## 19.1 Probabilistic Risk Assessment

Section 19.1 describes the probabilistic risk assessment (PRA) performed by AREVA NP for the U.S. EPR design. This PRA is a Level 1 and Level 2 PRA and addresses the risks associated with nominal full-power operation, low-power operation, and shutdown conditions. The PRA assesses both internal and external events (except acts of sabotage).

Section 19.1 provides the content as required by the NRC regulations and guidance including Section 19 of NUREG-0800, Standard Review Plan (Reference 1) for the design certification phase. The information provided in Section 19.1 includes a description of how the PRA was performed and the technical methods that were used. Section 19.1 also provides a summary of results that demonstrates the manner by which the PRA satisfies the intended uses.

### 19.1.1 Uses and Applications of the PRA

#### 19.1.1.1 Design Phase

AREVA NP has made use of the PRA through the design phase. These uses include the following:

- To determine how the risk associated with the design compares against the quantitative objectives established by the Commission that the core damage frequency (CDF) should be less than 1.0E-04/yr and that the large release frequency (LRF) should be less than 1.0E-06/yr.
- To determine how the risk associated with the design compares against the Commission's containment performance goals, which consist of two elements:
  - A probabilistic objective that the conditional containment failure probability (CCFP) be less than approximately 0.1 for the composite of all core-damage sequences assessed in the PRA.
  - A deterministic goal that containment integrity be maintained for approximately 24 hours following the onset of core damage for the more likely severe-accident challenges.
- To identify risk-informed safety insights based on systematic evaluations of the risks associated with the design.
- To provide PRA importance measures for input to the Reliability Assurance Program (RAP). Refer to Section 17.4 for a description of the RAP.

The PRA is not used for any formal risk-informed applications, such as 10CFR50.69, Risk-Informed Categorization and Treatment of structures, systems and components (SSC) and 10CFR50.48, Fire Protection.

A COL applicant that references the U.S. EPR design certification will describe the uses of PRA in support of site-specific design programs and processes during the design phase.

#### 19.1.1.2 Combined License Application Phase

This FSAR section is provided as part of the design certification process. Uses of the PRA that would be related to a specific COL application are not addressed at this time.

A COL applicant that references the U.S. EPR design certification will describe the uses of PRA in support of licensee programs and identify and describe risk-informed applications being implemented during the combined license application phase.

#### 19.1.1.3 Construction Phase

This FSAR section is provided as part of the design certification process. Uses of the PRA that would be related to a specific COL application and associated construction activities are not addressed at this time.

A COL applicant that references the U.S. EPR design certification will describe the uses of PRA in support of licensee programs and identify and describe risk-informed applications being implemented during the construction phase.

#### 19.1.1.4 Operational Phase

This FSAR section is provided as part of the design certification process. Uses of the PRA that would be related to the operating phase for the U.S. EPR design are not addressed at this time.

A COL applicant that references the U.S. EPR design certification will describe the uses of PRA in support of licensee programs and identify and describe risk-informed applications being implemented during the operational phase.

### 19.1.2 Quality of PRA

Section 19.1.2 identifies the attributes of the U.S. EPR PRA design that make the PRA suitable for use in support of the design process and design certification. The provisions of 10 CFR 50, Appendix B, do not apply to the PRA for design certification or COL. The PRA, however, was performed using applicable AREVA NP quality assurance procedures and methods to achieve and maintain a quality assessment. The quality methods include the following:

- Use of qualified personnel: qualified analysts have performed each of the technical elements of the PRA. Analysts completed technical tasks in areas where they were knowledgeable and understood the approach, methods and limitations of the respective analyses.

- Use of procedures to control documentation: each element of the PRA is formally documented in an evaluation report (or calculation) prepared according to AREVA NP procedures. Each PRA evaluation report was independently reviewed by a qualified member of the project team. Any change or addition to a PRA evaluation report is also governed by procedure to control the configuration of the PRA. Each document revision requires independent review consistent with that performed for the original version. The PRA evaluation reports are controlled documents and are maintained in archival form.

- Use of procedures to control corrective actions: The conduct of the PRA is governed by the AREVA NP Corrective Action Program, which establishes requirements for promptly identifying and resolving errors or conditions that are adverse to quality. In addition to corrective action requirements, the design control process provides a mechanism for changes in design, assumptions and supporting analyses to be reviewed by PRA personnel for potential impact on the PRA.

These are general but essential steps to ensure the technical quality of the PRA. With respect to producing a PRA adequate to meet the needs of the design certification process, Section 19.1.2.1 defines the scope of the PRA that AREVA NP has completed for the design. Section 19.1.2.2 addresses the level of detail reflected in the models and other elements of the PRA. Section 19.1.2.3 describes the standards and other guidance that AREVA NP has employed to provide a PRA that is technically adequate to support the applications described in Sections 19.1.1 and 19.1.3. Section 19.1.2.4 outlines the steps that have been taken to maintain the PRA as the design has evolved and to guide future updates to the PRA.

### 19.1.2.1 PRA Scope

The U.S. EPR PRA constitutes a Level 2 assessment. It includes an evaluation of the types of accidents that could lead to core damage, an assessment of their frequencies, an analysis of the containment response to these accidents, and characterization of the magnitude and frequencies of releases of radionuclides that could result. The PRA addresses all applicable internal and external initiating events and all plant operating modes. Some initiating events are screened from detailed analysis based on their applicability to the U.S. EPR design while others are treated qualitatively, (e.g., high winds external event). The PRA employs traditional PRA techniques for quantitative evaluation of plant risks.

The approach used for risk evaluation of seismic events includes a PRA-based margins assessment rather than a seismic PRA. The PRA-based margins assessment is an acceptable methodology according to NRC guidance and SECY 93-087 (Reference 2). Although the PRA-based margins analysis does not result in the estimation of CDF or containment release frequency, it does yield valuable information regarding the ruggedness of the seismic design with respect to the potential for severe accidents.

### 19.1.2.2 PRA Level of Detail

To be effective in supporting the design process and to provide meaningful results with regard to judging the overall risk posed by the design, the PRA reflects a level of detail limited only by the following:

- The availability of certain design details, operating procedures, and other information.
- The level at which useful reliability data are available.

At the present time, elements of the detailed design that are not available to support the PRA include the following:

- The specific routing of piping. This information is particularly useful in the assessment of internal flooding events.
- The routing of control and power cables, which is relevant to a detailed assessment of internal fire events.
- The specific location of some equipment within plant buildings.
- Emergency and other operating procedures that would define the manner in which operating crews would respond to upset conditions and the specific actions they would be expected to take.

Analysis has been performed that is consistent with the level of detail available. For example, calculations of the frequencies of internal flooding events due to pipe failures account for the expected number of pipe segments in relevant systems (which are available), rather than the length of piping (which is not). In the case of internal fire events, the frequencies and the evaluation of equipment that could be affected reflect bounding assumptions. These assumptions have been refined, within the context of the available information, to avoid masking risk contributors from other sources due to overly conservative treatment.

A COL applicant that references the U.S. EPR design certification will describe the process to review as-designed and as-built information and conduct walk-downs as necessary to confirm that the assumptions used in the PRA, including PRA inputs to RAP and severe accident mitigation design alternatives (SAMDA), remain valid with respect to internal events, internal flooding and fire events (routings and locations of pipe, cable and conduit), and human reliability analyses (HRA) (i.e., development of operating procedures, emergency operating procedures (EOPs) and severe accident management guidelines and training), external events including PRA-based seismic margins, high confidence, low probability of failure (HCLPF) fragilities, and low power shutdown (LPSD) procedures.

The PRA reflects the details of system design configurations consistent with the design submitted to the NRC for design certification. A number of internal revisions of the PRA have followed the design developments. However, due to a need to "freeze" the design in reasonable time to allow for the PRA model development and quantification, some design change features have not been specifically included in the latest PRA model. Refer to Section 19.1.2.4 for information on post-"model freeze" date design changes that were not included in the current PRA results.

### 19.1.2.3 PRA Technical Adequacy

The content of the PRA and the steps taken to provide for its technical quality are consistent with the guidance in the PRA Standard (Reference 61). The ASME PRA Standard presents high-level requirements and, for each of these, a set of more detailed supporting requirements. The supporting requirements are evaluated to the three capability categories defined in the standard. These requirements were generally formulated for application to operating nuclear power plants, and in some cases cannot be explicitly satisfied for a PRA performed in the design phase. Table 19.1-1—Characterization of U.S. EPR PRA Relative to Supporting Requirements in ASME PRA Standard provides a high-level summary of the degree to which the U.S. EPR PRA satisfies supporting requirements (at least the Capability Category I) for nine of the technical elements addressed in the PRA Standard.

Because of the lack of detailed spatial information associated with the certified design, supporting requirements for internal fires and external events, were not considered in Table 19.1-1. This lack of detailed spatial information is also identified as a key source of uncertainty in Table 19.1-131, The basis for fires and other external events analysis are discussed below:

- The internal fire analysis: The U.S. EPR PRA for design certification uses the guidance provided in NUREG/CR-6850 (Reference 6) as practical. This report documents the most up-to-date methodology available for practical assessment of internal fires in nuclear power plants. Limitations in applying this methodology because some design details are not yet available are identified in Table 19.1-131.

- Other external events: The U.S. PRA for design certification uses a screening method to address other external events that could represent challenges to safe operation. The screening approach follows guidance provided in ANSI/ANS-58.21-2003 (Reference 7) and in NUREG-1407 (Reference 8).

- The U.S. EPR PRA employs a margins approach to evaluate potential vulnerabilities to seismic events. The PRA-based Seismic Margins Analysis (SMA) was performed in accordance with the applicable NRC guidance documents ISG-020 and SECY-93-087 (Reference 2), and in accordance with the applicable guidance in Part 5 of ASME-ANS RA-Sa-2009 Level 1 /LERF Standard (Reference 61) as endorsed by Regulatory Guide 1.200 (Reference 62).

The ASME PRA Standards and the associated NRC guidance on PRA adequacy apply only to accidents initiated from power operation. The U.S. EPR PRA also addresses LPSD modes. The LPSD PRA methodology and level of detail is consistent with industry practice and is state of the art.

A COL applicant that references the U.S. EPR design certification will conduct a peer review of the PRA relative to the ASME PRA Standard prior to use of the PRA to support risk-informed applications.

The U.S. EPR design development and probabilistic evaluation of its design features have benefited from the international cooperation between the U.S. and European divisions of AREVA NP. This cooperation includes sharing of PRA experience and technology through technical review meetings, independent reviews, and collaborative work assignments. This interaction has helped development of the U.S. EPR PRA models and provides added assurance that the U.S. EPR PRA approach is technically adequate, uses mature PRA techniques, and is sufficient to meet the PRA objectives for design certification.

Appropriate assumptions and bounding treatment were applied consistent with the level of detail for design certification. Areas in which these approaches have been employed, the general impact on the PRA, and the steps taken so that risk insights are not masked, include those that follow.

#### 19.1.2.3.1 Human Reliability Analysis

The human reliability analysis for the U.S. EPR PRA uses the methodology developed for the accident sequence evaluation program (ASEP) for the evaluation of events accounting for failures associated with pre-initiator human actions (Reference 9), and the NRC SPAR-H method for post-initiator actions (Reference 10).

Pre-initiator actions are screened, both qualitatively and quantitatively, using the ASEP methodology. Equipment is postulated that could be left unavailable prior to a demand. The human failure events associated with these actions are assessed based on the level of post-activity verification that is expected to apply. This approach may overstate the importance of individual pre-initiator actions, but such actions are judged not important to the overall results of the PRA due to the redundancy available in safety systems for the U.S. EPR.

For post-initiator actions, the PRA makes assumptions regarding general operator response based primarily on equivalent procedural guidance for current-generation plants. The number of post-initiator human actions that are included and assessed in the U.S. EPR PRA is relatively small compared to most PRAs for current plants. This reflects both a somewhat conservative treatment (i.e., some actions that might be credited are not) and the fact that some actions that would be required for current plants are not needed for the U.S. EPR. For example, there is no need to switch

suction sources for the safety injection systems (SIS) during a loss-of-coolant accident (LOCA). Careful review of the core-damage cutsets has identified areas in which further consideration of available operator actions is desired to ensure that the significance of particular accident sequences is characterized appropriately. Sensitivity studies also address the importance of operator response to the overall results and the insights obtained from them.

#### 19.1.2.3.2 Reliability Data

The U.S. EPR PRA uses reliability data from generic sources, since there is no plant-specific operating experience. Both a parametric uncertainty analysis and a set of sensitivity studies aimed at investigating the importance of parameters of particular interest are included in the PRA. These analyses help to ensure that appropriate insights are drawn from the quantitative results of the PRA, irrespective of the basic values assigned to these parameters.

#### 19.1.2.3.3 Internal Flooding Analysis

The PRA uses methods for estimating flooding initiating event pipe break frequencies that are appropriate for the level of information available. The PRA makes bounding assumptions with respect to the specific locations of equipment that could be affected by a flooding event. These assumptions are acceptable because the safety system redundancy and separation afforded by the U.S. EPR design limits their impact.

#### 19.1.2.3.4 Internal Fire Analysis

The internal fire analysis for the U.S. EPR PRA uses conservative initiating frequencies and bounding assumptions regarding the equipment that could be affected by a fire. As in the case of the analysis of internal flooding, the potential that such assumptions could lead to a gross overstatement of the risk associated with internal fires is limited because of the safety system redundancy and separation inherent to the U.S. EPR design. The impact of these bounding treatments has been considered carefully to avoid the potential that important risk insights could be masked.

### 19.1.2.4 PRA Maintenance and Upgrade

Each of the technical elements of the PRA is documented in a PRA engineering report. The level of detail in these PRA reports meets the documentation requirements set forth in the ASME PRA Standard and the associated NRC guidance on PRA adequacy. During preparation of the PRA, as additional design details became available, or as the design was modified, the PRA analysts were kept informed via design meetings, review of design documentation, and through the design change control process. Accordingly, the PRA represents the state of the design as submitted for certification design except as noted below.

The U.S. EPR PRA model is an evolving model. It is revised as needed to reflect design changes and to implement modeling enhancements. Because of an iterative nature of the interface between design and PRA, it is not always possible to incorporate all differences identified between the plant design changes and the PRA model in a timely manner. It is a common practice that a freeze of design inputs occurs a few months before a planned PRA release, in order to allow for the results production. A summary of the few plant design changes not included in the PRA model presented here and planned for a future revision to the model is provided below. These design changes will be assessed for impact on the PRA results in accordance with the PRA maintenance and update process described in Section 19.1.2.4.1; only design changes expected to have more than a negligible impact on the PRA results are discussed below:

1. Changes related to Fukushima Response: Design changes incorporated to address the Fukushima Near Term Task Force (NTTF) recommendation 4.2 have not been incorporated into the latest PRA model. Currently, the events addressed in these initiatives (a prolonged total station blackout) are assumed to lead to core damage. The newly developed FLEX strategies may lead to recoveries of some of these out-of-design-basis events. However, some of these strategies, may also impact the current mitigating equipment, resulting in new flow diversion paths, or affecting modeled power recoveries. Overall, it is expected that the cumulative impact from these changes on the PRA results and conclusions will not be significant.

2. Changes in PAS and SAS Logic: Recent logic changes made in PAS and SAS are relatively minor and their purpose is to reduce the potential consequences of digital I&C common cause failure (CCF). As such, it is expected that the effect of these changes on the PRA is to decrease the uncertainty in the contribution of I&C common cause failure. The specific impact of these changes will be assessed in accordance with the PRA maintenance and update process described in Section 19.1.2.4.1.

3. RCP Seals Change: Changes to the RCP seals valves type and power supplies (as a part of Fukushima Response – Secondary Side Feed and Bleed) are analyzed in the sensitivity runs for internal, flood, fire and shutdown events. An overall impact on the total CDF is less than five percent.

### 19.1.2.4.1 Description of PRA Maintenance and Update Program

The U.S. EPR PRA model and supporting documentation are maintained so that they continue to reflect the as-designed characteristics of the plant. Consistent with the ASME PRA Standard, Reference 5, and RG 1.200, a process is in place to perform the following as applicable to the certified design:

- Monitor PRA inputs and collect any new information relevant to the PRA.
- Maintain and upgrade the PRA to be consistent with the design.
- Consider cumulative impacts of pending changes when applying the PRA.

- Consider impacts of changes for previously implemented risk-informed decisions that used the PRA (e.g., RAP).

- Maintain configuration control of the computational methods used to support the PRA.

- Document the PRA model and processes.

To meet the guidance of Regulatory Guide 1.206, the PRA should be maintained to ensure that it reasonably reflects the design to be certified.

Pending design changes will be assessed against the PRA model periodically and the cumulative impact on the CDF and LRF will be determined and documented. Depending on the impact to the cumulative CDF and LRF risk measures, further actions may be taken as described below:

1. If the impact on the cumulative CDF and LRF risk measures is less than 10 percent (positive or negative), then no further action is required.

2. If the impact on the cumulative CDF and LRF risk measures is greater than 10 percent (positive or negative), then further impact on the PRA will be evaluated. This evaluation will include the following steps:

   A. Determine if the new risk measures challenge the safety goal.

   B. Determine if the new results identify any changes to the PRA input to the Reliability Assurance Program (RAP) in terms of added or deleted items.

   C. Determine if the new results invalidate the PRA insights or assumptions documented in Tables 19.1-108 and 19.1-109.

If the results of all of the above inquiries are negative, no further action is required.

If the results of any of the above inquiries are positive, the impact(s) will be reported to the NRC. Any further actions will be determined and taken as appropriate, including any additional updates to the FSAR.

3. Section 19.1.2.4 will be updated periodically to summarize the impact of important design changes on the PRA results.

The NRC will be notified and a PRA model update will be initiated if it is determined that the effects of the design change(s) since the last update to the PRA Model of Record are such that the PRA no longer reasonably reflects the design to be certified.

A COL applicant that references the U.S. EPR design certification will describe the applicant's PRA maintenance and upgrade program.

### 19.1.3 Special Design/Operational Features

The U.S. EPR is a 4590 MWt evolutionary pressurized water reactor (PWR) that combines proven technology with innovative system configurations to enhance safety. The EPR was originally developed through a joint effort between Framatome ANP and Siemens KWU in the 1990s by incorporating key technological and safety features from the French and German reactor fleets. The U.S. EPR version is an adaptation of the EPR to conform to U.S. codes, standards, and regulatory requirements. The design features that contribute to the low core damage frequency and large release frequency compared to the current operating fleet of PWRs are described in the sections that follow.

#### 19.1.3.1 Design/Operational Features for Preventing Core Damage

The U.S. EPR design incorporates many features that reduce the potential core-damage accidents that have been assessed to be important for current-generation PWRs. These features are summarized below. Their relevance to the low CDF for the U.S. EPR is described in more detail in Section 19.1.4.

##### 19.1.3.1.1 High Level of Redundancy and Independence for Safety Systems

The U.S. EPR design incorporates four trains of safety systems, including the emergency core cooling systems (ECCS), the emergency feedwater (EFW) system, and the support systems needed to allow these systems to function. In addition to being highly redundant, these trains are housed in four separate buildings. This separation reduces the risk of common failure of multiple trains due to postulated internal or external hazards.

##### 19.1.3.1.2 Highly Redundant Onsite Power System

The U.S. EPR design includes four emergency diesel generators (EDGs), one supporting each safety division. In addition to the four EDGs, there are two backup SBO diesel generators. The SBO diesel generators are diverse from the EDGs in model, control power, HVAC, engine cooling, fuel system, and location. This U.S. EPR electrical design reduces the risk associated with loss of offsite power (LOOP) and SBO.

##### 19.1.3.1.3 Stand Still Seal System for Reactor Coolant Pumps

The potential for leakage or small LOCAs (SLOCA) due to failure of reactor coolant pump (RCP) shaft seals has been an important risk contributor for many PWRs. The U.S. EPR design includes a stand still seal for each RCP. The stand still seal is a pneumatic, “metal-to-metal” seal that serves as a back-up seal, and is independent of the normal shaft seal. The stand still seal system (SSSS) reduces the risk of a LOCA event as a result of postulated RCP seal degradation.

#### 19.1.3.1.4 In-Containment Refueling Water Storage Tank

The refueling water storage tank for the U.S. EPR is located inside the Reactor Containment Building. The SIS draws suction from the in-containment refueling water storage tank (IRWST). Because coolant discharged from the RCS drains to the IRWST, it is not necessary to switch suction sources following a LOCA. Thus, the IRWST eliminates the need for ECCS suction transfer for long-term recirculation. Failure to affect the suction transfer is an important contributor to CDF for many PWRs. Furthermore, the Reactor Containment Building affords the IRWST better protection against some types of external events than is the case for equivalent tanks at current-generation plants.

#### 19.1.3.1.5 Capability for Full-Load Rejection

The design includes the capability to withstand a full load rejection without tripping the reactor. In the event of a load rejection, the reactor and turbine would automatically run back to a power level sufficient to allow the main generator to continue to supply the plant auxiliary loads. This design would reduce the potential for reactor trip and challenge to onsite emergency power systems for grid-centered loss of power events.

#### 19.1.3.1.6 Arrangement of Auxiliary Transformers

During normal operation, two auxiliary transformers supply power directly from the switchyard to all four safety-related switchgear divisions. An additional two transformers supply the non-safety-related switchgear. Since the main generator does not normally supply auxiliary loads in this configuration, a reactor trip does not create a demand for fast transfer to an offsite power source. Moreover, there are redundant feeds for each switchgear division (safety-related and non-safety-related), so that loss of an individual auxiliary transformer will not affect the continued supply of offsite power to plant loads.

#### 19.1.3.1.7 Extra Borating System

The extra borating system (EBS) provides manual injection capability of highly borated water into the reactor pressure vessel (RPV) in the event that the reactor shutdown system does not function properly. EBS is a two-train system which further reduces the potential contribution of accidents involving a failure to scram.

#### 19.1.3.1.8 Digital Instrumentation and Control Systems

The U.S. EPR uses state-of-the-art digital systems for instrumentation and control (I&C) functions. The reliability of these systems enhances the automatic initiation of reactor shutdown, emergency feedwater, and safety injection functions. The man-

machine interface implemented through a computerized control room with conventional hardwired backup optimizes the information available to the operators.

#### 19.1.3.1.9 Medium-Head Safety Injection System

Among the features of the medium-head safety injection system (MHSI) is the provision for a shutoff head below the setpoints for the main steam safety valves (MSSV). In the event of an SGTR, the lower MHSI shutoff head limits the pressure differential which forces reactor coolant through the broken tube. The lower MHSI pressure will not challenge the associated MSSV to open. This reduces the potential for a release pathway from the RCS through the MSSV.

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

In addition to the features described in Section 19.1.3.1 to reduce the potential for core damage, the U.S. EPR design incorporates several measures to limit the possibility that a core-damaging accident could challenge containment integrity and cause a release. Among the measures that go beyond those found in current-generation plants are the following:

#### 19.1.3.2.1 Large, Robust Containment

The containment has sufficient free volume such that it is capable of withstanding the maximum pressure and temperature resulting from the release of stored energy during a postulated LOCA, main steam line break or severe accident.

#### 19.1.3.2.2 Primary Depressurization System

Core damage accidents in which the RCS is still at high pressure at the time the core debris causes failure of the RPV can be among the most severe challenges to containment integrity. The primary depressurization system is provided to allow the RCS to be depressurized during severe-accident conditions. This capability greatly reduces the potential for core melt ejection at high pressure and associated challenge to containment.

