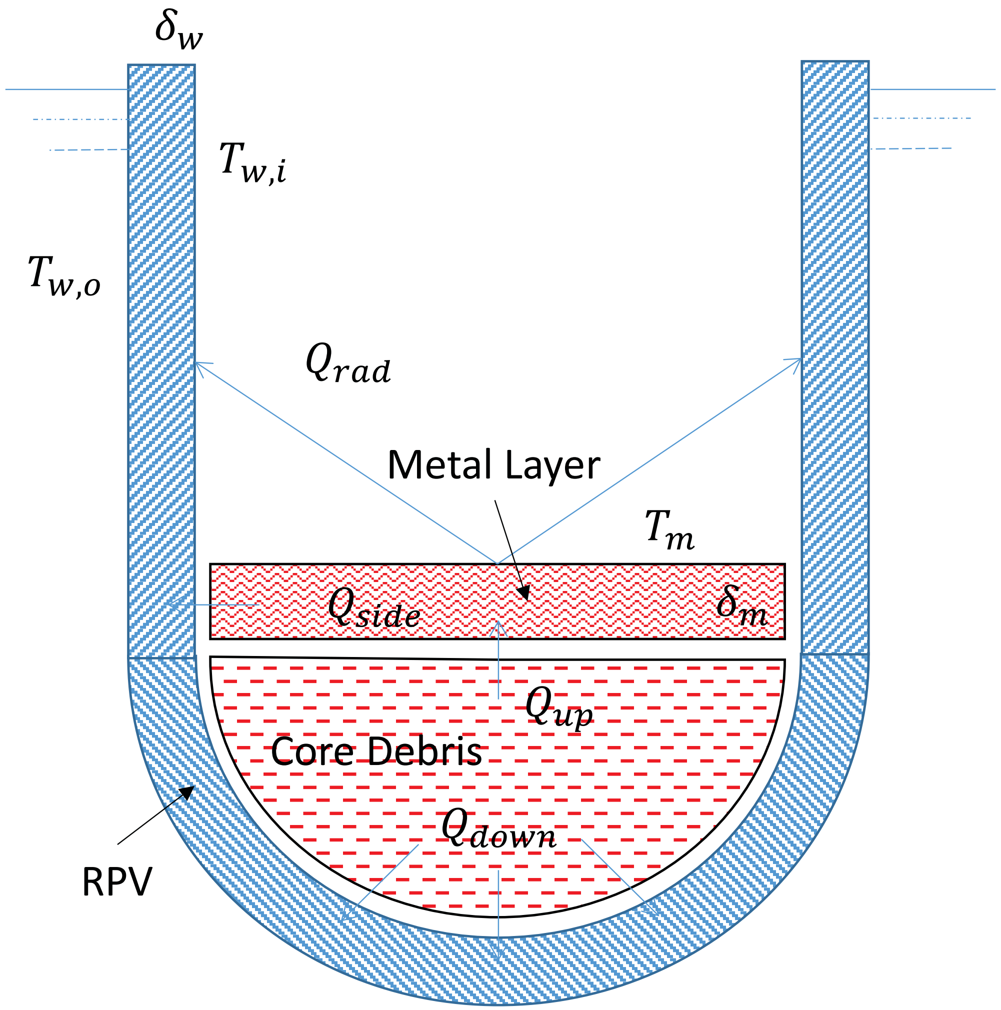


Figure 19.2-3: Illustration of Retention in Reactor Pressure Vessel versus Containment Vessel