#### 19.1.3.2.3 Hydrogen Control

In addition to a containment design capable of withstanding the effects of the combustion of hydrogen, the containment is equipped with passive autocatalytic recombiners. These recombiners prevent the buildup of hydrogen concentration to limit the size of any hydrogen deflagration and prevent hydrogen detonation.

#### 19.1.3.2.4 Core Melt Retention System

The core melt retention system (CMRS) maintains the integrity of the containment by providing the ability to passively stabilize/cool molten core debris. A combination of passive and active devices allows water from the IRWST to flood the corium spreading area to remove heat from below the core debris via the cooling water channels. This design limits the potential for core-concrete interactions that could cause pressurization of the containment via the generation of non-condensable gases.

#### 19.1.3.2.5 Severe Accident Heat Removal System

The severe accident heat removal system (SAHRS) provides an active mean for removing heat from containment following a severe accident. The SAHRS removes containment heat via containment spray and recirculation and cooling of the IRWST inventory.

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

As outlined in the previous two sections, many features of the U.S. EPR design limit the potential for core damage to occur and further limit the possibility of containment failure as an additional line of defense. Measures that would limit the consequences of possible releases from containment include the following:

#### 19.1.3.3.1 Containment Spray via SAHRS

The SAHRS has the capability to perform a containment spray function. Spraying the containment would scrub the atmosphere of fission products, reducing the inventory that would be available for release in the event of containment failure.

#### 19.1.3.3.2 Containment and Outer Shield Building

The Containment and Outer Shield Building are separated by an annulus. The annulus is maintained sub-atmospheric by an active ventilation system to collect and filter containment leakages before release to the environment. It is noted that no credit is given in the U.S. EPR PRA for the active function of the annulus ventilation system.

### 19.1.3.4 Uses of the PRA in the Design Process

The U.S. EPR design incorporates the features noted in Section 19.1.3.1 and Section 19.1.3.2 specifically to address characteristics assessed to be weaknesses in the designs of the current operating fleet of PWR power plants. Table 19.1-2—Features for U.S. EPR that Address Challenges for Current PWRs summarizes the features of the U.S. EPR relative to the weaknesses they are intended to reduce or eliminate. These features are primarily those identified in NUREG-1560 (Reference 11) and NUREG-1742 (Reference 12).

Throughout the design process, the PRA plays an important role both in identifying features that merit consideration with respect to opportunities to reduce risk, and to review proposed design changes to evaluate the potential risk impact. As indicated earlier, PRA review of design changes is incorporated into the AREVA NP design change control process.

AREVA NP has also used insights from the PRA to identify specific improvements to reduce the contribution to risk due to some aspects of the design. The specific areas of improvement include the following:

#### 19.1.3.4.1 SBO Diesel Generators

The SBO diesel generators were added to reduce the contribution of SBO events initiated by a LOOP. The PRA also identified the need for the SBO diesel generators to be independent and diverse from the EDGs. To that end, the SBO diesel generators differ from the EDGs in model, control power, HVAC, engine cooling, fuel system, and location.

#### 19.1.3.4.2 Cooling of Low Head Safety Injection Pump Motors

Cooling water for the motors for two of the four low head safety injection (LHSI) pumps (Pumps 1 and 4) is aligned to the safety chilled water system (SCWS). Since Divisions 1 and 4 of the chilled water system are air cooled, the diversity extends to the heat sink used for cooling. This configuration eliminates the potential that CCF of the pumps motor cooling could disable the LHSI system function.

#### 19.1.3.4.3 Increased Diversity of Cooling Water for the SAHRS

As noted in Section 19.1.3.2, the SAHRS is available for containment heat removal and other functions in the long term after an accident. To provide further diversity with respect to the systems whose failure could lead to core damage, cooling for the SAHRS heat exchanger is achieved via a dedicated train of component cooling water (CCW) and essential service water (ESW).

#### 19.1.3.4.4 Increased Capacity of the Safety Chillers

To provide more redundancy in the HVAC model, capacity of the safety chillers is increased so that one chiller can cool two divisions. In the event that the running train of HVAC fails to support cooling, an automatic switchover is provided. In addition, HVAC fans are diversified, so they can be assigned to two different common cause groups.

#### 19.1.3.4.5 Closure of the Fire Water Distribution System (FWDS) valves to Isolate FWDS piping in the Annulus

The annulus flooding event contribution to the risk is reduced by closure of the FWDS header isolation motor operated valves (MOV), significantly reducing the flooding sources capacity in the annulus.

### 19.1.4 Safety Insights from the Internal Events PRA for Operations at Power

A summary of the U.S. EPR design features that play an important role in the risk reduction, general PRA assumptions including initiating events, SSC, common cause failures, human actions, internal and external hazards, and important PRA based insights are found in the following tables:

- Table 19.1-102—U.S. EPR Design Features Contributing to Low Risk.
- Table 19.1-108—U.S. EPR PRA Based Insights.
- Table 19.1-109—U.S. EPR PRA General Assumptions.
- Table 19.1-131—Key Uncertainties Identified in the U.S. EPR PRA.

#### 19.1.4.1 Level 1 Internal Events PRA for Operations at Power

##### 19.1.4.1.1 Description of the Level 1 PRA for Operations at Power

###### 19.1.4.1.1.1 Methodology

The Level 1 U.S. EPR PRA uses the linked fault-tree approach, supported by moderate size event trees. The major steps of the methodology are defined below:

- Identification of potential accident sequence initiating events:
  - Plant initiating events are identified based on previous industry experience, supplemented with a system failure modes and effects analysis (FMEA) which is focused on the identification of plant-specific initiators.
  - Plant initiating events with similar accident mitigation requirements are grouped together.
  - The annual frequency is estimated for each initiating event or initiating event group.
- Accident sequence analysis:
  - An evaluation of the plant response is developed for each type of initiating event, by identifying the key safety functions that are necessary to reach a safe and stable state and prevent core damage.
  - Systems and operator actions that affect the key safety functions are identified.

- Event trees are developed as a graphical representation of the potential core-damage sequences for each initiating event. The top functional events in these event trees reflect failures of the systems and operator actions required to mitigate these initiating events.

- Success criteria are developed for each key safety function considered in the plant event trees. For each event tree top functional event, the minimum set of components/trains required in order for the system to adequately perform its accident mitigation function is identified.

- System analysis:

  - For each system considered in the accident sequence event trees, a fault tree is constructed to allow for quantification of the system unavailability to perform the required accident mitigation function.

  - The system fault trees identify all the various combinations of equipment failures that may result in failure of system function. Intra-system dependencies and CCFs of components are considered.

  - Fault trees are constructed for the systems represented in the top functional events in the event trees (the front-line systems) and various systems needed to support these systems (support systems). Inter-system dependencies are explicitly considered.

- Data analysis:

  - Available generic data sources are compiled and reviewed to allow for selection of the failure parameters associated with components modeled in the system fault trees.

  - CCF parameters are also considered for groups of components with similar design, environmental and service conditions.

- Human reliability analysis:

  - Human actions that are required for different accident sequences modeled in the PRA are identified (post-initiator HRA).

  - Human actions that, if not completed correctly, may impact the availability of equipment necessary to perform system function modeled in the PRA are identified (pre-initiator HRA).

  - Human recovery actions are considered in the cases where it could be demonstrated that the action is plausible and feasible.

  - Acceptable methods are applied to estimate the probabilities of failure for the human actions. Estimates of probabilities of failure consider dependency on prior human failures in the scenario.

- Quantification:

- Fault trees and event trees are solved in an integrated fashion to produce CDF and to support quantification of LRF.
- Quantification is performed by using the PRA Software RiskSpectrum®, and it accounts for its features and limitations.
- The quantification results are reviewed and significant contributors to CDF, such as initiating events, CDF cutsets, basic events (equipment unavailabilities and human failure events) are identified.
- Uncertainty in the results is characterized. Key sources of model uncertainty and key assumptions are identified. Their potential impact on the results is assessed by performing a sensitivity analysis.

Each of these elements is described in the sections to follow.

#### 19.1.4.1.1.2 Accident Sequence Analysis

As discussed previously, the accident sequence analysis includes the identification of potential initiating events; evaluation of the plant response to these initiators; the definition of success criteria for systems and operator actions that are needed to reach a safe, stable state and prevent core damage. This accident analysis is represented graphically in event trees, which are developed to delineate the accident sequences that could lead to core damage, for each modeled initiating event. This process is discussed in this section.

##### Identification of Initiating Events

The systematic identification of events that could initiate an accident sequence is an essential first step in assessing the potential for core damage. The identification of initiating events includes the following steps:

- Identifying a set of events that could cause a disturbance in the plant operating conditions resulting in a demand for a reactor trip.
- Grouping these initiating events based on similarities in plant mitigation requirements, including the demands placed on systems and the operator actions needed to achieve a safe, stable condition, and prevent core damage.
- Estimating the annual frequency of occurrence for each initiator or initiator group.

To develop a comprehensive list of initiating events that is relevant for the U.S. EPR during power operation, the following process was used:

- Available sources were reviewed to identify potential initiating events. These sources included NUREG/CR-5750 (Reference 13), the Advanced Light Water Reactor (ALWR) Utility Requirements Document (Reference 14) and safety analyses for the U.S. EPR. An example of this process is provided in Table 19.1-3—Example Review of Initiating Events for Applicability to U.S. EPR.

- The U.S. EPR systems were evaluated using an FMEA approach to identify plant-specific system failures and their impacts on plant operation.

- Initiators due to pipe breaks (e.g., LOCAs, SGTRs, and secondary line breaks) were evaluated and are included in the list of initiating events.

- A systematic evaluation of potential LOCAs outside containment was conducted, from a plant-specific perspective, and applicable events were included as initiating events.

Internal initiating events selected for analysis were grouped into the following categories for presentation purposes:

- Plant Transients.

- LOCAs.

- Interfacing systems LOCAs (LOCAs outside containment)

- SGTRs.

- Secondary side breaks (steam line and feed line).

- Support system failures (including LOOP).

The initiating events are summarized in Table 19.1-4—Summary of Initiating Events for the U.S. EPR PRA.

Transient initiating events are combined into broad categories based on the availability of balance of plant (BOP) systems credited in the accident sequence analysis (e.g., the main feedwater system (MFWS), the condenser, and the startup and shutdown system). Other initiating events listed in the table were identified through the process outlined previously. The transient initiators are summarized below:

- General Transient (GT) – This category includes events that result in automatic or manual reactor trips, but do not result in the direct unavailability of BOP equipment to provide secondary cooling after the plant trip. Typical events in this category include turbine trip, manual trip, loss of RCS flow, rod drop, and partial loss of or excessive feedwater.

- Loss of Condenser Heat Sink (LOC) – This category includes transient initiating events resulting in the unavailability of the main condenser as a heat sink. Typical events in this category include inadvertent closure of all main steam isolation valves (MSIV) and a loss of condenser vacuum.

- Loss of Main Feed Water (LOMFW) – This category includes a complete loss of all main feedwater (MFW) flow. Typical events in this category include loss of feedwater (FW) from various causes (e.g., low suction pressure, closure of all FW control valves prior to the trip, or loss of MFW support systems).

LOCA initiating events inside containment account for losses of RCS inventory at rates beyond the make-up capability of the charging system. LOCAs are grouped into three size categories–small LOCA (SLOCA), medium LOCA (MLOCA), and large LOCA (LLOCA)) based on the requirements for secondary cooling and inventory make-up, as summarized below:

- For SLOCA size (0.6 to 3 inches in diameter):
  - Heat removal via SGs is required for full mission time (24 hours).
  - RCS make-up requires one train of MHSI with PCD of RCS, or one train of LHSI with fast cooldown (FCD) of RCS.
- For MLOCA size (3 to 6 inches in diameter):
  - Heat removal via SGs is required only for the duration of initial inventory in SGs (steam removal required only).
  - RCS make-up requires one train of MHSI with partial cooldown of RCS, or one train of LHSI with fast cooldown of RCS.
- For LLOCA size (> 6 inches in diameter):
  - Heat removal via SGs is not required.
  - RCS make-up requires one train of LHSI and two accumulator injections, or one train of LHSI and MHSI and a single accumulator injection.

In addition to LOCAs due to pipe breaks, the following LOCAs were considered:

- RCP seal LOCAs: RCP seal failures are not modeled as an initiating event. Since RCP seal LOCAs can be automatically or manually isolated, they were judged to be insignificant contributors to the SLOCA initiating event frequency. However, failures of RCP seals due to a loss of seal cooling, and failure to isolate, are specifically modeled in the accident sequence analysis.
- Pressurizer safety valve (PSV) LOCAs are included in the small LOCA initiating event frequency. The U.S. EPR PSVs can be manually actuated. There are two solenoids in series (two of two are required to open the valve) that open the valve by manual action. Each solenoid is powered by separate non-interruptible vital buses and the PSV closes upon loss of power.

*Interfacing System Loss of Coolant*

Interfacing system loss of coolant accidents (ISLOCA) or LOCA outside containment initiating events are postulated losses of RCS inventory through interfacing system piping that extend outside of the containment. For the U.S. EPR, an interfacing system is any fluid system that is directly connected to the RCS and has the potential to be exposed to RCS pressure through the failure or misalignment of normally closed

valves or through failure of heat exchanger tubes. The scope of the ISLOCA evaluation includes 0.6-inch diameter pipes and larger. The approximate maximum RCS flow rate from a postulated 0.6-inch diameter (or smaller) break is not expected to exceed the make-up capacity of the chemical and volume control system (CVCS). Several industry studies including NUREG/CR-5744 (Reference 15) and EPRI-NSAC-154 (Reference 16) have concluded that ISLOCA events within the capacity of the charging system are not significant contributors to the ISLOCA CDF. However, the U.S. EPR ISLOCA evaluation conservatively considers the possibility that multiple tubes could fail at an RCS heat exchanger interface, resulting in primary leakage in excess of the charging system capacity.

Containment penetrations are reviewed to identify where an RCS connection could cause a significant ISLOCA outside containment. Penetrations are screened out if it is judged that they cannot result in an event challenging the safe shutdown of the plant. For instance, pathways are screened out if:

- The associated piping penetration diameter is 0.6 in. or less (see discussion above).
- The system does not have a direct connection to the RCS (e.g., sump system).
- The system is isolated from the RCS and is designed for RCS pressure.

Once this screen is performed, pathways are retained for further evaluation affecting three systems:

- Safety Injection System (LHSI, MHSI discharge lines, RHR suction line).
- CVCS System (charging line, letdown line).
- CCW System (high pressure cooler, RCP thermal barrier cooling coils).

For each of the pathways identified above, an ISLOCA frequency is calculated based on the frequency of the triggering event (e.g., valve rupture), and the failure probability of the isolation (manual and/or automatic). Pipe rupture probability for a low pressure system exposed to RCS pressure is assumed to be 1 (guaranteed failure).

The frequency of core damage for each postulated ISLOCA event is estimated as the product of two factors:

- The ISLOCA initiating event frequency for each ISLOCA pathway.
- The probability that the ISLOCA event cannot be successfully mitigated. For large ISLOCA events (e.g., RHR suction line break), this probability is conservatively assumed to be 1 (guaranteed core damage). For smaller ISLOCAs, such as heat exchanger tube breaks, accident mitigation can be achieved by depressurizing the RCS and aligning RHR cooling.

*Steam Generator Tube Rupture*

SGTR initiating events are defined as failures of SG tubes resulting in primary coolant leakage into the secondary side of the SG. These events are similar to SLOCA events, except there are no containment indications of the event and that the leak can be terminated if the ruptured SG is isolated and RCS pressure is maintained at a pressure below the relief setpoints of the secondary valves on the ruptured SG. However, if the ruptured SG is not isolated, or if RCS pressure is not maintained below the MSSV/ MSRT setpoint on the ruptured SG, RCS leakage could escape to the environment. The U.S. EPR SGTR mitigating strategy is based on having the MHSI shutoff head at a value below the lift setpoints on the secondary valves on the ruptured SG. The SGTR event is conservatively assumed to be a single double-ended tube rupture, although most historical SGTR events have been significantly less severe. The smaller leaks allow more time for operator response. Failure of more than one tube can be postulated. However, the analysis assumption that all SGTR initiators involve a double-ended break of a single tube is judged to result in a conservative estimate of the SGTR risk.

*Induced Steam Generator Tube Rupture*

Induced SGTRs are considered in the U.S. EPR as a separate initiating event. SGTRs can occur for initiating events that cause a large change in the pressure differential across the SG tubes, such as for main steam line breaks and main feed line breaks. The primary concern is with steam-line breaks outside of containment, as these events can result in a loss of RCS inventory outside containment if the RCS is not depressurized, whereas a break inside containment results in a loss of RCS inventory inside containment and behaves similarly to a LOCA event, with a much lower initiating event frequency. The induced SGTR initiating event frequency was estimated based on the NUREG/CR-6365 (Reference 17) methodology with consideration given to advances in materials technology (alloy 690), and consideration given to advances in degradation monitoring.

*Secondary Line Break*

Secondary line break initiating events include those secondary line breaks that are large enough to initiate secondary side isolation and safety injection actuation. The initiating events considered are discussed below:

- Steam line breaks can occur upstream or downstream of the MSIVs. Steam line breaks inside containment (SLBI) (i.e., breaks occurring upstream of the MSIVs) cannot be isolated. A break at this location assumes that at least one SG will always blow down. These breaks are modeled as inside containment breaks. Steam line breaks outside containment (SLBO) (i.e., breaks occurring downstream of the MSIVs) can be isolated, and are modeled as outside containment breaks. Spurious operation of an MSSV is also modeled.

- FW line breaks inside containment (FLBI) on the SG side of the containment isolation (CI) check valve are not isolable (i.e., at least one SG always blows down). FLBI and SLBI are currently considered as a single initiator, because the success criteria and required mitigating systems are similar. FW line breaks outside containment, and other feed line breaks that do not directly result in a loss of any SG inventory, are treated as a total loss of FW initiating events.

- The U.S. EPR PRA considers the inadvertent opening of an MSSV or an MSRIV as a potential initiating event. It is judged that spurious operation of an MSSV is much more likely than spurious operation of an MSRIV. Two solenoids need to spuriously operate to open the MSRIV. Each solenoid is powered from a separate power supply and the MSRIVs fail closed upon loss of either power supply. The normally open main steam relief control valves (MSRCV) in series with the MSRIV can be closed to isolate a spuriously open MSRIV. Additionally, these series valves also receive isolation signals on low steam-generator pressure.

*Support System Initiating Events*

- Loss of CCW/ESW – The CCW system provides cooling to the RCPs, the CVCS pumps, and the SIS pumps. Therefore, loss of component cooling has the potential to cause a reactor trip and to degrade systems required for safe shutdown. Each CCW system train has its own dedicated ESW train to remove heat to the environment, and the CCW system initiating event analysis incorporates applicable ESW failure modes as appropriate. Losses of one or two CCW common headers are considered as the initiator, which could occur as a result of multiple failure combinations (e.g., spurious operation of one of the CCW header relief valves or a failure of the running CCW/ESW train and failure of automated switchover to the standby train).

  Loss of an Ultimate Heat Sink (UHS) is also included in this initiator.

- Loss of Balance of Plant (LBOP) – The closed cooling water system removes the heat generated by components in the conventional part of the plant via the closed cooling water heat exchangers to the circulating water system or the auxiliary cooling water system. Complete loss of the closed cooling water system will result in a turbine trip and reactor trip. MFW and the startup and shutdown systems (SSS) are assumed to be unavailable because of a loss of cooling.

- Loss of Offsite Power – The LOOP event dramatically affects plant operations, because not only does it result in a unit trip, but also it affects mitigation response by placing demands on the onsite power system. Recovery of offsite power is considered for transient events in two hours and for the RCP seal LOCA events in one hour. Possible recovery for other times is not explicitly credited. Consequential LOOP is also considered. It is assumed that the consequential LOOP probability would be different between plant trips, LOCA events and events likely to lead to a controlled shutdown. A LOOP during a mission time of 24 hours is also considered.

- Loss of an Electrical Bus – Loss of a single switchgear (SWGR) is conservatively included in the accident sequence model as an initiating event to bound electrical

failures and to demonstrate that the risk from a loss of one safety train is relatively low.

- Loss of Heating, Ventilation and Air Conditioning (HVAC) – Initiating events due to a loss of HVAC to the SWGR rooms or the main control room (MCR) are not explicitly modeled. In the design certification phase, HVAC recovery procedures and guidelines are not available and any realistic estimates of HVAC recovery times are expected to be site specific. These events are assumed to have similar effects as for the loss of single division initiator, or the fires in the SWGR rooms, or the MCR. Losses of the HVAC system during a 24-hour mission time are explicitly modeled. (Recovery times were estimated based on the safeguard building heat loads.)

*Anticipated Transient Without Scram (ATWS)*

ATWS events are considered as a potential cause of core damage events. Reactor trip failure can result from three major causes:

- Failure of the reactor trip signal.
- Failure of the reactor trip devices.
- Mechanical binding of the control rods.

Each of these failure modes is considered in the accident sequence modeling.

Given that an ATWS event occurs, the primary functions required to mitigate it are:

- Primary system overpressure protection.
- Long-term shutdown.
- Adequate primary to secondary heat removal.

Each of these functions is considered in the ATWS event tree modeling.

### Assessment of Plant Response

An understanding of plant response is essential to the sequence development process. This understanding was gained through consideration of the system requirements following each category of initiating event. The process was based on available accident analyses. Event sequence diagrams (ESD) were developed to aid in modeling plant response, and in documenting the process. These ESDs served as a major input to the development of the core damage event trees.

### Definition of Success Criteria

To constitute a success end state for the Level 1 PRA model, each accident sequence must result in a safe, stable state for 24 hours. This period (24 hours) is applied as the

mission time for operation of most equipment. Two different considerations for the mission time are discussed below:

1. Given that only two times for a LOOP recovery are credited in the analysis (for transient events in two hours and for RCP seal LOCA events in one hour), possible later LOOP recoveries are partially credited through modification of the EDG running mission time, which was reduced to 12 hours. Since the recovery time to restore offsite power is not two hours from the time of the LOOP (as assumed in the event tree model), but rather two hours from the time of the last EDG failure the LOOP CDF is significantly over-estimated if an EDG mission time of 24 hours is applied, and the conservatism is reduced by applying a 12 hour mission time. The station blackout diesel generator (SBODG) mission time was not modified.

2. Mission times longer than 24 hours are not considered in the Level 1 PRA. Two sensitivity cases were selected to check the risk impacts of selecting different mission times for long term IRWST cooling by SAHR (36 and 72 hours - see Section 19.1.4.1.2.6).

In specifying system and function success criteria, core damage is defined as uncovering of the core, leading to heat-up of the fuel in the reactor to the point at which prolonged oxidation and severe damage to a large fraction of the fuel is expected. For most transient and LOCA events, core damage is further defined to occur if the peak cladding temperature exceeds 2200°F. For ATWS scenarios, an additional acceptance criterion was applied in that core damage was assumed to result if the RCS pressure exceeded 130 percent of the design pressure.

The thermal/hydraulic and other supporting engineering evaluations were performed to determine the accident progression parameters (e.g., timing, temperature, pressure) that potentially determine the requirement for mitigating systems and affect their operability. These analyses also determine timings and the requirement for operator actions. Computer codes MAAP4 (version 4.07) and S-RELAP5 are used to determine and justify success criteria for the at-power PRA. These computer codes are described further in Section 19.1.4.1.1.7.

### Development of Core-Damage Event Trees

The information compiled through an evaluation of plant response and definition of success criteria is used to construct event trees. These event trees graphically illustrate the combinations of successes and failures of systems and operator actions that lead to accident sequences. The basic end states for these sequences are as follows:

- Success—A controlled stable state with the reactor subcritical, sufficient inventory in the RCS to support core heat removal, and adequate heat removal from the core and RCS.

- Core Damage—This particular end state is reached when success cannot be established and maintained as described above.

In the construction of the event trees, for each modeled initiating event, every system and operator action required for each key safety function are explicitly included. Three key safety functions, that need to be satisfied in order to reach a success state, are described below:

- The reactivity control function ensures that the reactor is tripped in order to reduce heat generation. The reactor trip system is highly reliable with numerous diverse and redundant input signals. Reactor trip system failure or an ATWS does not guarantee core damage, because the boron injection can be used to reach a stable state. The ATWS event sequence analysis describes the mitigating systems and their success criteria.

- The inventory control function ensures that heat is removed from the fuel rods by the reactor coolant. This function can be challenged in a number of ways, including a LOCA initiating event, or because of system failures after the initiating event (e.g., RCP seal LOCA). The safety injection system is needed to provide inventory control and remove heat from the fuel to the IRWST. A safety injection signal is generated on low pressurizer pressure. The inventory control function could also be challenged if the secondary heat removal function is lost when the operators initiate primary feed and bleed (F&B) by opening the PSVs. The following systems can provide inventory make-up to the reactor vessel: MHSI, LHSI, Accumulators, CVCS and EBS. MHSI, LHSI and Accumulators are credited to mitigate LOCA events and to support feed and bleed function. For certain initiating events and accident sequences, inventory control is dependent on the secondary heat removal function described below. For example, MHSI pump injection during an SLOCA requires an SG partial cooldown. This is automatically initiated by an SI actuation signal. If all four MHSI trains fail, operator actions would be required to initiate fast cooldown to allow LHSI injection.

- The heat removal function ensures that the heat from the reactor coolant is removed and transferred to the environment. Heat removal requirements depend on the initiating event and the accident sequence. Secondary cooling with the SGs is sufficient for transients or events where RCS integrity is maintained (no LOCA condition). This can be satisfied with one main Feedwater (MFW) pump, or SSS pump, or one EFW pump supplying one SG with steam relief to the main condenser through the Main Steam Bypass (MSB), or to the atmosphere through an MSRV or MSSV (two per SG). If secondary cooling is unsuccessful, the operators initiate primary feed and bleed cooling. Primary bleed (PBL) is initiated through the PSVs or severe accident depressurization valves (SADV), and feed is provided by a safety injection train. The heat transferred to primary containment is removed by IRWST cooling. LHSI trains with heat exchangers or the severe accident heat removal system (SAHR) provide the IRWST heat removal function.

The event trees are provided in Appendix 19A.

#### 19.1.4.1.1.3 Systems Analysis

The event sequences are defined based on the successes and failures of plant mitigating systems. The failures of these systems are evaluated through the development of

detailed fault trees. The level of detail to which the fault trees were developed is consistent with that for comparable analyses for operating nuclear power plants. In some cases, specific design details are not available at the design certification stage. In these cases, if development of the fault trees was affected (e.g., if bounding assumptions had to be made), the treatment is documented in a detailed report.

The fault trees are integrated in two ways:

- Top events for system failures that include a core damage sequence are combined under AND logic, to perform the linking necessary for the quantification process.
- Connections to support systems are modeled in the fault trees, such that common dependencies among the various systems credited in the accident sequence analysis are accounted for in the quantification.

The systems for which detailed fault trees were developed are summarized in Table 19.1-5—Systems Analyzed in U.S. EPR PRA.

A brief description of the major U.S. EPR frontline systems and support systems that are modeled in the PRA is provided below. The differences between the designs of the digital I&C systems for the U.S. EPR and that of the I&C systems for currently operating plants are generally greater than they are for other systems. Therefore, a more detailed discussion of the design of the digital I&C system, and the manner in which it is treated in the U.S. EPR PRA, is provided in a separate section that follows. A discussion of system dependencies and their modeling is also provided.

Failure events and failure modes were screened from the PRA where they met the criteria described in supporting requirement SY-A14 of the ASME PRA Standard. Contributors to the unreliability or unavailability may be excluded if:

- The total failure probability of the failure mode results in the same effect on system operation and is at least two orders of magnitude lower than the highest failure probability of other components in the same train that have the same effect on system operation.
- The contribution of the failure mode to the failure rate or probability is less than one percent of the total failure rate for the component and the effect on system operation is the same.

### Modeling of Inventory Control Systems

#### *Medium Head Safety Injection System*

The MHSI PRA-credited function is to provide RCS inventory make-up to ensure adequate core heat transfer for events that result in a loss of RCS inventory. The MHSI consists of four 100-percent capacity, independent trains that are physically separated and protected within their respective Safeguard Buildings (SB). MHSI takes suction

from the IRWST. The MHSI pumps have a design shutoff pressure of approximately 1400 psig. For certain initiating events and accident sequences involving RCS pressure above MHSI shutoff pressure, MHSI is dependent on the secondary heat removal function via the SGs and MSRTs for RCS depressurization. The PCD signal is automatically initiated by an SIS signal.

*Low Head Safety Injection/Residual Heat Removal System*

The LHSI/RHR PRA-credited functions are to provide RCS inventory make-up to ensure adequate core heat transfer for events that result in low RCS level/inventory. The PRA also credits LHSI/RHR to remove core decay heat during accidents and in support of LPSD conditions. LHSI consists of four 100 percent capacity, independent trains that are physically separated from each other and protected within the respective SB. The trains can be cross-tied during preventive maintenance on one train. Divisional CCW/ESW trains remove heat from LHSI/RHR heat exchangers. The LHSI takes suction from the IRWST.

*Accumulators*

The PRA-credited function of the accumulators is to inject water into the RCS for loss of inventory events. There are four accumulators (one for each cold leg) that automatically inject their contents when RCS pressure is below approximately 600 psig.

*In-Containment Refueling Water Storage Tank*

The PRA-credited function of the IRWST is to provide a source of borated water for MHSI and LHSI in the event of loss of RCS inventory and for containment heat removal and core melt cooling in the event of a severe accident. The IRWST is a single tank, integral to the containment structure. The IRWST represents the lowest point in the containment and any water discharged from the RCS will drain back into the IRWST. The IRWST eliminates the need to actively transfer MHSI/LHSI pump suction to the containment sump for long-term recirculation. In order to retain debris that could originate from a LOCA and clog the SIS suctions from the IRWST, three levels of filters are provided: the trash racks retain the largest debris before they reach the IRWST, while the retaining baskets stop smaller debris at the IRWST inlets. Trash racks and baskets are arranged so that water would continue to flow into the IRWST even if they are clogged. The third level of retention is provided by six strainers arranged above each of the four SIS, SAHR and CVCS pump suctions. Common-cause failure of plugging the six strainers is evaluated in the PRA, even though it is unlikely because of the additional protection described here.

*Extra Borating System*

The EBS consists of two pumps with high head capacity. The PRA-credited EBS function is to provide emergency boration of the RCS during those events that require negative reactivity insertion. The EBS pumps are located in the Fuel Building.

*Chemical and Volume Control System*

The CVCS consists of two pumps with high head capacity. The CVCS PRA-credited function is to provide RCP seal injection. The CVCS pumps are located in the Fuel Building.

*RCP Stand Still Seal System*

In addition to the normal multi-stage RCP shaft seal, each RCP is equipped with a SSSS to provide backup seal capability. The stand still seal system is deployed pneumatically when the associated RCP shaft stops rotating. This added seal protection reduces the likelihood of an RCP seal LOCA-type event during scenarios caused by simultaneous loss of seal support systems, for example loss of barrier cooling (i.e., CCW) and seal injection (i.e., CVCS).

**Modeling of Heat Removal Systems**

*Main Feedwater System*

The MFW PRA-credited function is to provide SG inventory make-up for those events that require secondary heat removal via the SGs. The MFW is equipped with four electric, motor-driven, main feedwater pumps, which take suction from the feedwater tank. Each MFW pump is capable of handling approximately 33 percent of the full power load. The MFW system is located in the Turbine Building.

*Startup and Shutdown Feedwater System*

The SSS PRA-credited function is to provide SG inventory make-up for those events that require secondary heat removal via the SGs including support of the RCS partial cooldown and fast cooldown functions. The SSS consists of a single electric motor-driven pump, which takes suction from the feedwater tank. The SSS pump discharges to the SGs via main feedwater piping. The SSS is located in the Turbine Building.

*Emergency Feedwater System*

The EFW system PRA-credited function is to provide SG inventory make-up for those events that require secondary heat removal via the SGs including the RCS partial cooldown and fast cooldown functions. Each SG has a dedicated EFW train for maintaining SG level. Each EFW train consists of an electric motor-driven pump with a dedicated suction tank. The EFW pump suctions are interconnected via normally

closed manual valves and the EFW pump discharge lines are interconnected via normally closed MOVs so that any EFW train can be connected to any SG. In many accidents, inventory of all four EFW tanks may be needed to cool the plant during a mission time of 24 hours and an operator action is needed to manually crosstie these tanks. EFW discharge to the SGs is independent of the MFW and SSS piping. The EFW trains are physically separated and protected within their respective Safeguard Buildings.

*Main Steam System*

The main steam system (MSS) PRA-credited function is to provide secondary heat removal by discharging steam to the main condenser or to the atmosphere via the MSRTs or the MSSVs. Each SG is equipped with one MSRT and two MSSVs, which discharge to the atmosphere. In LOCA-type accidents, the MSRTs are credited in the PRA to perform the RCS PCD and FCD functions to support the MHSI and LHSI functions. SG isolation is also a PRA function that is modeled for SG tube rupture events and secondary side breaks.

*Pressurizer Relief System*

The RCS pressurizer relief system functions credited in the PRA are to protect the RCS from overpressure events, reduce RCS pressure in support of feed and bleed operations, and perform RCS depressurization during a severe accident to prevent RCS failure at high pressure. The U.S. EPR is equipped with three PSVs and two primary depressurization system lines. The primary depressurization system lines consist of two parallel trains, each line having two PDSVs in series.

*Severe Accident Heat Removal System*

The SAHRS PRA-credited functions are to provide cooling of the IRWST water as a backup to LHSI/RHR during accident conditions and to provide heat removal/spray of the containment space to prevent containment overpressure. The SAHRS is a dedicated containment heat removal system and consists of one 100 percent capacity train, which takes suction from the IRWST. The SAHR discharge depends on the primary operating modes, which could be one of the following:

- Passive cooling of molten core debris.
- Active spray for environmental control of the containment atmosphere.
- Active recirculation cooling of the molten core debris.
- Active recirculation cooling of the containment atmosphere.
- Active back-flush of IRWST strainers.

The SAHRS heat exchanger transfers the heat from the containment to the UHS via a dedicated CCW and ESW train. The SAHRS train is located in SB 4.

### Modeling of Support Systems

#### *Alternating Current Electrical Distribution System*

The alternating current (AC) electrical distribution system PRA-credited function is to provide AC electrical power to the frontline and support systems from both offsite and onsite power sources, through the distribution system consisting of switchgear busses, motor control centers, and uninterruptible power supplies. There are four independent AC electrical divisions that support the safety train divisions. Each division is located within a separate SB.

#### *Direct Current Electrical Distribution System*

The direct current (DC) electrical distribution system PRA-credited function is to provide divisional DC electrical power to the frontline and support systems from the associated division's DC battery. Each safety train division is equipped with a dedicated, Class 1E battery with redundant battery chargers. The divisional batteries are designed for a discharge of two hours based on the necessary loading of the batteries. The U.S. EPR design also includes a separate non-class 1E uninterruptible power supply (UPS) system for severe accident management. This system consists of redundant batteries designed for twelve hour discharge.

#### *Emergency Diesel Generators*

The EDGs PRA-credited function is for each EDG to independently provide onsite AC electrical power to its associated electrical division should the normal offsite power source become unavailable. There are four 100 percent capacity EDGs. Each EDG is dedicated to an electrical division. The EDGs are located in two separate Emergency Power Generation Buildings (EPGB), which are spatially separated on the plant site. The EDGs are also physically separated within the EPGBs.

#### *Station Blackout Diesel Generators*

The SBO diesel generators PRA-credited function is for each SBO diesel generator to provide backup AC electrical power to its associated electrical division, independent and diverse from the divisional EDG. The U.S. EPR design has two SBO diesels generators to supply power to plant loads in the unlikely event of a LOOP with failure of all four EDGs (SBO-type event). The SBO diesels are associated with train Divisions 1 and 4 and are auto started and manually connected and loaded from the control room. The SBO diesels are independent and diverse of the EDGs based on consideration of attributes (e.g., different model, control power, HVAC, engine

cooling, fuel system, location). The SBO diesels are located in the Switchgear Building.

*Essential Service Water System / Ultimate Heat Sink*

The ESW system PRA-credited function is to remove reactor heat and heat generated by equipment and components during normal operating conditions, transients and accidents. ESW supplies water to the component cooling water system (CCWS) heat exchangers and consists of four independent trains. Each UHS train configuration consists of the divisional ESW pump, a two-cell mechanical draft cooling tower with basin and fans and associated instrumentation, and isolation valves. Train 4 basin and cooling fans support the dedicated cooling train to the SAHRS.

*Component Cooling Water System*

The CCW System PRA-credited function is to remove reactor heat and heat generated by equipment and components by circulating water through the various heat loads and the CCW heat exchangers to transfer heat to ESWS. CCW consists of four trains located within the associated Safeguard Building. The system is further discussed in the system dependency section.

*Safeguard Buildings HVAC Systems*

The Safeguard Building ventilation system PRA-credited function is to remove heat generated by operation of equipment and components. The system is cooled via the SCWS. The system is further discussed in the system dependency section.

*Safety Chilled Water System*

The SCWS PRA-credited function is to remove heat generated by equipment and components and Safeguard Building ventilation systems. Two divisions of safety chilled water are cooled via the CCW system and two divisions are air cooled. The SCWS trains are located in the SBs. The system is further discussed in the system dependency section.

**Modeling of Digital I&C Systems**

Because the digital I&C system for the U.S. EPR design is somewhat unique relative to systems in current plants, additional discussion of the modeling in the PRA is provided here. This addresses the manner in which system faults are reflected in the models; the sources of reliability data used; and the treatment of common-cause failures, both of software and of hardware.

Of the various I&C systems, the PS is the most important to the PRA and is modeled in detail. The PS functions include automatic initiation of reactor trip and actuation of engineered safety features (ESF).

There are other I&C systems that are not modeled in detail in the PRA. This includes the SAS, which controls certain safety-related support systems, such as CCW and ventilation, and the PAS, which controls non-safety-related systems. For the SAS and PAS, simple, high-level models and conservative failure rates are used in the PRA (i.e., undeveloped events) for design certification. To capture dependencies, the undeveloped events are combined with power supplies and sensor inputs that could be shared with the PS.

Another I&C system that is modeled with an undeveloped event is the diverse actuation system (DAS), which performs some backup reactor trips for ATWS mitigation. The DAS also contains some backup functions for ESF actuation that are included in the design for diversity and defense in depth (D3). These functions, which involve implementation using technology that is diverse from the PS, provide additional reliability and diversity for reactor trip and ESF functions. DAS is included in the PRA model with a beta factor to account for potential software CCF with the analogous PS functions. The D3 functions are described in Technical Report ANP-10304 (Reference 58) and in Section 7.8.

The PS has four-division redundancy, which contributes to its high reliability. Each of the four PS divisions is further separated into two independent subsystems to allow implementation of functional diversity. For initiating events that require reactor trip, the primary trip signal and backup trip signals are assigned to opposite subsystems. For ESF actuation, the functions (e.g., EFW and SIS actuation) are distributed into the two subsystems, and this also provides a measure of functional diversity that increases the system reliability.

The PS is modeled to the level of detail of the rack mounted TELEPERM XS (TXS) modules. This level of detail is sufficient to resolve dependencies related to shared equipment (e.g., computer processors and I/O modules that perform multiple functions) and also corresponds to the availability of failure data from the worldwide TXS operating experience. Key PS components include computer-processor modules, I/O modules, signal-conditioning modules, communication modules, priority modules, subracks and power supplies, and a multitude of sensors.

The failure rates for the TXS components are derived from operating history. The TXS system is a proven design with over 14 years of operating history in reactor protection systems (RPS) and ESF actuation systems (ESFAS) in various European plants. The failure rates for the TXS components are obtained from field data and are calculated using the chi-squared distribution with a 95 percent confidence interval, and are also compared against theoretical (e.g., part stress) estimates. Due to the conservative statistical treatment inherent in the chi-squared distribution, the calculated failure rates used in the PRA are conservative relative to the observed experience. The field data for the TXS components are updated on a periodic basis.

The TXS hardware and software used by the PS have extensive self-testing features and fault-tolerant design. These features improve the reliability of the system, and minimize the need for periodic surveillance testing. However, the PRA model assumes that a portion of the failure modes are not "covered" by the self-testing and fault tolerance. With input from manufacturers analysis, the PRA model separates these failure modes and uses the failure rate equations built into the RiskSpectrum® PRA software to calculate separate component basic event unavailability for the self-revealed and test-revealed portions. The "non-covered" failure modes, although they present the smaller percentage, are more important to the PRA results, because they have a long mean time to repair (MTTR) relative to the self-revealed failures and a less favorable impact on the (fault tolerant) coincidence logic.

The PS PRA model includes two categories of software common cause failure (SWCCF): CCF of the TXS operating system (OS) software, and CCF of the application software. The OS CCF includes software that is common to the system including the OS itself and support software such as functional blocks. CCF of the OS is a hypothetical failure that is assumed to cause catastrophic failure of all of the PS computers. The application software CCF includes failures related to application-specific defects in functional specifications, analytical knowledge, or implementation. CCF of the application software is assumed to effect software functions or groups of related software functions that are common to redundant computer processors and share identical algorithms, sensor inputs, and signal trajectories.

Since there is uncertainty in SWCCF estimates, it is important to understand the design features that influence it. The OS design and the application software development are both significant parts of the TXS platform's defense against CCF. The quality of the software development life-cycle process is significant in preventing defects in the application software. TXS is a mature safety I&C platform with a well-structured and controlled application software development process. The TXS platform design includes software development tools to automate application software development and reduce the likelihood of human error. A verification and validation (V&V) process demonstrates that application program functional requirements are complete and correct, and that they are correctly implemented. There are also configuration control requirements for modification of the software after its initial installation.

Also significant for reducing SWCCF are the features of the OS software that reduce failure triggers. For example, application software defects can be triggered by unanticipated signal trajectories or data sets. Deterministic program execution and strictly cyclic processing are used in the TXS platform so there is only one path through the software instructions, and all of the application code is executed every cycle (i.e., the program always performs the same computations). Cyclic processing is executed with no process-driven interrupts, no real-time clock, no dynamic memory allocation, and strict measures against software exceptions (e.g., input data range

violations and not-a-number violations). This provides software execution on each processor that is independent of any input data trajectory or data-triggered interference (processor overload or software exception). These characteristics of the TXS design limit the opportunity for CCF due to untested software paths and data sets, and reduce the probability that postulated latent errors may be triggered to cause failure.

The OS design is also important for its capability to limit the impact of application SW failures, and prevent propagation of failures to redundant or diverse processing units. It is a fundamental objective of the OS design, that unanticipated application software failures would not cause failure of the OS, and, therefore, propagate to other functions. This is accomplished via features such as static memory allocation and asynchronous operation. These and other features provide separation between system software and application software and eliminate leading OS failure causes in the operating history of standard computer systems, such as failures due to memory conflicts and failures in releasing system resources.

Another leading cause of failure that plagues standard computer systems occurs when "special loading" overtaxes the OS capacity. These failures are eliminated in the TXS platform by constant bus loading (i.e., communication and processing buses). An important consequence of deterministic program execution and strictly cyclic operation is that the bus loading is constant by design and is unaffected by demands for system response. Unlike analog protection systems that sit in standby until demanded, the cyclic OS is always active, cycling many times per second, and always processing the same amount of data whether there is a demand or not. Consequently an actual system demand is no more stressful to the OS than any other cycle.

These features and others are discussed in EMF-2110(NP)(A) (Reference 54) (see also Section 7.1.1.2.1). As discussed in Reference 54, the TXS design features force a dissociation of the OS both from the application software and from external plant transients, which protects against event- or environment-related failure triggers of the OS software. This is significant with respect to the quantification of OS failure probability because it removes application-specific variability and demand-related stress from the OS reliability, and allows the OS portion of the failure probability to be calculated based upon the previous operating history.

The TXS operating history attests to the success of these features, and is used to generate a bounding value for the OS SWCCF probability. TXS I&C systems have been installed in 44 units at 28 plant sites located in 11 countries and utilizing 10 different reactor designs. TXS has broad operating experience in representative nuclear power plant applications directly applicable for use in the U.S. EPR design.

The computer processor modules have over 108 million operating hours of accumulated experience through calendar year 2009. During this time, there were

some random failures of the computer processor modules, and no OS failures. A Chi-squared distribution with 95 percent confidence level was used to provide an upper bound OS failure rate. The PRA makes the conservative assumption that the failure rate of a single OS represents a CCF of the computer processors in the PS system (i.e., beta-factor = 1.0). If there was a postulated OS CCF in the field (i.e., lockup of multiple computer processors in redundant channels), a Technical Specification LCO would be triggered with a short completion time (i.e., one hour). Allowing one hour for the downtime yields an unavailability that was rounded off to 1E-7 for use as the OS CCF probability.

For the application software, the CCF probabilities are assigned based upon subjective estimates. Subjective estimates are necessary because the software is application specific. In TXS, software customization is restricted to using only qualified software functional blocks from a controlled library. The function blocks represent easily understood functions, which are thoroughly verified and tested. The medium for communication of application-specific functional specifications are functional diagrams that are composed of these function blocks. The application software designer has no access to the programming within the functional blocks, and numeric and logical operations on signals are only performed within the function block modules. The function block diagram is readily understood by both the process engineers and the I&C engineers responsible for the application software. Since the same function blocks are used and tested in many applications, there is high confidence that they are error free. Nonetheless, the possibility of human error in specification, analytical knowledge or implementation cannot be eliminated, and it is difficult to quantify.

Therefore, the estimates for application software CCF are based on comparison of the TXS platform design characteristics and lifecycle processes for application software development with applicable international standards for digital systems of similar safety importance. The TXS design and processes are comparable to IEC-62340 (Reference 55) standards of good practice for defense against CCF, to IEC-60880 (Reference 56) standards of good practice for software, and to IEC-61508 (Reference 57) standards of good practice for safety integrity level four (SIL-4).

Reference 57 defines safety integrity level (SIL) as a relative level of risk reduction, which is assigned based on requirements in two broad categories: hardware safety integrity and systemic safety integrity (i.e., software). The TXS platform and RPS/ESFAS applications on TXS are designed according to a rigorous development process, which has proven to comply with SIL-4 requirements in previous I&C projects. Reference 57 also provides risk targets, which for a SIL-4 system correspond to a failure probability between 1E-4 and 1E-5 per demand. The risk target values were used as a general guide to assign a reasonable application software failure probability based on engineering judgment. Since the target values apply to the combined hardware and the software system, engineering judgment was used to allocate half of

the target range (between 5E-5 and 5E-6) to the software. Within this range, a value of 1E-5 was chosen for the application software failure probability in each of the diversity groups. The PRA makes the assumption of complete dependence between redundant channels of identical application software.