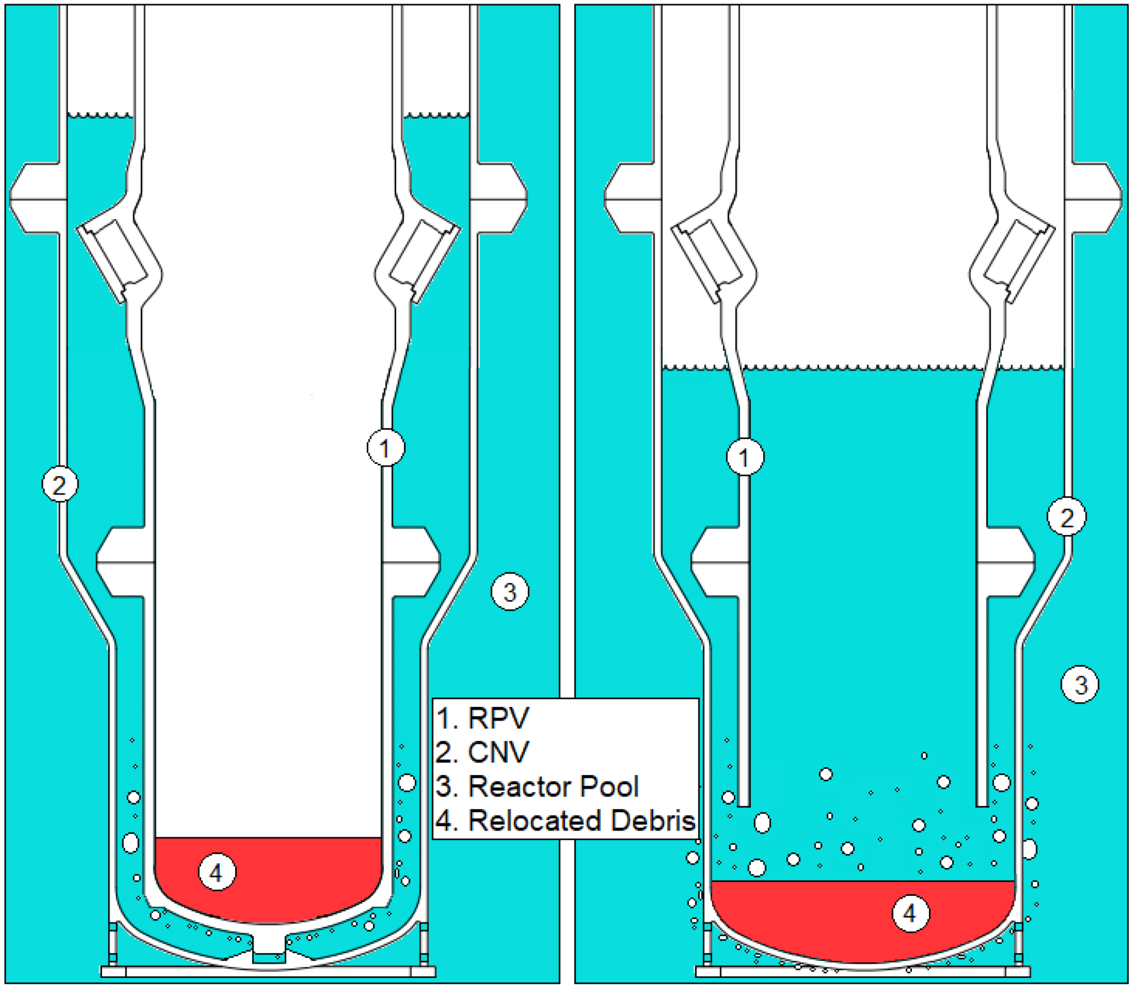


Figure 19.2-4: Hydrogen Generation versus Time

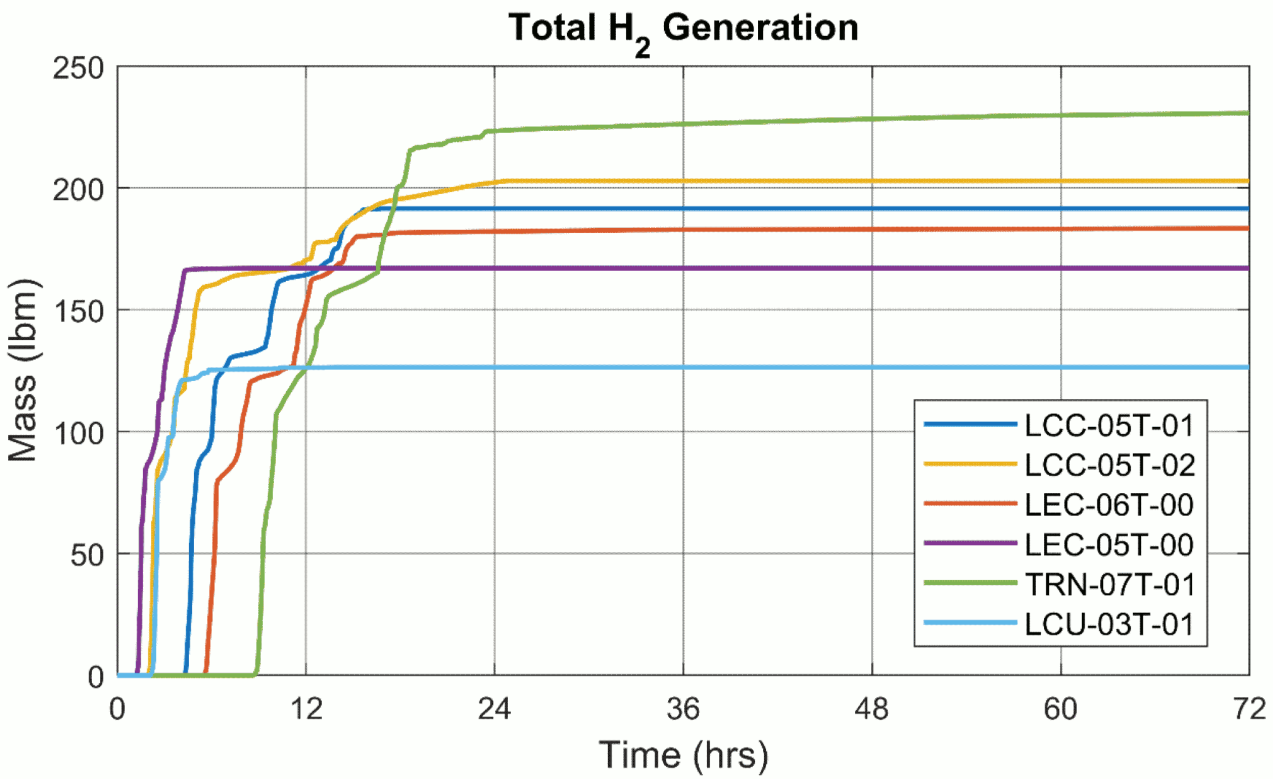


Figure 19.2-5: Oxygen Concentration versus Time