The defense against application software CCF relies not only on the quality of the software development life-cycle and an OS design that prevents failure triggers and propagation, but also upon functional diversity.

Functional diversity (such as provided by the A and B subsystems for reactor trip functions) protects against application software defects. The functions assigned to the two diversity groups have different functional specifications, different sensed parameters, and different signal trajectories. Reference 55 endorses functional diversity as an effective defense against application-specific software faults such as specification errors. By introducing different signal trajectories, function diversity also protects against common failure triggers.

In terms of the SWCCF in the PRA, the application software CCF probability addresses the vulnerability introduced in the application-specific input, such as functional diagrams and specifications. The OS CCF probability addresses potential vulnerability in the OS, function block programming, or other system software that is common to both diversity groups.

Additional diversity is provided by other I&C systems, and human diversity is provided by the operator. The complete diversity strategy employed by the U.S. EPR I&C design is described in Chapter 7. These multiple levels of defense are beneficial to the PRA, because they will reduce the significance of the uncertainty in the SWCCF estimates.

The PRA also includes credit for diverse automatic actuations that are required for D3. The D3 functions are backup automatic actuations that are intended to mitigate SWCCF. The D3 functions reduce the uncertainty associated with modeling of SWCCF, and the sensitivity of the PRA results to that uncertainty.

Hardware components of the PS are also assigned to CCF groups. CCF grouping is applied to the computer hardware, to reactor trip devices (i.e., breakers, contactors), and to the PS sensor inputs. CCF for hardware devices is generally modeled using the Beta Factor or MGL method.

A CCF probability is also included for mechanical failure of control rods. The probability for stuck control rod CCF is obtained from NUREG/CR-5500, Vol. 11, Reliability Study: Babcock & Wilcox Reactor Protection System (Reference 18). Reference 18 provides estimates for the control rod CCF probabilities for the existing PWR fleet. The B&W version of this report was used because, of the three PWR

vendors, the B&W design most closely resembles the U.S. EPR design in terms of total number of control rods and success criteria. The B&W design has a total of 69 identical control rods of which 61 trip and 41 are considered safety-related. The NUREG/CR-5500 calculates a probability of 4.1E-08/demand that 50 percent of the safety-related rods fail to insert, which corresponds to a CCF of approximately 20 rods. The U.S. EPR has 89 control rods, and analysis has shown that at least 38 control rods must fail to insert during a reactor trip before there is insufficient (less than one percent) shutdown margin. Therefore, the CCF probability from NUREG/CR-5500 is conservative for the U.S. EPR design.

Fault tree top events for the ESF actuation signals are developed on a train and function-specific basis. This allows the PS fault trees to be linked with the frontline system fault trees at the train or component level of the system. In this way, the fault tree quantification resolves the hardware and software dependencies and properly accounts for the divisional redundancy and subsystem functional diversity. Key ESF functions include EFW actuation on low SG level, actuation of safety injection and PCD on low RCS (pressurizer) pressure, main steam isolation on low SG pressure, containment isolation on high pressure, and EDG starting and loading.

Fault trees for failure of the reactor trip function are developed for representative initiating events. Reactor trip fault trees specific to every initiating event are not developed because of the low probability associated with ATWS, and the extensive redundancy and diversity built into the U.S. EPR reactor trip design. ATWS is unlikely in this plant because of the diversity of reactor trip signals, the diversity in the reactor trip devices, and the abundance of control rods. Instead, representative reactor trips are modeled with a typical set of challenged parameters. This assumption is based on the PS being designed so that each postulated initiating event will challenge at least two different measured parameters for reactor trip that are implemented in the two PS subsystems. This is conservative because often there will be additional trips that the PRA could credit if the trips that are credited in the safety analysis were to fail. The representative reactor trip signals in the model include the most common trips (RCS pressure, SG pressure, SG level) as well as one of the more complex trips (low departure from nucleate boiling ratio).

As would be expected, the PS contribution to the PRA results is dominated by CCFs. The results are sensitive to the assumptions made for SWCCF, as well as CCF of computers and key sensors. These sensitivities are tempered somewhat by additional functions, which are incorporated into the DAS for D3.

### Modeling of System Dependencies

This section provides an overview of some of the important system dependencies accounted for in the PRA of the U.S. EPR. In most cases the U.S. EPR dependencies are as expected (e.g., Division 1 of the EFW system relies on Division 1 of alternating

current and direct current power) and these dependencies are not discussed in this section. Rather, this section focuses on dependencies that are either unique to the U.S. EPR design, or are non-intuitive in nature. This focus provides further background for reviewing and understanding the accident sequence results. The discussion focuses on dependencies associated with component cooling water, ventilation for the SBs, and power supplies for specific functions.

The cooling water dependencies discussed herein are illustrated in Figure 19.1-1—Cooling Water Dependencies Modeled in the U.S. EPR PRA, the ventilation dependencies are illustrated in Figure 19.1-2—Ventilation Dependencies Modeled in the U.S. EPR PRA, and the power dependencies discussed in this section are illustrated in Figure 19.1-3—Selected Dependencies on Electric Power Modeled in the U.S. EPR PRA.

### CCW Dependencies

CCW Trains are cooled by corresponding ESW trains, taking suction from corresponding UHS pools. CCW Trains 1 and 2 provide supply to CCW Common Header 1 (CH1). One train supplies the header while the other train is in standby. Switchover between trains is automatic, and so is isolation of the leaking train or the header.

CCW CH1 provides the following functions credited in the PRA model:

- Thermal barrier cooling for seals for all four RCPs, 50 percent of the time.
- Pump motor cooling and thermal barrier cooling for seals for RCPs 1 and 2.
- Cooling flow to the Train 2 SCWS (QKA20), which is credited in the PRA to provide cooling to SB 1 and 2 (assumed in standby).
- Cooling for charging pump Train 1 (assumed running).
- Cooling for two of the four operational chilled water chillers (which are credited in the PRA to provide cooling to the maintenance trains of the ventilation system).

CCW CH 2 provides the following functions credited in the PRA model:

- Thermal barrier cooling for seals for all four RCPs, 50 percent of the time.
- Pump motor cooling for RCPs 3 and 4.
- Cooling flow to the Train 3 safety chilled water chiller (QKA30), which is credited in the PRA to provide cooling to SB 3 and 4 (assumed running).
- Cooling for charging pump Train 4 (assumed in standby).

- Cooling for two of the four operational chilled water chillers (which are credited in the PRA to provide cooling to the maintenance trains of the ventilation system).

In addition to supplying the CH, each train of CCW supplies cooling to the LHSI/RHR heat exchanger and to the MHSI pump in that division. Additionally CCW Trains 2 and 3 provide cooling to the LHSI pumps in the associated division.

### Safety Chilled Water Dependencies

The four trains of safety chilled water (QKA10, QKA20, QKA30 and QKA40) provide cooling for ventilation and other equipment in the four corresponding SB. Each train can support cooling of two Safeguard Buildings (trains 1 and 2 are interconnected, as are trains 3 and 4). One chiller is initially running supplying two interconnected divisions; QKA10 (assumed running) and QKA 20 (assumed in standby) are supplying cooling to SB 1 and 2, QKA30 (assumed running) and QKA 40 (assumed in standby) are supplying cooling to SB 3 and 4. In the event that the running train of QKA fails, an automatic switchover to the standby train is provided. Diversity is incorporated into the design of the SCWS through the use of air cooling for the refrigeration units in Divisions 1 and 4, and cooling via CCW CHs for the refrigeration units of Divisions 2 and 3. Safety chilled water provides the following functions that are credited in the PRA model:

- Cooling to the four EFW pump rooms (via safeguard building ventilation systems SAC61, SAC62, SAC63, and SAC64, respectively). The EFW pumps are conservatively modeled as having dependence on safety chilled water for room cooling.

- Cooling to the electrical rooms, safety-related trains, in the SBs (via units SAC01, SAC02, SAC03, and SAC04, respectively).

- In Trains 1 and 4 (only), the safety chilled water system (air cooled) provides motor and seal cooling to the LHSI pumps.

### SB HVAC Dependencies

The complete loss of HVAC to an SB is conservatively assumed to result in the following sequence of events:

- A relatively slow heat-up of the electrical and EFW rooms in the affected SB.

- Loss of the affected equipment (including all affected division pumps and I&C components that support the CCW automatic switchover) after more than four hours (if compensatory manual actions are not implemented).

- Failure of SB1 or SB4 HVAC results in loss of HVAC to the running CCW pump (the base PRA model assumes that CCW Pumps 1 and 4 are initially running). Therefore the model requires operator action to switch the affected common

header supply over to the CCW train that was initially in standby within 4 hours, in order to maintain cooling to the affected common header.

Based on the above, an impact of a complete loss of HVAC to SB 1 on the plant response in the U.S. EPR PRA model is summarized as follows:

- Results in a complete loss of the AC and DC buses in Division 1.
- If the operator fails to switch over to the CCW pump 2 to supply common header 1 before train 1 I&C fails (more than four hours), then CCW common header 1 cooling is assumed lost. Loss of CCW common header 1 results in:
  - A loss of CCW flow to RCPs 1 and 2 motor cooling,
  - A loss to thermal barrier cooling to all four RCP pumps (the 50 percent of the time when they are supplied from the CCW common header 1).
  - A loss of charging pump 1.
  - A loss of cooling to the SCWS chiller (QKA20). The loss of QKA20 in Train 2, results in a loss of HVAC to SB 2, and therefore (eventually), a loss of the AC, DC buses and EFW in Division 2.

Similarly, an impact of a complete loss of HVAC to SB 4 on the plant response in the U.S. EPR PRA model is summarized as follows:

- Results in a complete loss of the AC and DC buses in Division 4.
- If the operator fails to switch over to the CCW pump 3 to supply common header 2 before train 4 I&C fails (more than four hours) then CCW common header 2 cooling is assumed lost. Loss of CCW common header 2 results in:
  - A loss of CCW flow to RCPs 3 and 4 motor cooling,
  - A loss to thermal barrier cooling to all four RCP pumps (the 50 percent of the time when they are supplied from the CCW common header 2).
  - A loss of charging pump 2.
  - A loss of cooling to the SCWS chiller (QKA30). The loss of QKA30 in Train 3, results in a loss of HVAC to SB 3, and therefore (eventually), a loss of the AC, DC buses and EFW in Division 3.

In summary, a loss of HVAC in a division with an initially running CCW train (Division 1 & 4 assumed) could, over time, without operator action, result in a loss of two electrical divisions.

Since CCW Pumps 2 and 3 are assumed to be initially in standby in the PRA model, the impact of a complete loss of HVAC to Division 2 or 3 would cause a complete loss of the AC and DC buses in the affected areas, but would not have other consequences.

### Depressurization Valves Dependencies

The PRA credits the PSVs and the SADV valves to perform the primary depressurization function. With regard to the core-damage sequence, this function is relevant primarily with respect to the ability to perform feed-and-bleed cooling following loss of all feedwater.

The design includes three PSVs (valves 30JEF10AA191, 30JEF10AA192 and 30JEF10AA193). Opening of each PSV requires two associated solenoids to energize. The solenoids for PSV 30JEF10AA191 receive power from 480 Vac motor control centers (MCC) 31BRA and 32BRA; the solenoids for PSV 30JEF10AA192 are powered from 480 Vac MCCs 33BRA and 34BRA; and the SOVs for PSV 30JEF10AA193 are powered from MCCs 32BRA and 33BRA. Since success of feed-and-bleed cooling requires that all three PSVs open to provide an adequate primary bleed path, all four MCCs (31BRA, 32BRA, 33BRA and 34BRA) must be available. These MCCs are backed up by two-hour batteries.

The SADVs are two sets of two motor-operated valves (MOV) in series. The upstream valves (MOVs 30JEF10AA004 and 30JEF10AA006) are parallel-disk gate valves. They receive motive power from 480 Vac MCC 31BRB. The downstream valves (MOVs 30JEF10AA005 and 30JEFAA007) are globe valves that receive power from MCC 34BRB. Therefore, power must be available from both MCC 31BRB and MCC 34BRB to open either set of SADVs to establish a depressurization flow path. These MCCs are backed up by 12-hour batteries.

### Main Steam Relief Isolation Valves Dependencies

The MSRTs are credited in the PRA as the primary means of steam relief following a reactor trip. In LOCA-type accidents, the MSRTs are credited in the PRA to perform the RCS PCD and FCD functions to support the MHSI and LHSI injection. SG isolation is also a PRA function that is modeled for SG tube rupture events. Each SG has a single MSRIV controlled by four SOVs (two pilots in series on each of the two redundant control lines). On each MSRIV, the four solenoids are powered by 480 Vac MCCs 31BRA, 32BRA, 33BRA and 34BRA. Therefore, operation of each MSRIV requires that either both MCCs 31BRA and 32BRA are available, or both MCCs 33BRA and 34BRA are available. If certain combinations of two of these buses are unavailable (e.g., MCCs 31BRA and 33BRA/34BRA, or 32BRA and 33BRA/34BRA) then all four MSRIVs will fail closed. These MCCs are backed up by two-hour batteries.

#### RCP Standstill Seal Valves and Seal Leak-Off Isolation Valve Dependencies

The valves that engage the standstill seal (the MOV through which nitrogen is supplied and the associated vent valve), and the RCP seal leak-off valves are powered by MCCs 31BRB, 32BRB, 33BRB and 34BRB for RCPs 1, 2, 3 and 4, respectively. These MCCs are backed up by 12-hour batteries.

### 19.1.4.1.1.4 Data Analysis

The U.S. EPR PRA employs data of various types and from various sources to characterize events in the sequence and system models. The types of data required for the PRA include the following:

- Frequencies of initiating events.
- Failure rates for components.
- Unavailabilities of equipment due to testing and maintenance.
- CCF factors.

#### Sources of Initiating Event Frequencies

The PRA primarily uses the following sources for the development of initiating event frequencies:

- NUREG/CR-6928 (Reference 19), NUREG-1829 (Reference 20), and Reference 13. These reports provide generic frequencies for many initiating events, based on operating experience for U.S. nuclear power plants. Frequencies from these reports were applied for general transients, secondary line breaks, and all LOCAs except ISLOCAs for which frequencies were calculated via design-specific fault-tree analysis.
- NUREG/CR-6890 (Reference 21). This report provides an analysis of experience involving LOOP from 1986-2004 (including the 2003 major grid related events), and is an appropriately up-to-date source for estimating the frequency for LOOP.
- Fault tree analysis is used to calculate the initiating event frequencies for the support system failure initiating events: LBOP and losses of CCW headers (various combinations). This method is also used to calculate the initiating event frequencies for ISLOCAs.

Table 19.1-4 summarizes the initiating events for the U.S. EPR PRA, including the frequencies and the sources from which they were derived.

For the IEs (e.g., LOCCW, LBOP, ISLOCA initiators) that were represented as developed fault trees, these developed fault trees are utilized in the accident sequence

quantification. Both the base model runs and the uncertainty runs utilize the fault tree directly in the evaluation.

For the purpose of estimating the ISLOCA initiating event frequency in the point-estimate model, correlated failure events are multiplied by appropriate State of the Knowledge Correlation (SOKC) factors to correct for the SOKC. This is done to account for the fact that the uncorrected point-estimate values are not a reasonable estimate of the mean values. These SOKC factors are not used in the uncertainty evaluation (since the uncertainty calculation already accounts for the correlated data effect directly).

### Sources of Component Failure Data

The U.S. EPR PRA uses component failure data from a number of generic sources to characterize the failure probabilities of the U.S. EPR components. Selection of generic sources is based on relevant industry experience. These failure data sources include:

- "Generic Component Failure Database for Light Water and Liquid Sodium Reactor PRAs," EGG SSRE-8875 (Reference 22). This report serves as a source for most of the failure rates for mechanical and electrical components.

- "Centralized Reliability and Events Database of Reliability Data for Nuclear Power Plant Components," ZEDB Analysis for 2002 (Reference 23). This data source includes all German nuclear plants, Dutch Unit Borssele, and Swiss Unit Goesgen. This source is used to take advantage of the European operating experience for the components that are part of the basic U.S. EPR design.

- "European Industry Reliability Data Bank," EIReDA95 (Reference 24). This source is used for a limited number of the components (e.g., safety relief valves).

The preceding sources of data were compared with widely accepted U.S. data sources such as the Reference 18, and NUREG-1715 (Reference 25) series of studies, and the ALWR Database in Reference 14. This evaluation shows that the U.S. EPR data is comparable to the other U.S. data sources.

### Common Cause Component Groups and CCF Parameters

Modeling of CCFs is based on the methods presented in NUREG/CR-5485 (Reference 26). The following principles are used in selecting CCF groups:

- Intra-system CCFs are modeled for similar, non-diverse, active components. Independence is assumed for components of diverse design or function.

- Inter-system CCF is generally not modeled based on a high-level review and the current state of knowledge for component design and maintenance and testing practices. The exception to this approach is the modeling of CCF of the sump strainers for the IRWST, to capture the common impact of the potential for blockage by debris.

The CCF values used in the U.S. EPR PRA are based on an update to the data collected by the U.S. NRC (Reference 27).

#### 19.1.4.1.1.5 Human Reliability Analysis

The HRA identifies human actions that may impact the availability of equipment necessary to perform the system function modeled in the PRA, human actions that are required for different accident sequences modeled in the PRA and estimates the failure probabilities for these human events. The HRA considers two types of human actions:

- Pre-initiator actions: actions that, if not performed correctly, can leave equipment or systems unavailable to respond to a demand created by an initiating event.
- Post-initiator actions: actions that must be taken to initiate or control the function of a system, or to compensate for a system failure, during an accident sequence.

##### Pre-initiator Human Actions

Pre-accident operator actions are associated with routine test and maintenance (T&M) activities. These pre-accident operator actions, if not performed correctly, could impact performance of the mitigating system after an accident. Operating and maintenance practices and the procedures that will guide them are not yet available for the U.S. EPR. Therefore, pre-initiator human actions were systematically identified by evaluating each mitigating train credited in the PRA, and making T&M assumptions based on engineering judgment and experience with similar systems at currently operating nuclear power plants. The corresponding human error probabilities were estimated by using the methodology developed for the ASEP (Reference 28). The ASEP method is a slightly modified version of the Technique for Human Errors Rate Prediction (THERP) method, which provides a more conservative, but significantly faster evaluation of the HEPs associated with routine test and maintenance activities.

Based on the ASEP methodology, pre-accident HEPs are considered negligible if the component, usually a valve manipulated during a test or maintenance, has a status indication in the control room. A relatively minor change was made in applying the ASEP methodology for the U.S. EPR. Two error-discovery measures, test following the maintenance activity and an independent verification, are treated in ASEP as completely dependent. That is, if the post-maintenance test does not uncover the error, no credit is given to the independent verification. In the U.S. EPR PRA, this level of dependence was changed from complete to medium. This reduced the probability for cases in which both discovery mechanisms should come into play by a factor of 0.23 relative to the basic ASEP methodology. However, a check of equipment status during each shift was not credited. Two pre-accident HEP values used in the U.S. EPR PRA correspond to the HEPs with (modified ASEP Case VIII, HEP=7E-05)

and without (ASEP Case III, HEP=3E-03) an effective post-maintenance test (e.g., a pump flow test).

In addition to failures to restore equipment following test or maintenance activities, pre-initiator human actions typically consider actions that could lead to calibration errors as well. These errors are not explicitly evaluated for the U.S. EPR because there is not yet sufficient detail regarding design or calibration practices to permit a meaningful assessment. However, digital I&C systems are less susceptible to calibration errors than analogous analog systems because digital components are not vulnerable to drift. The mechanical parts (e.g., sensors) may require periodic calibration, and these adjustments are made by changing a software parameter in the digital system, which the PRA considers as part of the SWCCF contribution.

The actual analysis was performed and documented using the EPRI HRA Calculator software. This tool is discussed in Section 19.1.4.1.1.7 with other computer codes.

### Post-initiator Human Actions

The design philosophy of the U.S. EPR is that systems and controls are designed so that an operator action is not required to mitigate design basis accidents or anticipated operational occurrences within 30 minutes if the actions can be performed from the MCR, or within 60 minutes if they would be performed outside the MCR. The PRA is not limited to the design philosophy expectations and considers realistic timings for the different human actions consistent with the sequence of interest. The operator actions credited in the PRA model are generally well established actions that would be taken in response to sequences that include multiple failures of safety-related equipment. The actions include, for example, initiating feed-and-bleed cooling for accidents involving a complete loss of secondary side cooling, or starting the SBODGs upon a loss of AC power and failure of all EDGs.

A U.S. EPR design goal is to design the plant so that one licensed Senior Reactor Operator (SRO) and two operators with Reactor Operator (RO) licenses can safely monitor and control the plant under all operating conditions including normal operation, startup, shutdown, abnormal operation, and accident conditions. It is assumed that one of the two RO-licensed operators will not generally be required to be at the controls during normal, at power operations. Additionally, each operating crew will consist of one Shift Supervisor (SS) (SRO licensed), a Shift Technical Advisor (STA), and four non-licensed equipment operators (NLOs). A maintenance crew consisting of chemistry, radiation protection, I&C, electrical, and mechanical technicians and a maintenance supervisor is expected to support each shift.

Emergency operating guidelines and procedures are not yet available for the U.S. EPR. Therefore, as for the pre-initiator actions, the post-initiator human actions evaluation was based on engineering judgment and experience with currently operating nuclear

power plants. The corresponding HEPs were estimated by using the method referred to as Standardized Plant Analysis Risk – Human Reliability Analysis (SPAR-H) (Reference 10). SPAR-H is a simple and conservative method for estimating the probabilities associated with failures in deciding upon or implementing actions in response to initiating events. The use of SPAR-H is appropriate for the current stage of the U.S. EPR design when operating guidelines and procedures are not available.

The SPAR-H method bases its probability estimates primarily on time available for the diagnosis and action, coupled with high-level performance shaping factors (PSF). The PSFs that were evaluated for the HRA in the design certification include: (1) time available to decide on and take action, (2) the assumed level of stress, (3) the complexity of the decision and implementation, and (4) the assumed level of experience and training of the operating crew.

The PSFs relating to the time available account for the following:

- The total time window ($T_{sw}$). This is the time from the initiating event to the point at which the action could no longer achieve the intended result (e.g., the time at which core damage would be unavoidable). The time windows are generally estimated from design-specific thermal-hydraulic analyses.

- The time delay ($T_{delay}$). This is the time from the initiating event to when the first cue is received. This time is generally estimated from knowledge of the accident sequence, the available instrumentation, and thermal-hydraulic analysis.

- The median time needed for diagnosis ($T_{½}$). The diagnosis time is based on engineering judgment, accounting for a reasonable time for cognition based on the complexity of the cues and the clarity of the instructions anticipated to be provided in the relevant emergency operating procedures. Taken together, the delay time for the cue ($T_{delay}$) and the median response time for diagnosis ($T_{½}$) represent the nominal time needed for the crew to make the proper decision on a course of action.

- The time needed to perform the action ($T_M$). This time is estimated based on the complexity of the action, and whether or not it can be performed from the MCR. This time was generally estimated to be five minutes for simple MCR actions and 15 minutes for actions that must be performed locally (i.e., outside the MCR). These action times were adjusted as necessary for actions that entail multiple steps or complexity.

The PSF for stress is assigned as extreme (five times the nominal value), high (two times), or nominal. This assignment was based on engineering judgment and knowledge of the relevant accident sequence. For example, extreme or high stress was assigned for accident sequences that go well beyond expected conditions (e.g., an SLOCA with failure of safety injection) or where the proposed operator action is somewhat drastic (e.g., implementing feed-and-bleed cooling).

The PSF for complexity is assigned as high (five times nominal), moderate (two times), nominal (one time), or obvious (0.1 time). The latter factor is applied only to the contribution from diagnosis, not to the implementation. The selection for this PSF was also based on engineering judgment. For example, accident sequences in which cues might be ambiguous (e.g., an SLOCA that does not depressurize) are assigned high complexity. In other cases (e.g., SGTR), the cues may be compelling, and accordingly, obvious diagnosis is assigned.

For the experience and training PSF, the specific qualifications of the operators are not known at this time, and the base PSF reflects nominal conditions or insufficient information. For certain operator actions, a PSF reflecting a higher than nominal level of training and experience was applied. This factor (0.5 times the nominal value) was applied, such as to an operator failure to initiate feed-and-bleed cooling or to initiate cooldown of the RCS, because these are actions that are likely to receive extensive attention in operator training and to be practiced many times on the simulator.

The PSF for procedures are assigned to nominal (one) or insufficient information (one) for most of the operator actions because EOP are not yet available for the U.S. EPR design. However, since the EOP will be of the symptom-oriented type, the PSF for "symptom oriented" (0.5 times the nominal value) was assigned for certain operator actions that have symptom-based cues.

The PSFs for ergonomics, fitness for duty, and work processes are assigned to nominal (one) or insufficient information (one) until detailed design information is developed.

*Dependency between Operator Actions*

In some cases, the sequence cutsets include more than one post-initiator human failure event. The dependencies among these actions was modeled by applying the SPAR-H rating system to consider such factors as whether the same crews would be involved in multiple actions; the proximity of the actions in time and location; and the similarity of the cues for the actions. Four levels of dependencies were modeled: low, moderate, high and complete.

#### 19.1.4.1.1.6 Sequence Quantification

This section summarizes the process used to quantify the frequency of core damage. Because this process is heavily dependent on the computer codes used, the codes are described as well in following paragraphs.

The frequencies of the core-damage sequences are calculated by obtaining sequence-level minimal cutsets. Post-processing of these cutsets is performed to account for factors that are not readily incorporated into the fault trees themselves. For example, this post-processing allows the identification of cutsets that contain more than one

post-initiator human failure event. The dependencies between such events are assessed as appropriate, and included in the cutsets in post-processing.

The event trees and fault trees were developed and solved using the RiskSpectrum® computer code. The RiskSpectrum® model for the U.S. EPR constitutes a large, detailed set of event trees and fault trees. The model whose results are described in this report consists of the following:

- Over 4200 basic events (not including CCFs).
- Over 2500fault trees
- Over 8200 fault tree gates.
- Over 230 CCF groups.
- Over 6400 specific CCF events.

The model is solved by using a 1E-20 truncation limit, and a 1E-06 relative truncation limit. The CDF quantification, for Level 1 at power and shutdown, all events, resulted in over 260,000 cutsets. The first 100 cutsets represented close to one third of the total CDF; 95 percent of the CDF was represented by over 100,000 cutsets.

The quantification results are presented in the corresponding sections for internal, fire, flooding and LPSD events. The quantification results for the total CDF are summarized in Section 19.1.8.

The uncertainty analysis is performed by standard Monte Carlo simulation executed within RiskSpectrum® using the input distributions for the initiating events, failures rates, CCF, and human failure events. Both point estimate values and the mean values are reported for the CDF and LRF. Limited treatment of modeling uncertainty was also included in the calculations. The phenomenological uncertainties and most modeling uncertainties are addressed in the sensitivity analyses. The uncertainty analysis approach is discussed further in Section 19.1.4.1.2.7. The specific uncertainty analyses that were performed are discussed in the corresponding sections for internal, fire, flooding and LPSD events. The uncertainty analysis performed for the total CDF is discussed in Section 19.1.8.

The sensitivity analyses are performed to address phenomenological uncertainties (e.g., uncertainties in the success criteria) and the PRA model uncertainties (due to various assumptions made in the PRA model). Factors selected for sensitivity analysis are based on their perceived importance in the PRA model. The specific sensitivity studies that were performed are discussed in the corresponding sections for internal, fire, flooding and LPSD events. The sensitivity studies performed for the total CDF are discussed in Section 19.1.8.

### 19.1.4.1.1.7 Computer Codes used in PRA Level 1 and 2 Analysis

Specialized computer software was used for several of the technical areas in the U.S. EPR PRA. These codes are discussed below. The RiskSpectrum®, MAAP, S-RELAP5 and the EPRI HRA Calculator Software Codes are described as follows:

#### RiskSpectrum® Professional

The PRA model is developed and quantified using the RiskSpectrum® PSA software package. RiskSpectrum® PSA is a product of Scandpower AB of Sweden. This software supports use of the linked fault-tree methodology. Analysis cases are created for fault tree analysis, event tree sequence analysis, and consequence analysis. To create these analysis cases, the basic fault-tree models are specialized to the sequence of interest using house events, exchange events, and boundary-condition sets. When multiple sets of minimal cutsets are obtained, they can be merged to provide an integrated set of results for the PRA. A cutset editor allows for further refinement of the results. Several event trees can be linked, including Level 1 event trees with Level 2 containment event trees (CET). A comprehensive set of importance factors can be generated along with uncertainty.

Basic event reliability parameters can be presented as a probability, failure rate, or frequency and can incorporate mission time, test interval, MTTR, and time to first test within these models, as applicable. Parameters can be provided as point-estimate values or can be represented by various probability distributions, including normal, lognormal, beta, and gamma. CCF modeling is automated using common-cause groups and can use either the MGL method or the alpha-factor method.

RiskSpectrum® is designed to execute on a personal computer (PC). Test output supplied from ScandpowerAB is used to validate correct installation and operation of the code. RiskSpectrum® PSA is currently being used by half of the world's nuclear power plants, as well as in the oil and gas, defense, aviation, space, chemical process and transportation industries.

#### Modular Accident Analysis Program

The Modular Accident Analysis Program, Version 4 (MAAP4) is an integrated system code that combines, in one package, models for heat transfer, fluid flow, fission product release and transport, plant system operation and performance, and operator actions. Physical models exist for processes that are important during transients that lead to and go beyond fuel damage. The models are coupled at every time step.

MAAP4 provides an accident analysis tool to study all phases of severe accident studies, including accident management. MAAP4 includes models for accident phenomena that can occur within the primary system, the containment, or auxiliary-type buildings. For a specified reactor and containment system, MAAP4

calculates the progression of the postulated accident sequence (including the deposition of the fission products) from a set of initiating events to either a safe, stable state or to an impaired containment condition (by over pressure or over temperature), and the possible release of fission products to the environment.

MAAP4 version 4.07 is used to support the U.S. EPR PRA. This version of MAAP4 contains specific models for U.S. EPR design features. The U.S. EPR has specific containment regions devoted to debris stabilization and long term cooling should a severe accident lead to melting of the reactor core and RPV failure. The modifications performed to the MAAP4 code address the ways in which these specific containment features are represented in the MAAP4 framework. The AREVA NP Severe Accident Evaluation Topical Report (Reference 29,) provides further information on MAAP 4.07.

In the Level 1 analysis, MAAP4 is used to perform deterministic thermal-hydraulic analysis to support the development of system success criteria and to estimate the times available for particular operator actions. Developing success criteria for the wide variety of plant scenarios modeled in the PRA requires a large number of calculations. MAAP4 was chosen to perform these calculations because of its fast computation times relative to more detailed codes.

MAAP4 was used to analyze success criteria for the following initiating events:

- Loss of Main Feedwater (LOMFW).
- LOCAs (small, medium and large).
- Steam Generator Tube Rupture (SGTR).
- Steam Line Breaks Inside and Outside of Containment (SLBI and SLBO).
- Feed and Bleed Scenarios.

Because of the simplified modeling techniques employed by MAAP4, there is uncertainty as to MAAP4's ability to model the thermal hydraulic phenomena for certain events such as the larger LOCAs. In addition, MAAP4 does not calculate an actual peak clad temperature for the limiting fuel rod, but rather calculates a peak average clad temperature for a region of the core. Therefore, to obtain a better understanding of the MAAP4 results, a benchmarking effort has been performed for application of MAAP4 in the Level 1 PRA. For selected events, use of MAAP4 is justified by qualitative arguments and comparison to parallel calculations conducted with the S-RELAP5 computer code.

For Level 2 analysis, MAAP4 is used to perform deterministic severe accident analysis (i.e., the simulation of the course and progression of a severe accident sequence).

Calculations made using MAAP4 constitute an important input to the Level 2 PRA in three areas:

- To assist in developing the containment event tree and understanding the most likely event progression for important sequences within a damage state bin.
- To assist in quantifying the containment event tree by aiding in understanding the important phenomena resulting from a severe accident.
- To characterize the source term—the composition, magnitude, and timing of releases to the environment associated with each of the RC bins.

### MAAP Benchmarking

Some of the scenarios modeled for the Level 1 PRA may challenge the simplified modeling incorporated within MAAP4. The loss of feedwater event should be well represented with MAAP4, as long as the event does not lead to core uncovery. This is because the analysis of the event primarily requires that a proper mass and energy balance be performed, and MAAP4 satisfies this requirement. The same can be said for the LOOP event. For other events, the MAAP4 simplified modeling may result in uncertainties for calculated values. In these cases, the benchmarking provides additional insight for interpretation of the MAAP4 results.

To obtain a better understanding of the resulting accuracy of the MAAP4 results, and establishing success criteria in MAAP4, parallel calculations were performed for a selected set of cases using the S-RELAP5 code. These cases were chosen to envelop the significant thermal hydraulic phenomena expected in the events analyzed in the Level 1 PRA. The main conclusions are:

- LOMFW – MAAP4 compares well with S-RELAP5. Primary to secondary heat transfer agrees well between the codes. It is concluded that MAAP4 adequately models heat removal requirements for transients such as LOMFW, LOOP, and other general transient events.
- If the RCPs are running under conditions of very low RCS inventory, MAAP4 over-predicts the temperatures relative to S-RELAP5. This was seen in the three-inch SLOCA case. This is because, when there is void formation in the core, MAAP4 assumes a complete phase separation, while S-RELAP5 calculates a steam water mixture being pumped through the core, providing core cooling. Therefore, MAAP4 LOCA cases with RCPs running are not considered dependable and can be penalizing.
- For a two-inch SLOCA (with partial cooldown and one MHSI available), there was good agreement between the codes. Parameters such as SG water level, RCS pressure and break flow showed reasonable agreement between S-RELAP5 and MAAP4, and neither code predicted core uncovery. Therefore, MAAP4 can be considered acceptable for smaller SLOCA events.

- In a three-inch SLOCA, if the RCPs are tripped, MAAP4 over predicts the primary to secondary heat transfer relative to S-RELAP, along with early development of natural circulation. Approximately 20 minutes is required for natural circulation to develop in S-RELAP5. This does not have significant impact. For this case, most system parameters are in good agreement, and the peak cladding temperature (PCT) in MAAP4 was under-predicted by approximately 800°F. This provides information for interpreting the MAAP4 PCT value.

- For larger LOCAs, MAAP4 under-predicts PCT by approximately 400°F, while other system parameters are in good agreement. This provides additional information for interpreting MAAP4 PCT values. In any case, considering that MAAP4 calculations can have larger uncertainties for the analysis of large break LOCAs, the success criteria for larger LOCAs do not rely completely on MAAP4 results.

- In any core heatup transient, since MAAP4 does not model the core in detail, the peak cladding temperature for the hot rod is not captured. Using parallel calculations with S-RELAP5 for a TLOFW event, it is estimated that MAAP4 could under predict the peak cladding temperature by about 400°F.

Based on the above results, the following bases for success criteria are applied when using MAAP4:

- MAAP4 cases resulting in a PCT of 1400°F or less will be considered a success.

- MAAP4 cases resulting in a PCT of 1800°F or greater will be considered a failure

- MAAP4 cases resulting in a PCT greater than 1400°F and less than 1800°F will be examined in detail, possibly with a corresponding S-RELAP5 calculation.

### S-RELAP5 Accident Analysis Code

S-RELAP5 is used in the PRA to benchmark or validate event-specific MAAP4 calculations and acceptance criteria. AREVA NP developed the S-RELAP5 safety analysis code to perform LOCA and non-LOCA PWR safety analyses. S-RELAP5 has been approved by the NRC for PWR safety analysis.

S-RELAP5 uses a two-fluid, non-equilibrium, non-homogeneous, thermal-hydraulic model for transient simulation of the RCS that is used primarily for safety analysis calculations. The basic S-RELAP5 models include the following: hydrodynamic, heat transfer, heat conduction, fuel, reactor kinetics, control system, and trip system models. The hydrodynamics include generic component models (e.g., pumps, valves, accumulators) and some special process models (for choked flow and countercurrent flow limitations). The system mathematical models are solved by fast numerical schemes to permit cost-effective computations.

The input model of the U.S. EPR for the S-RELAP5 code contains detailed nodalization of the primary system, including the reactor vessel, cold and hot legs,

pressurizer, pressurizer relief valves, primary side of the SGs (four loops), and the SISs. For the secondary side, the S-RELAP5 model includes SGs, EFW, MSRTs, MSSVs, and steam lines.

The S-RELAP5 model of the U.S. EPR used for these analyses is based on the model developed for the U.S. EPR safety analysis. For the purpose of this benchmarking study, input parameters in the S-RELAP5 model were changed to be realistic (nominal values), consistent with the values used in the MAAP4 model. This is also consistent with how S-RELAP5 was benchmarked against experimental data as part of the USNRC approval process.

#### EPRI HRA Calculator

The U.S. EPR PRA uses the EPRI HRA Calculator. The EPRI HRA Calculator is a software tool designed to facilitate a standardized approach to HRA. The EPRI HRA Calculator is designed to step PRA analysts through the HRA tasks needed to develop and document human failure events (HFE), and to quantify their probabilities. The current version of the calculator provides a choice of evaluation methods, including the EPRI Cause-Based Decision Tree Method, the Human Cognitive Reliability/ Operator Reactor Experiments (HCR/ORE), the ASEP method, SPAR–H, and the THERP.

For the PRA, AREVA NP primarily uses the ASEP method for evaluating pre–initiator human failure events and the SPAR–H method for assessing post-initiator HFEs. The EPRI HRA Calculator incorporates the SPAR–H worksheet, which is a major component of the SPAR-H method, and the SPAR-H dependency rating system. Validation of proper installation and execution of the code is performed.

The EPRI HRA Calculator development is directed by the EPRI HRA/PRA tools Users Group. Membership currently includes 19 utilities comprising more than 60 nuclear power plants in the U.S. and one international member (the CANDU Owners Group).

### 19.1.4.1.2 Results from the Level 1 Internal Events PRA for Operations at Power

#### 19.1.4.1.2.1 Risk Metrics

Total CDF from internal events is 2.4E-07/yr, less than 1E-06/yr. This is well below the NRC goal of 1E-04/yr (SECY-90-016, Reference 30) and the U.S. EPR probabilistic design goal of 1E-05/yr. Mean value and associated uncertainty distribution can be found in Section 19.1.4.1.2.7.

#### 19.1.4.1.2.2 Significant Initiating Events

The significant initiating events and their contribution to the internal CDF are given in Table 19.1-6—U.S. EPR Significant Initiating Event Contributions - Level 1 Internal Events (Contributing more than 1% to Internal Events CDF). Only those initiating

events that contribute more than one percent to the total internal events CDF are listed in the table. All initiating events and their contributions are illustrated in Figure 19.1-4—U.S. EPR Initiating Events Contributions - Level 1 Internal Event. As can be seen from Table 19.1-6 and Figure 19.1-4, the LOOP initiating event strongly dominates the internal events CDF (over 40 percent). This is not a surprise because the U.S. EPR is an active plant with no passive systems. In order to illustrate in more detail the total LOOP contribution to CDF, the LOOP sequences were divided into four categories.

- LOOP events (no seal LOCA, no SBO) contribute over 13 percent to the total CDF.
- LOOP events (no SBO, seal LOCA) contribute 5 percent to the total CDF.
- LOOP events (SBO, no seal LOCA) contribute close to 25 percent to the total CDF
- LOOP events (SBO and seal LOCA) contribute close to 4 percent to the total CDF.

The next biggest contributors to plant risk are SLOCA and loss of component cooling events (both contribute above 10 percent to the total CDF).

- SLOCA contribution can be attributed to a larger range in the break sizes and the corresponding higher frequency of SLOCA, and to common injection system failures (IRWST strainers or common injection check valves).
- The loss of component cooling's relatively high contribution can be attributed to a high initiating event frequency (multiple combination of failures leading to losses of one of two CCW common headers), and to diverse impacts on the support systems, like RCP pumps seal cooling, ventilation chillers and safety injection pumps cooling.

#### 19.1.4.1.2.3 Significant Cutsets and Sequences

Cutset contribution to the internal events CDF is equally distributed. Only eight of the top cutsets contribute more than one percent to the total CDF. The number of cutsets that contribute to 95 percent of the CDF is over 50,000. That clearly shows there are no outliers in the U.S. EPR internal events CDF.

The significant cutsets for the internal events are illustrated in Table 19.1-7—U.S. EPR Important Cutset Groups - Level 1 Internal Events. In this table, the first hundred cutsets are grouped based on their similar/symmetric impact on mitigating systems. Groups of cutsets like these usually correspond to specific sequences in the event trees. These sequences are also identified in the table. Columns in the table show: group number, the number of cutsets included in the group, frequency range of the cutsets included in the group, group percentage contributions to the total CDF, cumulative percentage contributions to the total CDF, a selected representative cutset, with corresponding basic events and their descriptions, and the sequence description.

As shown in Table 19.1-7, the top 100 cutsets are grouped into 23 groups, representing over 30 percent of the CDF. One third of these groups are LOOP related, either started with a LOOP initiating event, or a consequential LOOP has occurred as a result of a different initiator. Five of these groups are related to an SLOCA initiating event.

Groups 1 and 15 represent sequences leading to a total SBO, starting with a LOOP event and a failure to recover power in two hours (or a general transient and an unrecoverable consequential LOOP), followed by a CCF of all EDGs and a failure of one SBODG and one EFW pump in the division of the other SBODG. Groups 2, 3 and 14 are similar except that instead of one SBODG failure and one EFW train failure, both SBODGs have failed.

Groups 4 and 16 represent a total loss of instrumentation, which started with a LOOP event (an initiator or a consequential LOOP), and is followed by a CCF of all safety-related batteries on demand. These sequences are conservatively assumed to lead to core damage, without crediting a LOOP recovery or non safety batteries, because no instrumentation will be available to operators.

Group 5 represents sequences leading to a partial SBO, starting with a LOOP event and a failure to recover power in two hours, followed by a CCF of three EDGs, failure to start SBODGs in non-SBO conditions and failure of the EFW pump and the SI pumps from the one available electrical division.

Groups 6 through 10 represent SLOCA cutsets. Groups 6, 8, and 10 describe cutsets resulting from SLOCA events followed by a failure of all safety injection either because of a common cause plugging of the IRWST sump strainers, and failure to open LHSI/MHSI common injection check valves, or because of a CCF of MHSI pumps and operator failure to initiate fast cooldown. Group 9 describes cutsets resulting from SLOCA events followed by the CCF to open MSRIVs resulting in the failure to perform partial or fast cooldown, followed by operator failure to initiate feed and bleed. One of the modeling assumptions can be noticed in the SLOCA groups, if MHSI is failed; it is assumed that operators would initiate an FCD. However, if MHSI fails because of a failure of a PCD function, it is assumed that operators would initiate feed and bleed. These modeling assumptions and timing of these sequences will be analyzed in more details after operating procedures are available.

Groups 11 to 13 describe ATWS events followed by a failure of reactivity or pressure control.

The remaining groups describe a few specific initiators: GT, LOMFW, induced SGTR, LOCCW, LBOP and LLOCA. A detailed description of these groups is provided in Table 19.1-7.

The important CDF sequences for internal events are presented in Table 19.1-127—U.S. EPR Important Sequences – Level 1 Internal Events (Contributing more than 1% to the Total CDF). The "important" CDF sequences are defined as those sequences with a sequence frequency greater than one percent of total at-power CDF, as presented in Section 19.1.8.1. For each sequence, Table 19.1-127 gives corresponding event tree, sequence number, event tree sequence identifier, the sequence frequency, and a brief description. It also connects the sequence to the corresponding cutset group in Table 19.1-7, which gives a more detailed description of the sequences.

#### 19.1.4.1.2.4 Significant SSC, Operator Actions and Common Cause Events

Table 19.1-8—U.S. EPR Risk-Significant Components based on FV Importance - Level 1 Internal Events through Table 19.1-11—U.S. EPR Risk-Significant Human Actions based on RAW Importance - Level 1 Internal Events shows the important contributors to the internal CDF. Importance is based on the Fussell-Vesely (FV) importance measure (FV ≥0.005), or the risk achievement worth (RAW) importance measure (RAW ≥2).

Table 19.1-8 shows the risk-significant structures, systems and components (SSC) based on the FV importance measure. The components with the highest FV are the EDG trains, SBO DG trains, and EFW trains supported by SBO DGs. The most important SSC can be explained by a high LOOP contribution to the total CDF.

Table 19.1-9—U.S. EPR Risk-Significant Components based on RAW Importance - Level 1 Internal Events shows the risk-significant SSC based on the RAW importance measure. Three of the five most important events are connected to the operation of the Division 4 cooling chain (ESW and UHS). Their high RAW rank can be explained by a high consequence of their failures: loss of the cooling Division 4 can potentially disable the CCW common header 2 and cooling to the operating HVAC chiller in Division 3. A failure of MSIV in the Division 4 is also important because all of the SG breaks (SGTRs and SLBs) are assumed to occur in the Division 4 and the failure of the corresponding MSIV would fail the break isolation.

Table 19.1-10—U.S. EPR Risk-Significant Human Actions based on FV Importance - Level 1 Internal Events shows the risk-significant human actions based on FV importance. The most important operator action based on the FV is the operator failure to recover room cooling locally given the loss of ventilation. This importance illustrates the importance of the HVAC system. This action, that follows any failure of ventilation to the SBs, shows in cutsets that contribute 12 percent to the total CDF.

Table 19.1-11—U.S. EPR Risk-Significant Human Actions based on RAW Importance - Level 1 Internal Events shows the risk-significant human actions based on RAW importance. The most important human actions based on RAW are: operator action to manually align EFW tanks within six hours given a failure of one EFW train, operator

action to depressurize RCS and initiate RHR, and operator action to initiate feed and bleed for transient events. Their high RAW rank can be explained by their relatively high reliability and by a high consequence of their failures.

Table 19.1-12—U.S. EPR Risk-Significant Common Cause Events based on RAW Importance - Level 1 Internal Events shows the significant common-cause events based on RAW importance. As it would be expected in a plant with four safety divisions, the common cause events are very important. The most important common cause event based on RAW importance is the CCF of the safety-related batteries on demand because, in the case of a LOOP event, this event is assumed to lead directly to core damage. The next most important common-cause events are the CCF of IRWST sump strainers and CCF of SIS common injection check valves, where both lead to a total failure of safety injection. The next two most important common cause events are the CCFs of the running ESW or CCW pumps, which could potentially lead to an initiator with impact on the multiple mitigating systems.