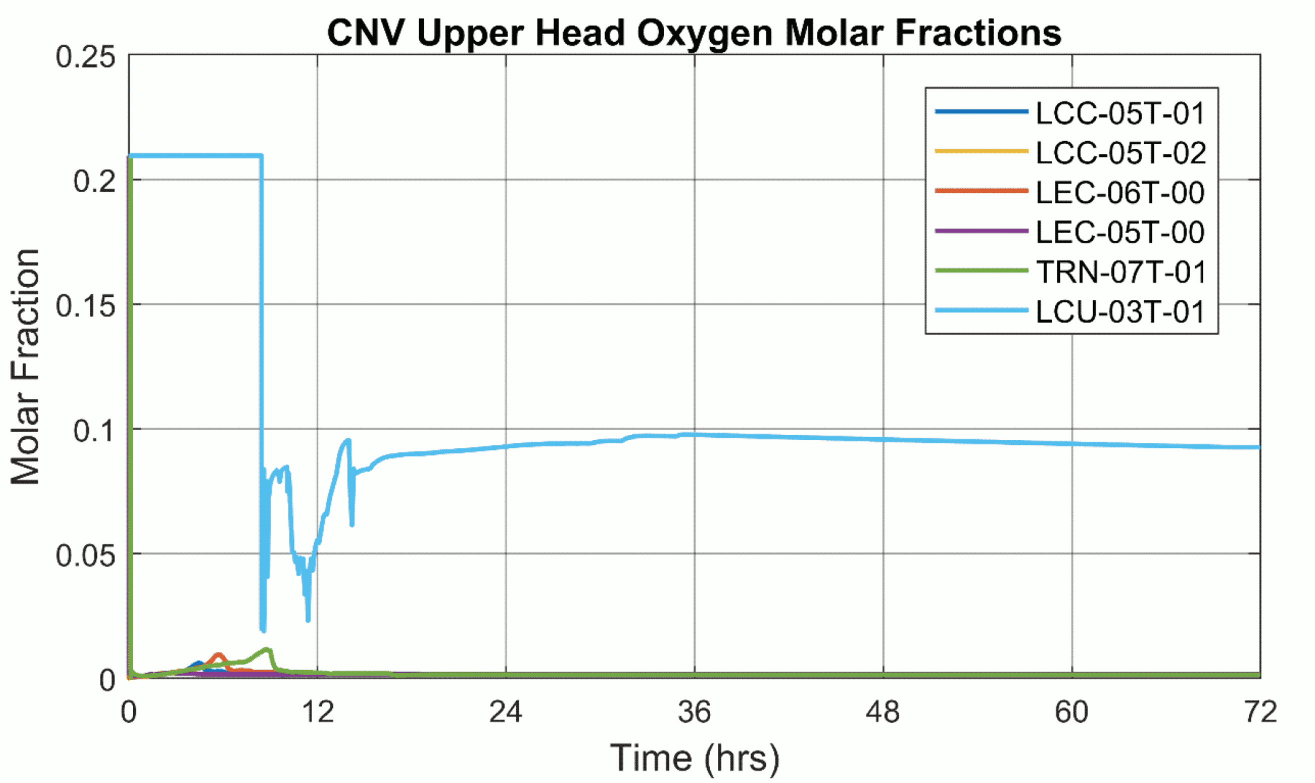


Figure 19.2-6: Pressure Differential between Reactor Pressure Vessel and Containment Vessel