Table 19.1-13—U.S. EPR Risk-Significant Common Cause I&C Events based on RAW Importance - Level 1 Internal Event shows the significant common-cause I&C events based on RAW importance. As illustrated in this table, I&C common-cause events (e.g., I/O modules, software, sensors, computer processors, or SAS) have a high RAW. This is because a CCF of the signals could lead to an actuation or control failure of safety systems such as EFW, SIS, or EDGs.

Table 19.1-14—U.S. EPR Risk-Significant PRA Parameters - Level 1 Internal Events shows the significant modeling parameters used in the analysis, the significant preventive maintenance performed on the various trains, and the significant LOOP-related basic events. The significance is determined based on either the FV or RAW importance measure, as defined above. This table illustrates a high significance (a high FV) of the parameters used in the modeling of an RCP seal LOCA. It also shows that a CCF of stuck control rods has a high FV value. This high importance could be attributed to an ATWS-related conservative assumption that for many high frequency events, which include a loss of MFW or a loss of condenser, a failure to scram is assumed to lead directly to core damage. LOOP-related basic events (a LOOP during 24 hours or a consequential LOOP) also show a high significance. Preventive maintenance importance measures illustrate importance of the various safety trains. Based on the FV values presented in Table 19.1-14, EDGs and SBODGs have the highest importance, which could be attributed to a general LOOP importance.

#### 19.1.4.1.2.5 Assumptions

Assumptions in the PRA development are divided into two groups:

- Key assumptions in response to key sources of uncertainty in the knowledge

- Modeling assumptions made because of limitations in the PRA logic models or software

The most important assumptions from these two groups are listed below:

**Key Assumptions:**

- EDGs and SBO DGs are assigned to different common-cause groups. This assumption will be confirmed by assuring diversity between EDGs and SBO DGs (different model, control power, HVAC, engine cooling, fuel system, location).

- The HRA is performed under assumptions that the operating procedures and guidelines will be well written and complete; and so will operator training.

- Different operator actions HEPs are estimated for the SBO conditions (LOOP and all EDGs not available) versus non-SBO conditions (LOOP and at least one EDG available). It was assumed that operators will have more clear direction about the crosstie of buses and equipment, in clear SBO conditions, when no emergency power is available. This assumption will be evaluated when the operating procedures and guidelines are available.

- It is assumed that if ventilation cooling is lost to a division of HVAC (both the normally operating safety train and the non-class powered maintenance train), that equipment survivability could be maintained by the operator aligning portable fans or by simply opening doors. Considering typical industry survivability information and the room heat-up analysis, this assumption is judged as acceptable. This action is included in the HVAC models as operator action OPF-SAC-2H. Based on the room heat -up analysis, it was concluded that the operators will have at least four hours available to align the maintenance train of HVAC or to provide an alternate means of cooling.

- Operator action "OPF-TB CH SO" considers operator action to switch RCP thermal barrier cooling to the alternate CCW header. Because of a short time availability, this action is credited only for slow developing initiating events like certain flooding events where it has been judged that adequate time is available to perform the action before thermal barrier cooling is lost from the in-service common header.

- For events that consider both MFW and SSS for event mitigation, the common dependencies of the two systems are modeled in both the SSS and MFW fault trees. Therefore, the common MFW and SSS dependencies are specifically accounted for in the accident sequence quantification. However, for a loss of main feedwater initiating event, only SSS is credited for event mitigation and there is a possibility that SSS could be disabled by the failures that resulted in loss of MFW. Therefore, for the loss of main feedwater initiating event, it is necessary to account for the possibility that the loss of main feedwater initiating event also fails SSS. This dependency was accounted for by quantifying the MFW fault tree, and examining the cutsets to identify the loss of main feedwater cutsets which would fail both SSS and MFW. It was determined that 81percent of loss of main feedwater events may potentially fail both MFW and SSS. Therefore, the basic

event "CF LOMFW/SSS" is included in the SSS fault model with a basic event probability of 0.81 to account for the possibility that SSS may be rendered ineffective for a loss of MFW initiating event.

- There are two UHS fans for each UHS cooling tower train, however a single fan is capable of handling the normal at-power operating UHS heat load. The major post-accident UHS heat load is the RHR heat exchangers, and when the RHR heat exchanger is in operation, both UHS fans are required. Both fans must be lost to initiate a loss of ESWS initiating event.

- CVCS is not credited for an RCS injection function. CVCS is only credited for the RCP seal injection. It is assumed that the CVCS supply from the volume control tank will be available for majority of the events where CVCS is credited for the RCP seal injection, with an estimated probability of 0.1. This assumption will be evaluated when plant–specific information is available.

- RCP seal LOCA probability, given a total loss of seal cooling and the RCP trip, is assumed to be equal to 0.2.

- A full year (8760 hours) was used for evaluation of the initiating event frequencies at power. It was not adjusted for time assumed to be spent at shutdown. For the current assumption on the shutdown duration (18 days), an adjustment factor would be 0.95. This assumption will be evaluated when plant –specific shutdown information is available.

**Major Modeling Assumptions:**

- The PRA Model is not symmetric. For modeling simplification purposes, assumed configurations are as follows:

i. CCW10/ESW10 and CCW40/ESW40 are assumed to be initially running with CCW20/ESW20 and CCW30/ESW30 either in standby or unavailable due to maintenance.

ii. QKA10 and QKA30 are assumed to be initially running with QKA20 and QKA40 either in standby or unavailable due to maintenance.

iii. QNA chillers 21, 22 and 23 are assumed to be initially running with QNA chiller 24 either in standby or unavailable due to maintenance.

iv. CVCS10 is assumed to be initially running with CVCS20 either in standby or unavailable due to maintenance.

v. For thermal barrier cooling, the two possible configurations are modeled, with a weight of 50 percent each. The selection of configuration is done in the model by creating two basic events, "CONF CH1 TO TB" and "CONF CH2 TO TB." Each basic event has a probability of 0.5. The configuration basic events are also used to disallow preventative maintenance on the side of the common header aligned to the RCPTB.

vi. UHS Fan 1 (PED10AN001 and PED40AN001) are assumed to be initially running and the other six fans (PED10AN001, PED30AN001, PED10AN002, PED20AN002, PED30AN002 and PED40AN002) are assumed to be initially in standby.

vii. All breaks (LOCAs, SLBs, SGTRs) are assumed to occur in Loop/Division 4.

These symmetry related assumptions effect train-specific importance measures.

- In the calculation of the IE frequencies by fault trees, all year mission time was used for the common cause events. However, running and stand-by pumps were modeled in different common cause groups.

- In modeling SLOCA events, if the MHSI system fails, it is assumed that operators would initiate a fast cooldown. However, if a partial cooldown function fails (therefore failing MHSI), it is assumed that operators will initiate feed and bleed. These modeling assumptions and timing of these sequences will be analyzed in more details after operating procedures are available.

- Because of the circular logic problem, a failure of electrical supplies to the HVAC/ CCW/ESW trains used in the electrical system fault trees was not considered.

- Consequential LOOP is considered. It is assumed that the consequential LOOP probability would be different between plant trips, LOCA events and events likely to lead to a controlled shutdown.

- Recovery of offsite power is considered for transient events in two hours and for RCP seal LOCA events in one hour. Possible recovery for other times is partially credited through modifying the EDG running mission time, which was reduced to 12 hours. SBO DGs mission time was not modified.

- Conservative simplifying assumptions are made when modeling ATWS events; possibility to relieve RCS pressure is not credited for any events which lead to a loss of FW, (e.g., a loss of MFW or a loss of condenser). Exceptions are LOOP events, when the RCP are tripped instantly.

Some of these assumptions are addressed in the sensitivity analysis, Section 19.1.4.1.2.6.

#### 19.1.4.1.2.6 Sensitivity Analysis

A sensitivity analysis was performed to evaluate the impact of a series of modeling assumptions, including most of the above assumptions, on the internal events CDF. The sensitivity results are shown in Table 19.1-15—U.S. EPR Level 1 Internal Events Sensitivity Studies and organized in eleven groups. Table 19.1-15 illustrates the importance of operator actions, LOOP, I&C common cause, and HVAC-related events to the internal event risk. Several insights can be drawn from the sensitivity cases analyzed.

The CDF is very sensitive to HEPs, and it increases over 200 percent if those are set to a 95 percentile value. One operator action in particular, local recovery of cooling to the switchgear room (with a high RAW), increases the CDF by a factor of 20 if it is set to failure.

Cases studying parameters or assumptions related to onsite or offsite electrical power supply show a high sensitivity of the risk. The CDF more than doubles when assumptions crediting LOOP recovery or diversity of EDGs and SBO DGs are changed.

Cases studying assumptions related to preventive maintenance show that if one safety train is taken out of service for the year, the CDF increases by 20 percent. This evaluation should not be considered equivalent to estimating risk from a three-train plant, because some simplifying assumptions are used for the inter-dependent support systems.

The modeling assumption on the I&C software and hardware common cause parameters has significant impact on the CDF. The other modeling assumption, an RCP seal LOCA probability, also shows a non-negligible impact on the CDF.

A very conservative sensitivity case was evaluated to estimate combined effects of different assumptions; many assumptions with the worst effect were combined as presented in the table. The overall result is an increase by approximately 16 times in the CDF to 4E-06/yr, still well below the NRC goal of 1E-04/yr.

The CDF results were not sensitive to the assumption on mission time for long term cooling.

Impact of the design changes not incorporated into the current model is less than 5%.

Table 19.1-15 also shows total contributions from the consequential LOOP events, HVAC related events, and preventive maintenance by analyzing the model with these set to success.

#### 19.1.4.1.2.7 Uncertainty Analysis

Uncertainty on the Level 1 Internal Events PRA results is quantified using the built-in uncertainty analysis capabilities of Risk Spectrum. The results are shown in Figure 19.1-5—U.S. EPR Level 1 Internal Events Uncertainty Analysis Results - Cumulative Distributions for Internal Events CDF. Two distributions are presented, one that only incorporates parametric uncertainty and one that incorporates three cases of modeling uncertainty. The results of parametric uncertainty are summarized below:

- CDF Internal Events Mean Value: 3.5E-07/yr.

- CDF Internal Events 5 percent Value: 3.8E-08/yr.
- CDF Internal Events 95 percent Value: 9.5E-07/yr.

This ninety-fifth percentile CDF value is more than two orders of magnitude below the NRC goal of 1E-04/yr.

As can be seen from the results for parametric uncertainty, the mean value from Monte Carlo simulation is larger than the point estimate. This is due to the "state of knowledge correlation" as defined in the ASME PRA Standards, which is most important for cutsets that contain multiple basic events whose probabilities are based on the same data, particularly when the uncertainty of the parameter value is large. Given the redundancy of the U.S. EPR safety trains, such cutsets are expected in the U.S. EPR PRA model. In this case, in the Monte Carlo sampling approach, the same value is used for each basic event probability, since the "state of knowledge" about the parameter value is the same for each event. This results in a mean value for the joint probability that is larger than the product of the mean values of the event probabilities.

Importance of the redundant equipment and the state-of-knowledge dependencies is limited for the equipment where common cause failures dominate the results. The impact of the redundant equipment is more important in the case where equipment single failures are also significant contributors to the results, like in the cases of the diesel generators. In this evaluation a state-of-knowledge correlation between EDGs and SBODGs was not considered because they belong to the different common cause groups (different vendors, locations, cooling and starting systems, fuel supplies).

More detailed discussion on parametric and modeling uncertainty is as follows:

Parametric uncertainty was quantified by selecting an uncertainty distribution for each input parameter. Distributions mostly applied are Lognormal, Beta and Gamma, as described below for each type of parameter:

- Initiating Events: Uncertainty distributions were obtained from the same source as the mean values. A constrained non-informative distribution (CNI) was used for fire frequencies. A lognormal distribution with an error factor of 5 was used for flooding frequencies. This will be shown in the corresponding sections for internal fire and floods.
- Failure Rates: Uncertainty distributions were obtained from the used data source supplemented by engineering judgement when limited information was available.
- Digital I&C Failure Rates: Lognormal distribution was used, an error factor of five was estimated from upper & lower confidence bounds in TXS documentation. The exception is the software CCF probabilities, which are based on limited information; for their modeling, a CNI distribution was used.

- Common Cause Parameters: Uncertainty parameters were obtained from the same source as CC factors. They were fit to lognormal distribution and only applied to the "beta" factor.

- LOOP Related Basic Events: Gamma distribution for LOOP frequency, with upper and lower bounds, was fit to various LOOP events (consequential LOOPs and LOOP in 24 hours).

- Human Error Probabilities: For pre-accident HEPs, a lognormal distribution with an error factor of 10 was used, as recommended in the ASEP method. For post-accident HEPs, a constrained non-informative prior (Beta) distribution was used, as recommended in the SPAR-H method.

- Various Parameters & Undeveloped Events: Undeveloped events and other various parameters fall into one of two general cases. For parameters where little or no design information or other specific knowledge was used to develop the mean parameter value, a CNI prior (Beta) distribution was used to account for the limited state of knowledge. For parameters where some design information or other knowledge was used to develop the mean parameter value, a lognormal uncertainty distribution was selected. The error factor was selected to provide a reasonable 95th percentile value. In some cases a very small error factor was used to prevent the calculated 95th percentile value from exceeding a value of one.

- Time Related Parameters: For time-related parameters, like preventive maintenance duration (and corresponding unavailability), a beta distribution was used with an error factor of 2.5, consistent with NUREG/CR-6928.

Modeling uncertainty was also specifically treated, but limited to three cases selected to illustrate a specific lack of modeling designs details. These cases are described below:

- CASE 1: This case is based on the uncertainty of success criteria for the number of EFW trains required to cool the plant through MSSVs. The considered spectrum of success criteria included (1) one, (2) two, (3) three, or (4) four out of four EFW pumps required. Success criteria four out of four EFW pumps required is not considered for the LOOP events. Each of the inputs was combined with the estimated probability of that particular success criterion. This uncertainty is modeled because in a design phase, the pump flow curve is not final.

- CASE 2: This case is based on the uncertainty of success criteria for the number of pressurizer safety valves required for a success of feed and bleed. The considered spectrum of success criteria included (1) one, (2) two or (3) three out of three required. Each of the inputs was combined with the estimated probability of that particular success criterion. This uncertainty is modeled because in a design phase, conservative assumptions are made on PSVs "bleeding" capabilities.

- CASE 3: This case is based on the uncertainty of success criteria for recovery of HVAC to SBs: electrical equipment & EFW pump rooms. The considered spectrum of success criteria included: (1) Loss of HVAC will not disable equipment, (2) Operator recovery is required in 4 hours, or (3) Operator recovery

is required in 2 hours. This uncertainty is modeled because in a design phase, not enough information is available to predict room heat-up rates and equipment survivability.

#### 19.1.4.1.2.8 PRA Insights

The U.S. EPR is an active plant, thus CDF is dominated by LOOP-related events (approximately 40 percent). Still, total LOOP CDF is small at <1.5E-07/yr. This small contribution is a result of the U.S. EPR high redundancy in trains and diversity in emergency power supplies.

Loss of cooling trains (CCW/ESW) and seal-LOCA contributions to CDF are less than 10 percent. This relatively small contribution is a result of the U.S. EPR redundancy in the cooling trains and the SSSS design, which contributes to RCP seal reliability.

The top cutsets show that the plant risk is strongly influenced by the performance of support systems – cooling chain, HVAC and electrical. This is because the support systems reflect important dependencies between highly redundant safety systems. These dependencies are discussed in this report, and the most important are summarized below:

- A total loss of an electrical division which supplies running CCW pump, could, without operator intervention, disable the second division through a loss of HVAC.
- Loss of two electrical divisions, combinations 1 & 3, 1 & 4, 2 & 3, or 2 & 4, would disable MSRTS.
- Loss of Division 1 or Division 4 would disable the primary bleed function, a switchover of the CVCS to the IRWST suction, and the SAHRS.

Sensitivity studies did not identify any events where a design change would lead to a significant reduction in the CDF.

Even though Level 1 PRA analysis (at-power, internal events) identifies some hidden dependencies, it shows no outliers and confirms the robustness of the U.S. EPR design.

### 19.1.4.2 Level 2 Internal Events PRA for Operations at Power

#### 19.1.4.2.1 Description of the Level 2 PRA for Operations at Power

##### 19.1.4.2.1.1 Level 2 PRA Methodology

The objective of the Level 2 PRA is to assess the response of the containment and its related systems to potential loads and to assess characteristics of radiological releases from severe core damage accidents. The Level 2 PRA calculates the probability, composition, magnitude, and timing of fission product releases from the plant. It is

performed using a combination of deterministic and probabilistic analyses consisting of the following:

- Integration of the Level 1 and Level 2 analyses through the definition of core damage end states (CDES). The CDESs from Level 1 provide the "initiating events" for the Level 2 analysis.
- Identification of physical phenomena important to containment integrity that could occur during the course of a severe accident.
- Accident progression analysis to support development of the containment event trees and determination of branch probabilities.
- Level 2 systems analysis.
- Development of release category (RC) bins to characterize fission product release to the environment.
- Determination of the source terms for key nuclides for each RC.
- Uncertainty and sensitivity evaluations.

There are two types of interfaces between the Level 1 and Level 2 PRA models, which are the core damage end states and the systems credited in the event trees. Both interfaces are described separately below.

### Core Damage End States

The CDESs are used to bin the core damage accident sequences identified in the Level 1 analysis. The purpose of the CDES bins is to organize the numerous sequences, for which the accident progression will be similar, from Level 1 into categories, to facilitate linking to appropriate CET models in a convenient manner. Each CDES is characterized by a set of attributes that defines similar Level 1 core damage sequences. Refer to Table 19.1-16—Core Damage End States and their Treatment in the CETs for a description of the CDESs used in the Level 1 to Level 2 interface.

### Systems Interface

The systems interface is handled via direct linking of the Level 1 and Level 2 models. The U.S. EPR Level 1 and Level 2 models form a single linked fault and event tree model. Therefore, the inputs to the CET preserve the Level 1 accident sequence information (the status of Level 1 event tree top events), correctly accounting for dependent top events between the Level 1 and Level 2 analyses, without the need for explicit representation in the Level 1 - Level 2 interface. This is important when systems perform a function in both Level 1 and Level 2 analyses, or when different frontline systems have common support systems. In addition to the support systems,

several frontline systems credited in the Level 2 CET model are also credited in the Level 1 PRA model. These systems include:

- PSVs and SADVs–These valves are credited in both Level 1 and Level 2 for primary system depressurization.
- SAHRS–The SAHRS is credited in the Level 1 PRA model for containment heat removal by cooling the IRWST. In the Level 2 PRA Model, SAHRS is credited for core spreading area flooding, active core melt cooling and containment spray functions.
- Safety Injection System–Used for RCS inventory control in the Level 1 and Level 2. In the Level 2 PRA Model, LHSI can prevent RPV failure. LHSI injection through the RHR heat exchanger is also credited for active core melt cooling as a backup to SAHRS.

Refer to Section 19.1.4.2.1.3 for a description of the plant systems that are evaluated in the Level 2 PRA model.

#### 19.1.4.2.1.2 Physical Phenomena

Phenomenological evaluations (PE) are performed to develop the plant specific phenomenological information needed to quantify the CET. The PEs address those severe accident phenomena judged to be significant in determining the eventual outcome of a severe accident. Each PE evaluates the current state of knowledge concerning the phenomenon and considers inputs from available sources, including experiments, industry studies, and plant-specific accident progression analyses.

The PEs develop the probability values and uncertainty distributions used in the Level 2 models. The probability values and uncertainty distributions are input to the basic events used in the CET top events (or supporting fault trees). In some cases, the PEs developed decomposition event trees (DETs), which are small event trees produced and calculated independently of the CET, to produce probability values for use in the CET models. The following PEs have been developed for the U.S. EPR Level 2 PRA:

- Induced rupture of the reactor system pressure boundary
- Fuel coolant interactions.
- In-vessel core recovery.
- Phenomena at vessel failure.
- Hydrogen deflagration, flame acceleration, and deflagration-to-detonation transition (DDT).
- Long-term containment challenges.

Each of these physical phenomena is described below.

### Induced Rupture of the RCS Pressure Boundary

Following core uncovery, natural circulation of superheated steam (and hydrogen) can occur in the reactor vessel and the RCS. Natural circulation is a result of small differences in gas density between various regions in the reactor vessel and the reactor coolant system as a result of heat losses to the structures in each region. Experiments have been performed in the U.S., using a 1/7th scale model of a PWR reactor coolant system. These tests have shown that three distinct natural circulation patterns can be established for an event occurring at high system pressure in this type of system. These circulation patterns are: (1) between the core region and upper plenum of the reactor vessel, (2) between the upper plenum of the reactor vessel and the SG inlet plenum, and (3) between the inlet plenum and outlet plenum of the SG.

The natural circulation flows have been shown to be a strong function of system pressure, with the flow decreasing to nearly zero at pressures below approximately 1700 psi. The natural circulation flows are also quickly disrupted by forced circulation flows, such as the opening of the pressurizer primary depressurization system valves or safety relief valves; however, the natural circulation flow is rapidly reestablished when the forced circulation flow is terminated.

Natural circulation of gases in the reactor system during the core degradation phase is important since it transports heat away from the overheating core, and into the structures of the upper plenum, hot leg and SG tubes. The heat transport has two major effects:

- It slows the heat-up rate of the core, and causes the degradation to proceed more uniformly; however, the heat removal by this process is not large enough to arrest core degradation.

- It causes the heat-up of the reactor system structures in contact with the circulating gas flow. This heat-up can be sufficient in certain cases to cause failure of the reactor coolant system pressure boundary before vessel failure. This potential failure may occur in any part of the system exposed to the heat-up effects of the gas circulation–principally the hot leg, surge line or SG tubes.

For a high pressure transient or SLOCA, residual water present in the crossover legs and in the lower plenum of the reactor vessel is expected to 'block' full loop natural circulation of gases. This is what was observed in experiments. However, in some sequences, clearance of these loop seals could occur, in which case the preferential natural circulation pattern would be that shown in Figure 19.1-6—Natural Circulation Flowpaths in the Primary System (i.e., the 'normal' full loop circulation path). Though less likely, this situation must be considered since it gives rise to higher gas flow rates, and in principle to structural heating rates. For example, in the case of a break in the cold leg, including pump seal leakage, a unidirectional circulation flow, instead of a

counter-current flow, may prevail with resulting increased heat transfer to the structures. As a consequence, higher temperature in the SG tubes will occur, especially if these tubes are not cooled by water from the secondary side.

The probability of primary system structure failure depends on:

- The temperature of the structure–The temperature is higher close to the RPV and considerably lower for the SG tubes.
- The pressure differential across the structure–Because the failure temperature of the material decreases with increasing pressure, pressure difference is higher for the pipes of the hot leg than for the tubes because the pressure on the secondary side could be up to approximately1450 psi.
- The geometric properties of the structure. The SG tubes have a higher thickness relative to their radius compared to large reactor coolant lines. As the stress on a structure scales with quotient of the thickness and the radius of a line, the stress is higher on the MCL than on the SG tubes for the same pressure difference.
- The material properties of the structure. Different steels are used for the different parts of the reactor coolant system, each of which has a different response to high stresses.
- The duration of high temperature–The time period corresponds to the period from the beginning of core heat-up until core slumping. Under certain circumstances a late phase increase of structural temperature may occur just before vessel failure.