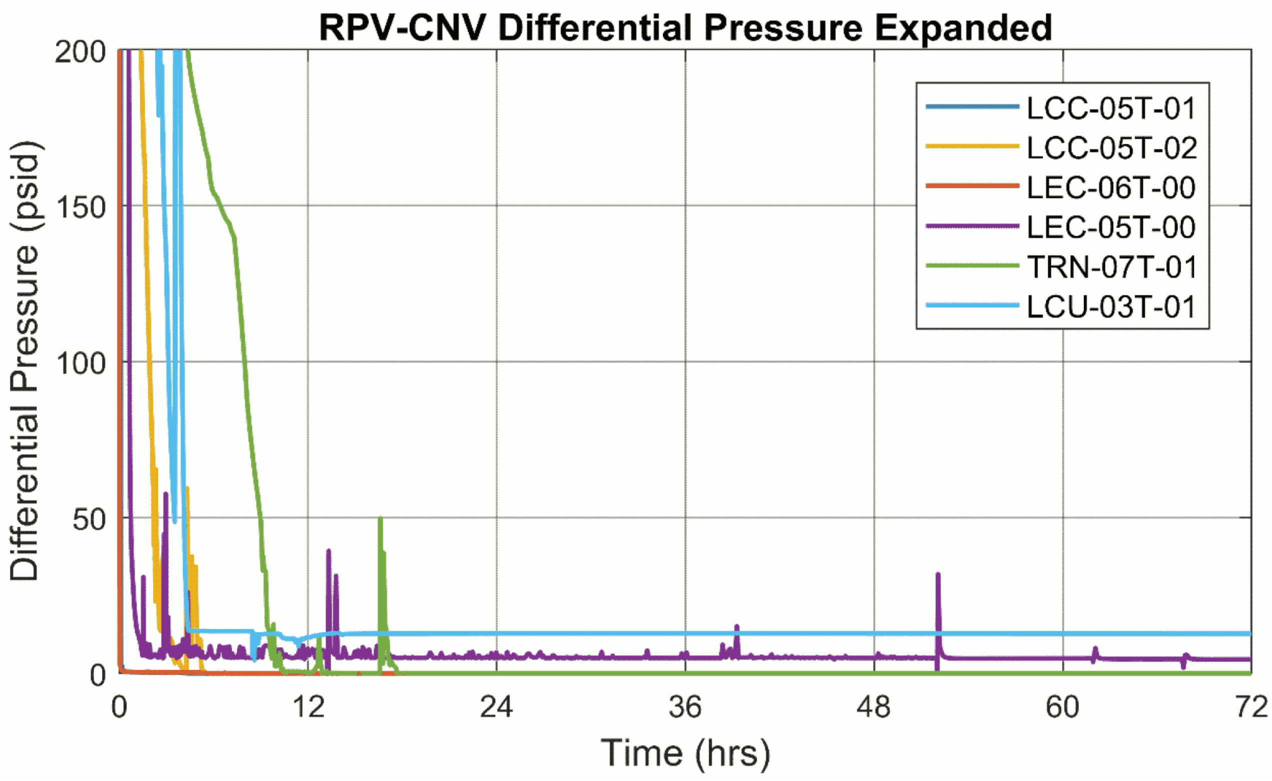
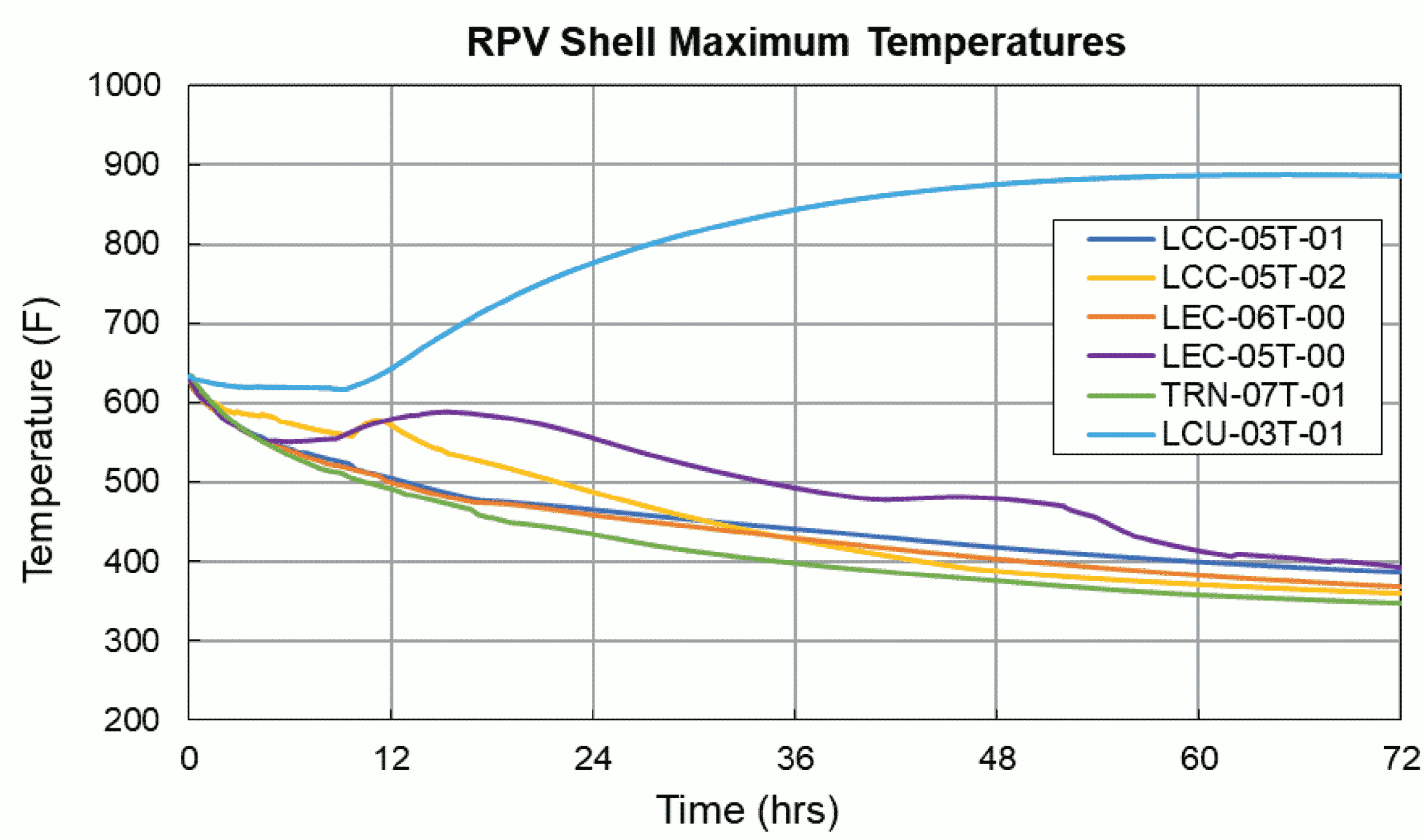


Figure 19.2-7: Maximum Reactor Pressure Vessel Shell Temperatures during Severe Accidents



19.3 Regulatory Treatment of Nonsafety Systems

Nuclear Regulatory Commission (NRC) policy requires regulatory oversight for certain nonsafety-related structures, systems, and components (SSC) that perform risk-significant functions. The Regulatory Treatment of Nonsafety Systems (RTNSS) process addresses the regulatory oversight necessary for SSC that fall into this category.

The RTNSS process provides assurance that

- the design of the nonsafety-related, risk-significant SSC satisfies the performance capabilities and reliability and availability (R/A) missions.
- proper design information for the Reliability Assurance Program, including the design information for implementing the Maintenance Rule, is included.
- 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 scope, process, and criteria are consistent with the guidance of NUREG-0800 Section 19.3.

19.3.1 Regulatory Treatment of Nonsafety Systems 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.

The designation of the SSC within the RTNSS program scope reflects the applicable criterion. For example, the SSC that satisfy RTNSS criterion A are RTNSS A SSC.

COL Item 19.3-1: An applicant that references the NuScale Power Plant US460 standard design will identify site-specific Regulatory Treatment of Nonsafety Systems structures, systems, and components and applicable process controls.

Identification of nonsafety-related SSC in the RTNSS process involves the following probabilistic and deterministic evaluations:

- Probabilistic:
  - Focused PRA insights
- Deterministic:
  - anticipated transients without scram (ATWS) rule (10 CFR 50.62)
  - Station Blackout (SBO) rule (10 CFR 50.63)
  - Actions required beginning 72 hours after a design-basis event and lasting the following 4 days
  - Seismic considerations

- Adverse interactions between nonsafety-related SSC and safety-related systems
- Design Reliability Assurance Process (D-RAP) expert panel decisions

19.3.2 Structures, Systems, and Components Identification and Designation within Regulatory Treatment of Nonsafety Systems Program Scope

The scope of the RTNSS Program includes those nonsafety-related SSC that satisfy the RTNSS criteria and are therefore subject to additional regulatory treatment. The following sections discuss evaluation of the nonsafety-related SSC and the results of the evaluation.

19.3.2.1 Regulatory Treatment of Nonsafety Systems A

Evaluation of nonsafety-related SSC functions identified through the D-RAP process in Section 17.4 provides the basis for whether they are relied upon to meet beyond-design-basis deterministic performance requirements for ATWS (10 CFR 50.62) or SBO (10 CFR 50.63).

The design does not include an auxiliary or emergency feedwater system; therefore, portions of 10 CFR 50.62(c)(1) are not applicable. Based on the design of the module protection system (MPS), the design supports an exemption from the requirement of 10 CFR 50.62(c)(1) for a diverse turbine trip system, as described in Section 15.8. The intent of the diverse turbine trip system is met through diversity within the MPS design that addresses the concern of a common cause failure. The MPS is a safety-related system and is not subject to RTNSS criteria. Examination of the focused PRA to determine if nonsafety-related SSC are required to mitigate an ATWS indicates that a NuScale Power 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. Section 8.4 describes the SBO coping analysis for the NuScale Power Plant, and concludes that the design functions adequately during an SBO. The SBO analysis described in Section 8.4 demonstrates that core cooling and containment integrity are successfully maintained with only safety-related systems and no reliance on alternating current power systems. As such, there are no SSC for mitigating SBO that meet RTNSS criteria.

Based on the MPS design resulting in an ATWS contribution to CDF lower than the safety goal, and the SBO transient analysis concluded that nonsafety-related SSC functions are not required to meet the SBO regulatory acceptance criteria, no SSC are classified as RTNSS A.

19.3.2.2 Regulatory Treatment of Nonsafety Systems B

Nonsafety-related SSC functions identified through the D-RAP process described in Section 17.4 are evaluated to determine whether they are relied upon to provide a long-term nonsafety-related backup to passive system functional capability and to address seismic events.