Induced RCS structure failure is important for two reasons:

- Failure of the SG tubes–SG tube failure may lead to containment bypass in case the SG cannot be isolated and a closure of the main steam valves is not possible. Additionally, the closure of the main steam valves may fail, as they are not designed for the temperature loads following SG tube failure. This failure mode is of most concern in the Level 2 PRA, because it has the potential for a large early release of fission products. The Level 2 PRA models a single probability representing one or more SG tube ruptures.
- Failure of the hot leg close to the RPV (hot leg nozzle) or surge line (surge line nozzle)–RCS piping failure prior to reactor vessel failure can have a substantial effect on other in-vessel and ex-vessel degraded core phenomena. The sudden pressure decrease will lead to flashing of the water in the bottom head of the reactor which passes through the overheated core or by the discharge of accumulator water onto the overheated core. This may lead to an increase of hydrogen production. Further, the reactor coolant system pressure at the time of reactor vessel failure will be close to near the containment pressure, eliminating the potential for high pressure reactor vessel failure events (e.g., vessel rocketing, melt dispersion and direct containment heating). Also, the fission product releases to the containment are substantially increased due to the creation of a large

blowdown from the RCS about the same time the fission product releases from the core.

It is important to note that the failure modes are mutually exclusive when considering multiple SG tube ruptures. Thus, once a failure occurs at any location, the resulting depressurization and reduction in stress on other components precludes subsequent failures.

This phenomenological evaluation uses analyses performed with MAAP4.0.7 to investigate various high pressure accident sequences, and to evaluate the sensitivity of the induced rupture phenomena to various key parameters, including:

- Impact of natural circulation flow rate.
- Rupture location.
- Impact of different initiators.
- Impact of degraded tubes.
- Impact of SG pressure.
- Impact of seal leaks and SLOCAs and behavior of loop seals.
- Impact of materials/creep correlation fitting parameters.

### Probabilistic Evaluation of Induced Rupture

The Level 2 PRA provides a probabilistic evaluation of the potential for rupture of either the RCS loop or the SG tubes for applicable (high pressure) situations. The probabilistic evaluation is performed by developing uncertainty distributions for the key uncertain parameters, and performing Monte Carlo simulations to determine the predicted times to hot leg, SG tube, and vessel rupture.

This CET top event is only evaluated for cases where the primary system has not been depressurized using the dedicated severe accident depressurization valves. The probability of depressurization failure is evaluated separately in the Level 2 study. For cases with no primary depressurization via the pressurizer, the strongest sensitivity observed is to SG pressure. If the SGs remain pressurized, there is no risk of tube failure for any case analyzed. Hot leg rupture is, however, highly likely (0.94 - 1.00 probability for different cases). The location of hot leg rupture is predicted to be at the nozzle near the hot leg pipe weld. This is important for some sequences because it leads to a break flow discharge into the reactor pit. If SGs are depressurized, either due to failure of one or more secondary relief or safety valves, or due to operator action, the situation is more severe, because SG tube failure is predicted to occur first with a probability of up to 0.38 for transients and up to 0.79 for sequences involving seal failure or small LOCAs.

### Fuel Coolant Interactions

The key fuel coolant interaction is steam explosion. Steam explosions may occur, and are potentially significant, in both the ex-vessel and in-vessel phases of a nuclear reactor accident. In-vessel steam explosions are postulated as potentially failing the upper or lower head of the reactor pressure vessel. A possible consequence of upper head failure, if sufficiently energetic, is containment failure. Ex-vessel steam explosions may cause local damage to internal containment structures.

The initial condition from which a steam explosion process would start in a nuclear reactor accident scenario is at core relocation following a core melt. Core melt can occur at high or low RCS pressure. Eventually, following extensive core melting and slumping, a large mass of molten material falls into the lower head, where water is present. This is the in-vessel steam explosion scenario. For the ex-vessel scenario the initial condition would be a pour of molten corium into an ex-vessel water pool located either in the reactor pit or in the spreading area.

When hot molten liquid enters into a volatile coolant, explosive interactions are a possibility. There is general agreement that the steam explosion process can be broken down into a series of sequential phases. These phases include: (1) initial course mixing phase (pre-mixing), (2) trigger phase, (3) detonation propagation phase and (4) hydrodynamic expansion phase. These four phases are described below.

1. Initial Course Mixing Phase: During the initial premixing phase, the molten liquid entering the coolant undergoes fragmentation (i.e., vapor generation causes breakup of the jet or drops into smaller diameter drops and depends on breakup due either to acceleration or velocity difference between molten material and coolant). The breakup increases the surface area for heat transfer and, therefore, steam generation increases. However, a quasi-stable state is reached because steam can settle into a stable blanket around the fragments and the fuel cooling (and, therefore, steam production) rate is lowered by this isolating vapor film.

2. Triggering Phase: Triggering starts when the quasi-stable vapor film collapses due to local perturbation. This allows (liquid) water to come into (closer) contact with the molten fuel. Heat transfer is thus enhanced and the local steam production rate and local steam velocity increases. The next phase, detonation propagation, is entered.

3. Detonation Propagation Phase: In the detonation propagation phase, sharp micro-interaction zones propagate through the mixing zone. The process escalates as the fuel is further fragmented, meaning that there is a rapid increase in the surface area for heat transfer and, therefore, further increased steam production. Intensive steam generation could generate shock waves.

4. Hydrodynamic Expansion Phase: In the expansion phase, thermal energy is converted into mechanical energy which acts on its surroundings (upper head, lower head, internal or ex-vessel structures). This leads either to missile

generation or lower head failure in the in-vessel scenario (a slug of water becomes a high-energy missile which transfers its energy to the upper head and then to the containment) or to loads on internal containment structures (possibly dynamic loads) in the ex-vessel scenario.

### Probabilistic Evaluation of Fuel Coolant Interactions

The phenomenological evaluation performed for steam explosions addresses in-vessel and ex-vessel steam explosions. The evaluations involve the use of Monte Carlo simulations.

#### *In-Vessel Steam Explosion*

For the in-vessel scenario, the probabilistic evaluation centers on a comparison of steam explosion loads in terms of the mechanical energy generated to a threshold above which the energy is sufficient to cause containment failure. Both the load and the threshold are treated as uncertain parameters, although it was conservatively assumed that any load sufficient to fail the RPV upper head would fail the containment. The probabilistic evaluation was performed for two scenarios, these being (1) core melt at low pressure, and (2) core melt at high pressure. These two scenarios were evaluated separately because triggering is generally considered more likely at low pressure, whereas the conversion ratio of thermal to mechanical energy is expected to be higher at high pressure.

The loads resulting from an in-vessel steam explosion were calculated by multiplication of the following factors to give the resulting energy of a molten slug potentially affecting the upper head:

1. The total mass of the core.
2. The fraction of the core material in the lower head that participates in pre-mixing.
3. The thermal energy stored in the core materials per unit mass of core. (It is assumed that the composition of the molten core in the lower plenum maintains the same proportions of materials in the proportions present in the core as whole.)
4. The conversion ratio from thermal to mechanical energy.
5. The fraction of the mechanical energy that is transmitted to the slug. (There are expected to be losses due to venting around the slug during the expansion phase.)

Each of the above factors (except the total core mass which was modeled by a single value) was assessed using a probability distribution. The probability distributions were generated by review of various references containing information and assessments of steam explosions (mostly non-probabilistic). The distributions generated in this process are based on an assessment of the likelihood ranges for each parameter based on the assessed knowledge base. The use of Monte Carlo simulations enables the

distributions on the above basic parameters to be propagated through the multiplicative model described above to give a probability distribution for the load on the upper head.

The strength of the upper head (stated in energy load terms) was based on generic estimates of this strength. The median value used for the strength of the upper head was 1GJ. This value was treated as an uncertain parameter and assigned a probability distribution, centered on 1GJ, to model this uncertainty.

The load and strength distributions (as discussed previously) were compared in the Monte Carlo simulation to generate the probability of containment failure given a steam explosion occurring in-vessel (for low-pressure and high-pressure scenarios). The final result for in-vessel steam explosion leading to containment failure also factors in the probability of a steam explosion occurring, which is not modeled by the factors (1) to (5) described above. The assessment generated the following approximate values for the probability of in-vessel steam explosion failing containment:

A. A value of 8.6E-04 for a high-pressure core melt scenario.

B. A value of 5.6E-06 for a low-pressure core melt scenario.

A further possible consequence of an in-vessel steam explosion that was investigated is lower head failure. Where lower head failure is assessed as occurring, damage in the reactor pit is assumed without taking credit for the distribution of energy loads the pit structures would actually experience or the capacity of the pit to withstand these. This approach is somewhat conservative. It should also be noted that the CET modeling assumes that the impact of pit damage on the progression of the postulated severe accident would be early release of melt from the pit into the spreading area. Since such a release is not the design pathway for the U. S. EPR melt stabilization approach, it is conservatively assumed that MCCI would not be prevented in such a case.

The assessment of the lower head failure probability closely followed the procedure outlined above for the upper head failure (leading to containment failure). The difference between the two evaluations is that the factor for the fraction of the mechanical energy that is transmitted to the slug that impacts the upper head was not applied for the lower head evaluation. Rather 100 percent of the mechanical energy was assumed to impact the lower head. This assumption is conservative.

The results of the probabilistic evaluation of a steam explosion causing failure of the lower head were approximately as follows:

- A value of 8.4E-04 for a high pressure core melt scenario.
- A value of 2.5E-05 for a low pressure core melt scenario.

*Ex-Vessel Steam Explosion*

Ex-vessel steam explosions were evaluated for scenarios in which molten corium is released from the vessel into a stable water pool in the reactor pit cavity. An evaluation of the relevant RCS failure modes concluded that only creep-induced hot leg rupture at the RV nozzle could lead to a stable water pool in the reactor pit at the time of RV failure. A probabilistic evaluation of the consequences of an ex-vessel steam explosion is performed for that specific scenario.

An important parameter for this assessment is the RV rupture location. The probabilistic evaluation of vessel failure described later in this sub-section concluded that among the possible RV failure modes, the lateral failure is the most likely failure location. This is due to the focusing effect at the junction of the oxidic and metallic layers of the corium pool, leading to high heat densities in proximity of the RV wall. Based on this evaluation it was concluded that:

- The lateral failure mode represents 94 percent of the RV failure modes. Steam explosion loads from a lateral melt outflow could challenge the structural integrity of the pit wall.

- The central failure scenario represents 5 percent of the RV failure modes. Steam explosion loads from a central melt outflow could fail the melt plug.

The remaining one percent represents complete circumferential failure modes that have no impact on steam explosion scenarios.

The impact of an ex-vessel steam explosion on the pit wall and the melt plug was evaluated through a comparison of the dynamic pressure loads on these structures to their respective strengths. This evaluation was performed in two steps; first the best estimate dynamic loads resulting from an ex-vessel steam explosion under realistic conditions were estimated, then these loads were compared to the probability density function representing the fragility of the pit structure.

The dynamic pressure loads used in this evaluation are the result of a deterministic analysis performed by the University of Stuttgart Institute for Nuclear Technology and Energy Systems (IKE). To envelop the range of realistic scenarios, the analysis used different sets of initial conditions such as the leak location and size, flow rate, melt temperature and composition, and water pool depth. The resulting pressure loads reached a local maximum of 5400 psi on the pit wall with a metallic melt composition and about 6400 psi with an oxidic melt composition and a maximum of 1300 psi on the melt plug with an oxidic melt composition.

The fragility curves used in this evaluation are the result of a structural evaluation of the pit wall and the melt plug responses to the steam explosion loads evaluated above. This evaluation concluded that the maximum steam explosion loads that the pit wall

and the melt plug withstand with a zero probability of failure are about 2.3E+04 psi and 1200 psi, respectively.

The comparison of the pressure loads against the pit wall and melt plug structural strengths was accomplished through a Monte Carlo sampling and resulted in a conditional probability of failure for the pit wall (given a lateral leak) and for the melt plug (given a central leak).

The probabilities of failures of the pit wall and the melt plug are then weighted by their respective probabilities of occurrence (94 percent and 5 percent). This yields a total failure probability of the pit of approximately 2E-03. A value of 5E-03 is conservatively used as an upper bound instead.

The CET logic reflects the conditions necessary for steam explosion by applying the calculated probability of pit failure only to core damage sequences depressurized by hot leg rupture prior to RV failure.

An analysis of the impact of the reactor pit failure on the severe accident progression has been performed in light of the results of the above analysis that identified the melt plug as the weakest structure in the pit. The purpose of the melt plug sacrificial material is to provide temporary retention of the melt before the transfer to the corium spreading area. Without a retention period, this release would create undefined and potentially unfavorable conditions for subsequent melt spreading. A conservative approach has been adopted in the Level 2 PRA which assumes that an early release of the melt will result in failure of melt stabilization ex-vessel and subsequent molten core concrete interaction (MCCI) with a probability of one.

### In-Vessel Core Recovery

The principal cause of core heat-up in a severe accident is the lack of cooling water. Depending on the time when safety injection (SI) is recovered, the accident progression can be stopped or delayed. Thus the SI recovery time has a direct impact on the RCS and containment conditions after injection is initiated to a degraded core. Depending on the injection flow rate, the hot corium can either be quenched or not. If the flow rate is too low, the accident progression will be delayed, but reactor vessel failure is not prevented.

The effects of the re-flooding of a damaged core include an enhanced oxidation leading to temperature escalation and high hydrogen peaks. Flooding a damaged core can also lead to the formation of a debris bed due to thermal shock collapse of the upper fuel rods located above the core molten pool, as with the Three Mile Island (TMI) accident.

A severe accident starts with insufficient cooling conditions in the core followed by continuous heat-up of the fuel. The heat transferred from the fuel rods to the steam is not sufficient to remove all decay heat, but is able to heat-up the steam close to the

highest temperature of the fuel rods that normally occurs at the top of the core. Core exit temperature of the steam is therefore a measure of the early accident progression and is therefore used as a criterion for dedicated bleed (approximately 1200°F).

To mitigate further accident progression, in particular the consequences of a high pressure core melt scenario, the RCS depressurization strategy aims at opening the depressurization valves to allow injection of available safety injection and accumulators before the start of core melt. If the depressurization and the injection of the SIS accumulator or the LHSI are not successful, fuel element degradation will continue.

The exothermic reaction of the superheated steam with the Zirconium (Zr) of the fuel rods produces hydrogen, which is transported with the remaining steam through the RCS into the containment. The production rate is governed by the diffusion of the steam through the boundary layer of hydrogen that establishes around the fuel rods and through the oxidic layer to the unoxidized Zr. When the temperature has reached approximately 2200°F the oxidation reaction becomes significant and dominates the heat-up of the fuel, which is significantly accelerated because the reaction is strongly exothermic. The availability of steam influences the production rate. The rate can be limited in the late phase, when water level and heat transferred to the water are low (steam starvation) and, on the other hand, enhanced in case of re-flood, particularly when the core is already exposed to high temperature.

The core melt onset starts with eutectic interactions between core materials, relocation of cladding, structural materials and fuel with formation of blockages near the bottom of the core forming of a molten pool. Generic behavior with natural convection in a volumetrically heated molten pool leads to a first sideward relocation through the heavy reflector to the lower head, which occurs earlier than a downward relocation through the thick core support plate.

The interaction of the melt with water in the lower plenum could result in mechanical loads on the RPV and, in case of its failure, also on the containment shell. Dispersion of (or a part of) the melt within the RCS could also occur. As a result of the latter process, heat sources are distributed along the RCS piping with potential consequence to thermal failure and also to re-vaporization of deposited fission products.

Corium heat up in the lower plenum after the first relocation into the water consists of the dry out of debris which re-melts, and which, in combination with the gradually relocating corium, forms a molten pool involving development of crusts on the top and along the vessel wall. If no water injection is available, this debris bed at the bottom of the RPV will possibly grow to a large size melt pool. Convection within this pool will transport heat to the top of the pool with the expected consequence of a lateral failure of the RPV at an elevation close to the surface of the oxidic pool. This failure mode competes with (local) failure at the bottom of the vessel, where, however, heat fluxes

are much lower. In this case a high pressure local failure of the RPV, possibly before a large pool of molten material has developed, can be postulated.

Vessel failure can be due to several possible mechanisms:

- The molten metal located on top of the oxidic melt, which thermally attacks and weakens the vessel wall and causes failure due to the internal residual pressure.
- Weight of the corium and thermal loads result in creep rupture.
- A jet impingement occurring in the relocation phase may cause localized ablation of the lower head.

### Probabilistic Evaluation of In-Vessel Core Recovery

The approach used in the Level 2 PRA considers the beginning of the severe accident as the on-set of core heat-up and that the end of the in-vessel accident progression occurs at vessel failure.

The probability to successfully arrest the core in vessel, $P_{success}$, is a product of the probability to quench the core $P_{quench}$ from a thermodynamic point of view multiplied by the probability to succeed in the quenching as per experimental study:

$$P_{success} = P_{quench} * P_{recovery}$$

where:

$P_{quench}$ = probability for the amount of water brought to the degraded core to remove the decay heat, the stored energy, the vaporization energy and the oxidation energy when applicable at a given time t.

$P_{recovery}$ = conditional probability to quench the corium at a given time t, given sufficient water for heat removal.

The process of quenching the core begins at the time when primary depressurization is initiated. The time that it takes to quench the core $t_{quench}$, is calculated using a spreadsheet analysis that uses a mass and energy balance to determine how long it will take to quench the core. This spreadsheet analysis uses a single LHSI pump as the source of injection, and uses the PDSVs as the mode of depressurization. The analysis evaluates this energy balance over a range of times during each phase of the event, and calculates $P_{success}$ for each of these times.

In-vessel recovery is evaluated as follows:

- Phase 1: Core Heat-up to Core Melt Onset
  During this phase the core is in a coolable geometry, and the injection in-vessel shall recover the core cooling in most cases. During this phase there is no molten

core material. Once heat removal exceeds heat generation, the core will begin to cool and maintain a coolable geometry. The maximum quenching mission time is considered to be 24 hours.

- If the calculated time to quench the core is less than 24 hours, then $P_{recovery} = 1$, otherwise $P_{recovery} = 0$.

- In all cases $P_{quench}$ is the value of the average of the values of $P_{quench}$ at the end of the depressurization and the end of quench.

- Phase 2: Core Melt Onset to Relocation into the Lower Head of the Vessel
  During this phase, the corium is above the support plate. Water is assumed to be available in the lower plenum but not in contact with the hot material. The probability to successfully restore core cooling based on the injection in-vessel at a given time is a function of the quenching probability, but also depends on the availability of the volume of water required to quench the hot materials.

- During this phase core geometry changes may continue while the core material is molten. If heat removal exceeds heat input during this phase, the time to relocation could be extended. However, the extension of this time is conservatively ignored and a limiting time is calculated as the time from depressurization to the end of the phase.

- If the time needed to quench the core is less than the time to the end of Phase 2, then $P_{recovery} = 1$ and $P_{quench}$ is the average of the values of $P_{quench}$ at the end of the depressurization and at the end of the quench.

- If the calculated time needed to quench the core is greater than the time to the end of Phase 2 but less than 24 hours, then $P_{recovery} = 1$ and $P_{quench}$ takes an average value between reference $P_{quench}$ at the end of the depressurization and at the end of quenching, with a minimum value of 0.1. If the calculated time needed to quench is larger than 24 hour, then $P_{recovery} = 0$ and $P_{quench} = 0.1$.

Phase 3: Relocation into the Lower Head of the Vessel to Vessel Failure
At the start of this phase, the corium will fall into the water, which experiences a boiling off phase. This event depends on the amount of water present in the lower plenum. If hot material is quenched by the water in the lower plenum, the probability to successfully restore core cooling based on the injection in-vessel at this time and until the corium reheats is 100 percent. After boil off, the corium will again eventually melt and the same evaluation as in Phase 2 is performed, except that the oxidation rate of the Zr is neglected, and the water required to refill the core is reduced. The presence of a molten pool at the bottom of the vessel will increase the probability of failure to recover the core.

### Phenomena at Vessel Failure

The phenomenological assessment performed considered the following phenomena at vessel failure:

- Overpressurization of the reactor pit due to release of gases from the vessel at vessel failure (high RCS pressure).

- Rocketing of the vessel, due to a net upward force onto the vessel when it fails at high RCS pressure.

- Direct containment heating (DCH) due to entrainment of debris into the main containment volumes with concurrent rapid heat transfer from the debris to the containment atmosphere and generation and combustion of hydrogen following vessel failure at high pressure.

An additional consideration was to assess the likely failure modes of the vessel (in particular the size of the failure) to the extent these can impact downstream events in the CET, including those events assessed in this phenomenological assessment.

The events described above were considered for inclusion into the CET since they have the potential to lead to containment failure and an associated release of radionuclides or otherwise impact the accident progression. The overpressurization of the reactor pit may lead to damage that potentially affects the subsequent accident progression (i.e., retention, spreading and cooling of corium ex-vessel).

An outline of the phenomenology associated with each of the items introduced above is presented in the following sub-sections:

### *Vessel Failure Modes*

The different vessel failure modes that are considered to be possible following a core damage accident are:

1. An off-center tear of the lower head.

2. A rupture of the lower head at its lowest point.

3. An ablation failure of the lower head due to jet impingement.

4. A complete circumferential failure of the lower head.

The first failure mode noted, an off-center tear of the lower head, has been seen in the EU FOREVER experiments (see, for example, Reference 31) and is anticipated due to high heat loads expected to result at the top of corium pools in the lower head. If the corium relocates to the lower head without a prompt jet-impingement failure (discussed later), high heat loads can arise at the top of the pool if (a) the melt constituents are well mixed and there is strong convection within the pool, or (b) the metallic and oxide phases separate when the corium is in the lower head, in which case the upper metal layer could lead to a “focusing” effect whereby the highest heat fluxes occur at the top of the melt pool.

The second failure mode noted, lower head rupture, could occur if the pool in the lower head forms a static, but mixed, configuration. In this case, the highest heat fluxes will occur at the base of the pool since there is a radiation heat removal mechanism at the pool surface. This pool configuration is generally considered much less likely than convective or stratified behavior.

The third failure mode noted, ablation failure due to jet impingement, may occur as a result of a sideways relocation mode or a bottom failure of the crust in which a "jet" of molten debris is generated, leading to jet impingement and an ablation failure. Such a failure would be prompt, but localized. One mechanism by which this relocation mode could occur is a side breach of the debris crust layer which forms during the in-vessel melt progression, opening a path through the baffle (heavy reflector for the U.S. EPR design) and allowing molten material to reach the lower head. A vertical pour with a jet is also possible; in this case, it is postulated that the crust failure occurs at the base, with a small opening, leading to a debris jet impinging on the lower head wall. Wall ablation is postulated to occur due to enhanced convective heating during the pour process. This failure mode is unlikely because of the narrow range of jet diameters over which it might be postulated.

The fourth failure mode noted, complete circumferential failure of the lower head, could be postulated if the vessel failure occurs at the top of a corium pool in the lower head, either in the convective mixing scenario or the stratified melt scenario. A circumferential failure might be postulated either (a) due to a situation with highly symmetric head loads and vessel wall strength, or (b) following a localized tear at the top of the pool which subsequently propagates (rapidly) around the lower head. This failure mode has not been observed experimentally, even though convective pools have been studied and the tear failure mode has been observed. It is considered of negligible probability if the vessel fails by jet impingement and ablation, since jet impingement is expected to lead to the smallest, most localized failure.