Safety analyses, PRA insights, and sensitivity studies (discussed in Chapter 15, Section 19.1, and Section 19.2, respectively) provide reasonable assurance that core cooling and containment integrity is maintained during the time period beginning 72 hours after a design-basis event and lasting the following 4 days, with only safety-related SSC, consistent with SECY-96-128.

The NuScale Power Modules are partially immersed in the reactor pool. The reactor pressure vessel is housed in a steel containment vessel that transfers sensible and core decay heat through the containment vessel walls and the decay heat removal system (DHRS) to the ultimate heat sink that provides a passive heat sink for both short and long-term heat removal. 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 perform the functions of core cooling and containment cooling.

Demonstration of core cooling and containment integrity is addressed as follows for initiating events that result in cooling using DHRS:

- The reactor remains subcritical during DHRS operation. The core reactivity balance depends on time in cycle and the success of control rod insertion. The emergency core cooling system (ECCS) actuates after a reactor trip to maintain subcriticality, but operators can bypass ECCS if subcriticality under cold conditions is confirmed.
- Maintaining coolable geometry requires ensuring that boron precipitation does not occur. The DHRS operation is non-limiting compared to ECCS operation for boron precipitation.
- The DHRS transfers decay and residual heat to the reactor pool. Limiting conditions for heat removal occur within 72 hours of event initiation while the DHRS condensers remain covered. A pool boil off analysis demonstrates that, assuming the ultimate heat sink is initially at the minimum level and maximum temperature allowed by technical specifications, and six modules are rejecting heat to the reactor pool, with realistic decay heat, the pool level remains above the top of the DHRS condensers for more than 7 days.
- During DHRS operation, there is no sustained mass and energy release into containment, and containment integrity is not challenged.

Demonstration of core cooling and containment integrity is addressed as follows for initiating events that result in cooling using ECCS and DHRS:

- The reactor remains subcritical during ECCS and DHRS operation. The initial core reactivity balance depends on time in cycle and success of control rod insertion. Safety analyses, described in Section 15.0.5, Extended Passive Cooling for Decay and Residual Heat Removal, demonstrate that the core boron concentration remains above the concentration required to demonstrate subcriticality, accounting for the highest worth control rod stuck out. These analyses demonstrate that the limiting time for subcriticality occurs in the first

72 hours of the event. Therefore, the analyses bound the 7-day evaluation conditions with respect to subcriticality.

- Maintaining coolable geometry requires ensuring that boron precipitation does not occur. Safety analyses biased for cold pool conditions, described in Section 15.0.5, demonstrate the boron concentration in the reactor coolant system remains below the precipitation limit in the first 72 hours of these initiating events. The reactor coolant system temperature rise due to reactor pool heatup provides additional margin to the solubility limits during the 7-day period considered by RTNSS.
- The ECCS and DHRS transfer decay heat to the reactor pool. As described above, the DHRS condensers remain covered for more than 7 days. The ECCS cooldown analysis presented in Section 15.0.5 that is biased for maximum temperature assumes pool temperature is close to boiling, and uses a bounding low reactor pool level. These assumed conditions bound the 7-day pool boil off analysis described above.

Therefore, analyses demonstrate core cooling and containment integrity are maintained, and nonsafety-related SSC are not relied on to perform a RTNSS B function for the period beginning 72 hours after a design-basis event and lasting the following 4 days to ensure long-term safety.

The RTNSS B evaluation process also considered if nonsafety-related SSC are candidates for additional regulatory oversight from seismic considerations.

As described in Section 19.1.5, the seismic margins analysis (SMA) models both active and passive nonsafety-related SSC as well as safety-related SSC. This analysis identifies few component failures that have the potential to contribute to seismic risk.

For passive nonsafety-related SSC, SMA evalution concludes that the design meets the regulatory requirement for a high confidence of low probability of failure value that is greater than 1.67 times the design-basis safe shutdown earthquake with safety functions being maintained utilizing only safety-related SSC. Thus, additional regulatory oversight for these components is not in the scope of the RTNSS program.

Therefore, no nonsafety-related SSC meet the RTNSS B criteria.

19.3.2.3 Regulatory Treatment of Nonsafety Systems C

Nonsafety-related SSC functions are evaluated to determine whether they are relied upon under power operating and shutdown conditions to meet the NRC core damage frequency (CDF) goal of less than 1.0E-4 each reactor year and large release frequency (LRF) goal of less than 1.0E-6 each reactor year.

A focused PRA, described in Section 19.1.9, uses the PRA model to evaluate CDF and LRF by crediting only safety-related SSC and assuming that all nonsafety-related SSC fail. The results of the focused PRA meet the CDF and LRF RTNSS C acceptance criteria.

The scope of the RTNSS program includes consideration of nonsafety-related active systems to compensate for uncertainties in the PRA and in the modeling of severe accident phenomenology. The PRA assesses the uncertainties in the modeling and performance of passive safety systems, including the likelihood that the passive safety systems might operate outside of the conditions where core heat removal would be effective.

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

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

19.3.2.4 Regulatory Treatment of Nonsafety Systems D

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

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

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

19.3.2.5 Regulatory Treatment of Nonsafety Systems E

Evaluation of RTNSS E criteria involves identification of potential significant adverse interactions among passive safety-related systems and active nonsafety-related SSC. This evaluation is accomplished by analyzing the system functions that are identified through the D-RAP process. After identification of passive safety-related functions, the active nonsafety-related functions that interface with the passive safety-related functions are identified. Potential adverse interactions among the systems that could prevent accomplishment of the passive safety-related functionality are then evaluated.

Results of this evaluation demonstrate that all passive safety-related functions operate independently and no nonsafety-related SSC function is relied on to prevent an adverse interaction between a passive safety-related function and active nonsafety-related SSC. Therefore, no SSC are classified as RTNSS E.

19.3.3 Functional Design of Regulatory Treatment of Nonsafety Systems Structures, Systems, and Components

An 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.

Reliability and availability missions are not established for the nonsafety-related, risk-significant SSC because, 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

Section 19.1.9 describes the focused PRA. 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 systems. The focused PRA demonstrates that nonsafety-related SSC are not needed to meet the NRC's CDF and LRF safety goals. Because the calculated risk metrics are 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 below.

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?

Section 19.1.4 discusses the criteria for internal event initiators evaluated for potential risk-significance (Reference 19.3-1). Nonsafety-related SSC that contribute to potential initiating events are evaluated for inclusion in the RTNSS program.

Nonsafety-related SSC need not be included in the RTNSS program where unavailability of nonsafety-related SSC would either (1) preclude module operation (e.g., chemical and volume control system), such that it would no longer contribute to an initiating event frequency, or (2) would require that another nonsafety-related SSC (e.g., an alternating current 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. Additionally, sensitivity studies 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 NRC goals.

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 are identified for the 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 ensure they meet their RTNSS B function.

Because no RTNSS B SSC are identified for the NuScale Power Plant design, no RTNSS augmented design standards are applied.

19.3.6 Regulatory Controls for Nonsafety Structures, Systems, and Components

Regulatory oversight of RTNSS structures, systems, and components 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 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 availability control limited conditions of operation and surveillance requirements provides assurance that the RTNSS structures, systems, and components can meet their R/A missions and that the component availability is consistent with its R/A mission.

Because no RTNSS SSC are identified, no additional regulatory oversight is required for nonsafety-related risk-significant SSC.

19.3.7 References

19.3-1 NuScale Power, LLC, “Risk Significance Determination,” TR-0515-13952-NP-A, Revision 0, October 2016.

19.4 Strategies and Guidance to Address Mitigation of Beyond-Design-Basis Events

An applicant that references the NuScale Power Plant US460 standard design has the responsibility of addressing mitigation of beyond-design basis events in accordance with 10 CFR 50.155.

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). NuScale performed a design specific aircraft impact assessment (AIA), of the Reactor Building (RXB), using realistic analyses to demonstrate that:

- the reactor core remains cooled or the containment remains intact; and
- spent fuel cooling or spent fuel pool integrity is maintained.

The NuScale Power Plant US460 standard design meets the criteria as discussed in the following sections.

The specific assumptions for the AIA are based on the guidance in Regulatory Guide (RG) 1.217, Revision 0, "Guidance for the Assessment of Beyond-Design-Basis Aircraft Impacts." The assessment follows the guidelines in NEI 07-13 (Reference 19.5-1) with no exceptions.

19.5.2 Scope of the Assessment

NuScale assessed the following effects of a large commercial aircraft impact:

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 structures, systems, and components (SSC).

3) Fire damage resulting from aviation fuel-fed fire.

19.5.3 Assessment Methodology

The methodology in NEI 07-13 is used to assess effects of aircraft impact on the structural integrity of the 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 or integrity.

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 six 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, prevents wreckage from perforating exterior steel-composite walls of the RXB, and prevents pressurized or propagated fire from entering SC-I areas of the

RXB. Therefore, the RXB is a building of concern. The Control Building (CRB) is a building of concern prior to an imminent aircraft impact because core cooling is accomplished by operator control actions upon notification of a threat. Section 1.2 addresses key design features of the RXB.

19.5.3.2 Impact Locations

Below-grade portions of the RXB are not susceptible to a direct impact by an aircraft. Based on NEI 07-13 (Reference 19.5-1) screening criteria, there are no adjacent structures or buildings credited as intervening structures for the AIA. No credit is taken for the Radioactive Waste Building (RWB), CRB or the Turbine Generator Building (TGB) as intervening structures. All 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 is maintained in the reactors and SFP.

19.5.4 Assessment Results

19.5.4.1 Physical Damage

The RXB external walls 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 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 consists of two doors (Figure 19.5-1). The outer door (impact door) serves as a barrier for aircraft impact and other design basis conditions. An inner door (blast door) serves primarily for security, airtightness, blast, fire, flood, and other design-basis conditions. The impact door is designed to be wider on each side of the blast door framing to support bearing on the SC walls. Local reinforcement is provided as required at the wall to slab connection at the 146 ft 6 in. elevation. This is a key design feature. Local detailing in the wall to wall connection region as required using ties is a key design feature. The structural beam seat connections of roof beams on 187 ft elevation are key design features.

The design of the Reactor Building penetration and piping protections are key design features for preventing physical damage and fire from entering the RXB. The exterior wall penetration protection (awning) is designed and constructed to provide strength to prevent perforation due to a direct aircraft strike. The exterior wall penetration protections are constructed of 7000 psi concrete with two #11 bars at 12 inches on each face of the awning and each way (horizontal and vertical directions). In addition, the awning protection has #5 shear ties at 12 inches on center.

The NEI 07-13 criteria (Reference 19.5-1) are used to minimize physical damage from strikes to external openings in the RXB external walls. Doors and penetrations leading into SC-I portions of the RXB are protected to prevent physical damage and fire from an aircraft impact from entering SC-I portions of the RXB.

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 do not result in the crane falling into the reactor pool area and damaging the NPMs or damaging the RXB structure containing the UHS. The design and location of the RBC as described in Section 9.1.5 is a key design feature for protecting the NPMs.

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 affected equipment.

Shock effects do not affect the spent fuel pool structure nor the ability to retain the pool water inventory. The NPMs are shut down by operator action before impact, and core cooling is provided by passive systems (e.g., the decay heat removal system (DHRS)). There are no SSC susceptible to shock (sensitive electronics or active components) on the NPMs that interrupt or prevent successful core cooling once the reactor is tripped, the DHRS is actuated, and containment is isolated.

There is no impact of concern below the 55-ft elevation. The SFP cooling equipment is located on elevation 55 ft and 70 ft of the RXB. Other affected equipment at the 55 ft, 70 ft, 85 ft, 100 ft, 126 ft, and 146 ft 6 in. 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 in the RXB are key design features for the protection of core cooling equipment from the impact of a large commercial aircraft. The assessment credits the design and location of fire barriers, as depicted in Figure 1.2-8 through Figure 1.2-15, to limit effects of internal fire in the RXB to non SC-I areas, where there is no equipment required to maintain core cooling. In addition, the design and location of 5-psid blast dampers in the Reactor Building HVAC system air intakes and exhaust lines (described in Section 9.4.2) 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, passive containment isolation barriers, and containment instruments.

The CNV is an evacuated pressure vessel described in Section 3.1.5, Section 3.8.2, and Section 6.2.1. The CNV is maintained partially immersed in a below-grade, borated-water-filled, stainless-steel lined floor, reinforced concrete (RC) basemat and slabs and steel-plate composite (SC) pool walls to facilitate heat removal.

The containment remains intact if the ultimate pressure capability of the CNV, as described in Section 3.8.2, is not reduced as a result of the aircraft impact. As stated in Section 19.5.4, there is no physical damage or fire damage to equipment required for fuel cooling in the NPM, including the CNTS. Far shock 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, shown on Figure 1.2-3, 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 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 air cooled condenser system.

Post reactor trip, two independent safety-related passive DHRSs, described in Section 5.4.3, 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 TGB 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 (MCR) 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) 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 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 necessary after aircraft impact for 72 hours, as described in Section 9.2.5.

The NuScale Power Modules, reactor coolant system, containment vessel, decay heat removal system, containment isolation valves, and ultimate heat sink are key design features for ensuring core cooling. The closure of the main steam isolation valves and feedwater isolation valves as described in 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 main control room, as described in Chapter 7 are key design features for ensuring the reactor is tripped, containment is isolated, and the DHRS is actuated before aircraft impact. Because 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 main control room 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 is not scrammed before 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 design uses SC interior and exterior walls and RC basemat and slabs. The foundation of the SFP is constructed as described in Section 3.8.5. The reinforced concrete floor has 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, 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 1.2-8 through Figure 1.2-15, is a key design feature for maintaining SFP integrity from a direct aircraft impact.

There are multiple 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. The reactor building crane is designed to the ASME standards specified in Table 9.1.5-1. There are seismic restraints on the RBC, as shown on Figure 9.1.5-1. 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. The design and location of the fuel handing equipment and reactor building crane, are key design features for ensuring the hoists remain intact and cannot fall into the SFP.

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 for beyond the mission time, even with the loss of forced SFP cooling. The SFP is part of the ultimate heat sink, which provides water inventory and ensures an adequate water level is maintained above the spent fuel assemblies.

19.5.5.5 Plant Monitoring and Control

For the postulated aircraft impact event, required operator actions occur before 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-aircraft impact monitoring is determined to be unavailable, mitigating strategies for the loss of large area (LOLA) beyond-design-basis event are invoked. The actions taken by the operators before 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 US460 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, Revision 8, Washington, DC, April 2011.

Figure 19.5-1: General Arrangement Reactor Building Equipment Door

{{ Withheld - See Part 9 }}