*Overpressurization of the Reactor Pit*

This phenomenon may occur when the blowdown rate of the vessel exceeds the venting capability of the reactor pit at a relatively low pressure (i.e., gases from the failed RPV discharge rapidly into the pit and the flow paths out of the pit are not sufficiently large for the blowdown gases to exit the cavity without resulting in pressurization). The pressurization of the pit is expected to be more likely for larger failure sizes of the RPV, since this would imply a more rapid inflow of gases into the pit which is more likely to overwhelm the pressure relief capacity of flow paths out of the pit. Additionally, the pressure increase in the pit will be greatly enhanced if one or more of the reactor coolant lines fail due to the forces upon the RPV.

The potential consequences of overpressurization of the reactor pit are expected to be structural damage. The potential structural damage is expected to be more likely to

result in an impact on downstream nodes in the containment event tree than to result in direct containment failure. A possible example of a downstream impact would be impact on severe accident melt stabilization.

*Rocketing of the Vessel*

Rocketing of the vessel was originally proposed as a failure mechanism for the containment in the WASH-1400 study. Vessel rocketing is possible if the upward forces on the vessel accelerate the vessel enough to exceed the hold-down capability of the vessel supports to cause a failure of the reactor coolant lines. If this is the case, the vessel will be accelerated upwards and become an energetic missile posing a potential threat to the containment.

*Direct Containment Heating*

The postulated sequence of events for direct containment heating include:

1. The RPV fails at high pressure.

2. Molten core material ($UO_2$ and zircaloy) and molten steel are forced out of the vessel at high pressure and this material becomes highly fragmented into small particles.

3. There is therefore a large surface area for interactions and energy exchange with the containment atmosphere.

4. Heat from the fragmented debris is transferred to the containment atmosphere, pre-existing hydrogen burns and more hydrogen is generated and burns due to the chemical reactions of zircaloy and steel with steam in the containment.

5. The resultant energy input into the containment atmosphere results in a rapid pressure increase, and possible containment failure.

More recent experimental and modeling investigations have tended to result in lower estimates of the peak pressures from DCH than earlier evaluations. The main reasons have been the mitigating influence of lower containment compartments where debris may be retained and limitations on the interaction zone inside the containment for heat exchange and chemical reactions. Reference 32 presents a resolution of the DCH issue for large dry containment design U.S. PWRs. While resolution is formally stated as meaning that the conditional containment failure probability given a core damage accident is less than 0.1, the results in Reference 32 strongly suggest large margins between the containment strengths and the potential loads from DCH. This implies that, from a Level 2 PRA perspective, containment failure probabilities from DCH could be relatively small.

## Probabilistic Evaluation of Vessel Failure

### *Vessel Failure Modes*

The probabilistic evaluation of vessel failure modes was performed by developing a decomposition event tree containing the following headers:

- Location of crust breach - side or base: This considers two mechanisms of melt relocation:
  - A side jet/pour where the breaching of the debris crust layer which forms during the in-vessel melt progression occurs at the side, and a path opens through the heavy reflector for the U.S. EPR design;
  - A vertical jet/pour, in which it is postulated that the crust failure occurs at the base. The first mechanism was evaluated as the more probable of the two mechanisms.
- Prompt vessel wall failure by jet impingement: This considers jet impingement of the vessel wall which could result in enhanced heat transfer from the jet to the wall location and thus in rapid wall ablation and localized prompt failure. Based on a review of recent investigations, this vessel failure mode was evaluated as an unlikely scenario. It was also noted that in the case of a base crust penetration, the melt will either fall into water (leading to possible break-up of the jet) or if not, the jet will eventually be submerged in the melt pool which accumulates in the lower plenum. Thus, prolonged direct contact of the jet and the wall is more likely if a side failure of the crust was evaluated under the preceding header, leading to a reduction in the assigned probability for a base failure mode.
- Pool state: This considers which of the following classes of pool would be expected to form in the lower header following relocation:
  - Phase separation and metal layer focusing of heat towards the top of the pool
  - Fully mixed convective pool, leading to higher heat loads at the top of the pool due to convective flows.
  - A fully mixed static pool, with highest heat loads at the base of the vessel. Of the three configurations, the fully mixed static pool was assigned the lowest probability, implying that it was judged to be more likely that the highest heat loads would be at the top of the pool.
- Vessel failure: This considers the mode of wall failure and breach area. Specifically, the following failure modes and characteristics were addressed:
  - “Small base” or “Small base/side”, local failure modes due to jet impingement and ablation of the wall (the base/side variant was used for the case that the jet impingement results from a sideways relocation);

- "Base", a localized failure due to formation of fully mixed static pool, expected at the bottom center of the lower head, and assigned probability 1.0 conditional on formation of fully mixed static pool;

- "Side tear", a failure mode where the initial wall breach is near the top of a relocated debris bed, but where it is not postulated that the entire circumference of the wall fails simultaneously;

- Complete breach of vessel (CBV), a rapid gross cross-sectional failure of the lower head, which applies only to convective pool or separated phase situations, and for which creep strain is postulated to be exactly equal all around the vessel wall. When failure is postulated to occur, the entire vessel head is instantaneously detached (this failure mode is considered unlikely since the expected presence of non-uniformities in the melt, and also possibly the wall material, would favor an initial localized failure, as seen experimentally).

The outcomes of the DET were classified according to failure mode of the RPV, resulting in the following overall outcomes:

| Failure Diameter | Failure Mode | Probability |
|---|---|---|
| 0.1m | Small base, Small base/side | 0.04 |
| 0.1m – 0.5m | Base | 0.048 |
| 0.5m – 1.0m | Side tear | 0.902 |
| 4.87m | CBV | 0.010 |

*Direct Containment Heating*

The probabilistic evaluation of DCH consisted of the development of a model for the DCH pressure rise, based on the NUREG/CR-6338 TCE model together with the use of dispersion factors based on experimental information, to model the specific dispersion properties of the EPR reactor pit. This model of the DCH pressure rise was evaluated probabilistically using a Monte Carlo simulation to generate a probability distribution representing the uncertainty on the DCH pressure rise. This probability distribution was compared to the EPR containment fragility curve to generate an overall probability of failure of the containment by DCH, given a high pressure vessel failure.

The adaptation of the NUREG/CR-6338 DCH loads was based on the pressure rises predicted by the NUREG model compared to the initial or baseline pressure conditions. Initial pressure conditions for the phenomenological analysis of DCH for the EPR were taken from U.S. EPR MAAP analyses, to ensure EPR specific initial conditions.

The other parameters accounted for in calculating the DCH pressure rise for the EPR were:

- Dispersion.
- Zircaloy mass (total in core).
- Steel mass in lower plenum at vessel failure.
- $UO_2$ Mass (total in core).
- Coherence Multiplier.
- Containment Volume.

The above parameters were chosen since a review suggested that these were the main parameters that varied between the different plants and were also judged qualitatively to be those most likely to significantly influence the DCH loads.

The probabilistic evaluation of DCH concluded that probability of containment failure following a DCH event with the vessel failing at high pressure is 5.5E-04.

*Cavity Overpressure*

The probabilistic evaluation of cavity overpressure centered on the comparison of potential loads on the cavity for a range of vessel failure sizes with the structural capacity of the cavity. The loads (overpressure) were estimated using a series of MAAP runs for the vessel failure sizes evaluated in the vessel failure modes DET described above.

Based on the above analyses, and an assessment of the pressure capability of the cavity, cavity overpressure following high pressure vessel failure was evaluated very unlikely. As described in the subchapter on Ex-Vessel Steam Explosion, the melt plug and the pit walls will withstand maximum explosion loads of approximately 1200 psi, which is much higher than the calculated pit pressure except in the case of a CBV. For this reason, failure of the pit walls as a result of high pressure vessel failure is eliminated as a probabilistically relevant phenomenon. Failure of the melt plug in the case of CVB can lead to the failure of melt stabilization and subsequent molten core concrete interaction (MCCI).

*Vessel Rocketing*

Rocketing of the vessel was assessed by use of the so-called “Rocket equation” which evaluates the total rocketing upward force as the sum of a momentum term (due to the exiting flow) and a pressure term (due to the net upwards pressure on the vessel with a hole in the lower part of the vessel, plus the upward pressure on the vessel from the pressure in the pit). Based on this assessment, together with an assessment of the total

hold-down force on the vessel (due to the cold legs), rocketing was discounted for small hole sizes (0.1m and 0.5m diameter breaches) on the basis that the restraining forces exceed the maximum possible rocket thrust force in these cases. A sensitivity study was performed for a 1.5m hole size. In this case, it was also seen that the rocketing forces would not exceed the hold-down forces, although the calculated margin was lower. It is noted that the assumed 1.5m hole size is larger than the maximum hole size for the side tear failure mode (0.5 - 1.0 m hole size). Additionally, the location of the side tear failure mode makes rocketing unlikely, since forces onto the vessel would be directed mainly sideways, not upwards. For the complete circumferential rupture of the vessel (CBV case), which is assessed as an unlikely failure mode, with a probability of 0.01 in high pressure sequences, rocketing is expected, as the restraining forces are exceeded by nearly an order of magnitude. The CET models assume containment failure in this case.

### Hydrogen Phenomena Description

A deflagration is a combustion form in which the combustion front travels at sub-sonic speed relative to the unburned gas. If the flame speed is small compared to the speed of sound, the pressure rise is expected to be uniform throughout the containment volume and the loads will be quasi-static in character. Loads from deflagration can be estimated by (1) assessing the heat input to the containment atmosphere arising from combustion (based on heats of reaction) and (2) evaluating the final peak pressure of the mixture at the resulting gas temperature, based on the thermal properties of the constituent gases and the heat input. When this calculation is based on assumptions of complete combustion of all reacting gases and no heat losses to structures (etc), it is referred to as an Adiabatic Isochoric Complete Combustion (AICC) calculation. Codes such as MAAP and MELCOR (refer to Reference 3) also include models where losses are taken into account and deflagrations are allowed to propagate through different volumes in the containment, tending to lead to lower calculated pressure rises than those arising from the AICC method, which can be seen as an upper bound for deflagrations.

Detonation is a form of combustion where the flame travels at supersonic speed relative to the unburned gas, typically exceeding 2000 mph. In this case, a shock wave is formed, and, depending on the time constants of the containment structure and the detonation pulse, the structural load is determined either by the peak pressure or the impulse of the detonation pressure wave, or by a combination of these two items.

The peak pressure from a detonation is expected to be in the range of 12 to 20 times the base containment pressure. This implies high containment failure probabilities given the occurrence of a detonation. The effective pressure (i.e., the static pressure that would give a load equivalent to the dynamic detonation load) due a deflagration-to-detonation transition is in the region of 1.5 to 2 times the pressure that would arise from a slow deflagration. Nuclear power plant (NPP) containment structural response

natural frequencies are in the range 5-25 (or 5-50) Hz (i.e., characteristic times of 20-200 ms), with the effective pressure factor quoted being consistent with this frequency range.

An accelerated flame can also lead to structural loads on short time scales compared to the structural response time and therefore to higher effective pressures. In the range of NPP containment structural response frequencies, the effective pressure from an accelerated flame is in the region of 1.5 to 2 times the pressure that would arise from a slow deflagration (i.e., a similar ratio to that obtained for the case of deflagration-to-detonation transition). Flame acceleration is essentially a pre-condition for DDT since direct initiation of a detonation is considered very unlikely. Occurrence of an accelerated flame, followed by DDT is a more likely scenario in a NPP containment, given an atmospheric mixture that allows flame acceleration in a large enough part of the containment to reach flame speeds that exceed the local speed of sound.

Based on the above discussion, it can be seen that deflagration, flame acceleration and DDT should all be considered as potentially unfavorable loadings for the containment of an NPP during a severe accident. This is different to the historical position regarding destructive failure modes, where, in the past, only DDT was considered a potential containment challenge. Recent references are however clear that the loads from fast flames may approach or even exceed those from DDT.

### Probabilistic Evaluation of Hydrogen Phenomena

The phenomenological assessments performed for containment loads derived from hydrogen combustion processes addressed containment failure due to overpressure from hydrogen deflagration or because of dynamic loads from "destructive" combustion modes (flame acceleration or deflagration-to-detonation transition, DDT).

#### *Deflagrations*

The deflagration assessment was performed on a global basis, based on the global AICC pressure. The main parameters considered in the global deflagration assessment were as follows:

- In-vessel hydrogen production.
- Ex-vessel hydrogen production.
- Steam concentration.

Consumption of hydrogen and oxygen by recombiners was accounted for by reference to the MAAP analyses performed. Consumption of hydrogen by random hydrogen burns at lower concentrations was conservatively ignored. In-vessel hydrogen production was assessed as being in the range 30 percent to 65.5 percent equivalent zircaloy oxidation.

This assessment of deflagrations in the U.S. EPR containment identified three scenarios as having non-zero probabilities of containment failure:

- Deflagration during the in-vessel phase of a high pressure core damage transient, resulting in a probability of containment failure of 2.0E-06.
- Deflagration during the in-vessel phase of a high pressure core damage transient following a hot leg rupture and the consequent release of hydrogen into the containment. The resulting probability of containment failure is 2.8E-04.
- Deflagration at vessel failure of a high pressure core damage scenario results in a probability of containment failure of 1.5E-03.

The above results represent the total containment failure from rupture and leak and were based on bounding assessments in terms of hydrogen and steam conditions (i.e., top of range zircaloy oxidation and high baseline pressures from steam concentration.

The probability of a long-term hydrogen deflagration leading to containment failure at the time of vessel failure was dismissed as being of negligible probability. The arguments presented in reaching this conclusion for long-term hydrogen deflagrations include a justification that oxygen leakage back into containment (and resultant de-inerting of the containment atmosphere) is not expected.

*Destructive Combustion Modes*

An analysis of potential local concentrations was carried out for a range of scenarios. Containment nodes and time periods of potential susceptibility to flame acceleration were identified and assessed based on MAAP analyses for these scenarios. This required the assessment of the mixture property histories for all 27 MAAP nodes for the MAAP analysis cases considered. For each node, a limiting hydrogen concentration for flame acceleration was dynamically calculated (as a function of oxygen and steam concentrations) and compared to the calculated hydrogen concentration histories. The limits used were based on the recent OECD/NEA State-of-the-art report on hydrogen (Reference 34).

A number of nodes were identified as presenting mixture properties that were susceptible to flame acceleration for short periods during the scenarios analyzed. These nodes and time frames were grouped into the scenarios (cases) listed below, together with the assessed probabilities of flame acceleration causing local or global containment damage:

- Case 1. Transients at high pressure, in-vessel phase, period of discharge from RCS via pressurizer valves:
  - Assessed probability of local damage in the equipment rooms (SG compartment), in particular PARs damage = 6.3E-04.

- Assessed probability of containment failure due to flame acceleration loads = 6.3E-04 (including rupture and leak failures).

- Case 2. Transients at high pressure at vessel failure with possible damage to the reactor pit and containment

  - Reactor pit:

    - Assessed probability of local damage in the reactor pit = 4.5E-02. Since there is no equipment in the pit this scenario is irrelevant for PARs damage.

    - Assessed probability of reactor pit failure due to flame acceleration loads = 0

  - Containment:

    - Assessed probability of local damage in the equipment room, in particular PARs damage = 2.1E-02.

    - Assessed probability of containment failure due to flame acceleration loads = 1.9E-03 (including rupture and leak failures).

- Case 3. Transients at high pressure, with short term MCCI after vessel failure:

  - Reactor pit:

    - Assessed probability of local damage in the reactor pit = 2.3E-3. Since there is no equipment in the pit this scenario is irrelevant for PARs damage.

    - Assessed probability of reactor pit failure due to flame acceleration loads = 0

- Case 4a. Scenarios with MCCI in the long term following vessel failure with dry spreading area and 100 percent PAR efficiency:

  - Assessed probability of containment failure due to flame acceleration loads = 9.0E 05 (including rupture and leak failures).

- Case 4b. Scenarios with MCCI in the long term following vessel failure with dry spreading area and reduced PAR efficiency of 50 percent:

  - Assessed probability of containment failure due to flame acceleration loads = 1.0E 04 (including rupture and leak failures).

- Case 4c. Scenarios with MCCI in the long term following vessel failure with dry spreading area and reduced PAR efficiency of 25 percent:

  - Assessed probability of containment failure due to flame acceleration loads = 5.0E 04 (including rupture and leak failures).

In both cases 4b and 4c, the probability is conditional on the probability of PARs damage from cases 1 and 2.

### Long Term Containment Challenges

The evaluation of long term containment challenges deals with potential long-term challenges to the containment integrity, starting at the time of core debris arrival in the spreading area. The important phenomena include containment pressurization due to steaming during quench, or in the longer term, containment pressurization due to the absence of heat removal, and molten core concrete interactions (MCCI).

This evaluation identifies and decomposes the treated phenomena, which relies on the results of the analyses performed using MAAP4.07. The EPR core melt stabilization system and the SAHRS are included in the MAAP4.07 model, because these systems are key to the maintenance of long-term containment integrity.

The details of the design and function of the SAHRS are described in Section 19.2.3.3.3.2.

The U.S. EPR melt stabilization process involves the following phases:

- In-vessel melt progression and release from the RPV - this process is described in the Section 19.2.3.2.1 – In-Vessel Melt Progression.
- Temporary retention and accumulation of the molten fuel mixture in the reactor cavity with a subsequent failure of the cavity retention gate.
- Melt spreading and distribution.
- Flooding, quenching and long term cooling of melt in the lateral spreading compartment - this process is described in Section 19.2.3.2.2 – Ex-Vessel Melt Progression. The details of the design and function of the Core Melt Stabilization System are described in Section 19.2.3.3.3.1. The specifics of the process of core melt retention, gate failure, melt spreading, melt flooding, quenching, and long term cooling are discussed in Sections 19.2.4.4.2.1 through 19.2.4.4.2.4.
- Containment heat removal - the process of long term containment heat removal, along with the various modes of operation of the SAHRS are discussed in Section 19.2.3.2.2.

#### *Long Term Containment Challenge Mechanisms*

The following challenge mechanisms are identified based on review of the melt stabilization process:

- Melt quench in the core spreading area.
- Incomplete transfer of core debris to the spreading area.

- Failure of passive flooding and molten core concrete interaction.
- MCCI after passive flooding.
- Damage to reactor pit.
- Containment overpressurization.

These mechanisms have been organized into the DET shown in Figure 19.1-7—Decomposition Event Tree for Long Term Challenges. This tree provides the framework for performing the probabilistic evaluation described below.

### Probabilistic Evaluation of Long Term Containment Challenges

The probabilistic evaluation of long term challenges consists of the quantification of the failure probability expected due to the failure mechanisms listed in the DET. The DET headers that are quantified elsewhere in the Level 2 study and are not included in this discussion are:

- Success / failure of passive flooding (essentially a passive system analysis – covered in systems analysis models).
- SAHRS spray availability (covered by system analysis and HRA).
- Active cooling availability (covered by system analysis and HRA).

The remaining DET headers are discussed below.

DET Header: No Containment Overpressure Failure due to Debris Quench

The following are considered as key uncertain parameters for the containment overpressure analysis requiring quantification using distributions:

- The fraction of the core debris which is quenched, fq.
- The pressure increase in containment per fraction of debris quenched, ΔP.
- The base (initial) containment pressure at the time of debris flooding, Pco.

The peak containment pressure resulting from corium quench is determined by the formula:

$$Pc_{peak} = Pco + fq \times \Delta P$$

This pressure is compared with the fragility curve developed in the Containment Fragility analysis, and the CCFP is calculated using Monte Carlo simulation analysis.

For the fraction of core debris quenched, the MAAP4.07 model uses a distribution describing the fraction of the debris quenched assuming heat transfer is limited by

heat conduction through a solid crust. This distribution has a median at 10 percent and lower and upper bounds at 0 and 80 percent, respectively. This treatment assumes that crack formation and water ingression during quench is impossible. While it may be likely that a stable crust will form, at least initially, it is not considered impossible that crust cracking could occur during quenching. A modified distribution has been developed using the following hypotheses:

- A likely situation is that a stable crust will form and heat transfer will be conduction limited. In the distribution, a probability of 0.45 is assigned for quenching between 8 and 12 percent of the debris.

- Another likely configuration would be debris cracking and water ingress during debris quench, resulting in a critical heat flux limited heat transfer rate, which could allow quenching of close to 100 percent of the debris. In the distribution, a probability of 0.45 is assigned for quenching between 96 and 100 percent of the debris.

- All other physical situations of crust and water interaction are assumed to be equally likely. A uniform distribution, total probability of 0.1, is assigned to these.

For the probabilistic analysis of pressure increase during quench, to avoid potential non-conservatisms, the distribution for containment pressure rise per fraction of debris quenched is developed based on the MAAP results with fixed values of FCHF (the flat plate critical heat flux (CHF) Kutateladze number) for the LLOCA sequence. The basis for this distribution is:

- Most likely value (from FCHF=0.1 case): 54 psi pressure increase.

- Upper bound (from FCHF=1.0 case): 62 psi pressure increase.

- Distribution type: symmetric triangular. The triangular distribution is chosen because FCHF = 1.0 is seen as very extreme and this implies that care has been taken to choose a distribution that gives greater weight to the median value (i.e., a higher concentration of probability near the center of the distribution as the tail values are deemed to be very unlikely.

- The same distribution is used for all CDES since this value is not expected to be dependent on the initiator.

The following values are chosen, with a uniform distribution taken between the two endpoints, for the base pressure in the core damage end states listed:

| CDES | Expected Value | Upper and Lower Bounds |
|---|---|---|
| TP/TR: | 28 psia | ±7 psi |
| PL: | 29 psia | ±7 psi |
| SL / ML / SS / LL | 30 psia | ±7 psi |

The results of the Monte Carlo simulation using two million samples show a conditional probability of containment failure of zero for all CDES. A nominal value of 5E-7 will be used for the probability of leakage due to quench overpressure and a nominal value of 1E-7 will be used for the probability of rupture due to quench overpressure for all CDES cases.

DET Header: No Significant MCCI

This header is evaluated only if passive flooding succeeds. If passive flooding fails, significant MCCI is assumed to occur. When passive flooding succeeds, the potential for MCCI beneath flooded debris is judged to be of very low probability, and for this reason only limited investigation of the phenomenon has been performed. AREVA NP has studied melt spreading and corium heat transfer extensively as a basis for the melt stabilization design, and as such this outcome is judged to be of very low probability. Conservatively, the conditional probability for failure at this node is assigned as 1.0E-3 based on engineering judgment.

DET Header: No Containment Overpressure Failure before Basemat Penetration

This header is only evaluated for the case of significant MCCI in a dry spreading area with sprays unavailable. Currently it is assumed that overpressure failure does not occur for MCCI in a flooded spreading area. Results from analysis of the containment pressurization rate during MCCI show a rate of approximately 0.48 psi/hr. At 60 hr, the pressure is approx. 58 psia. Thus to reach the median failure pressure of 226 psia, would take approximately 17 days.

The rate of ablation in the spreading area is approximately 4 inches/hr. The thickness of the basemat below the spreading area is taken from the containment general arrangement drawing and is 14.5 feet, or 4.4 m. The time to penetrate the basemat is therefore, approximately 2,4 days.

Although approximate, this calculation indicates that the first failure mode to occur due to sustained MCCI would be basemat penetration. If it is further assumed that penetration of the basemat would prevent further pressure increase, then the probability for overpressure failure should be taken as a low value.

Based on the above discussion, containment overpressure is judged to be very unlikely in cases where there is ongoing MCCI, and is assigned a probability of 0.01.

DET Header: No Basemat Penetration

This header is evaluated for significant MCCI where sprays are available, and where sprays are not available but overpressure failure does not occur. Theoretically, due to the large spreading area, the possibility exists that even a dry core debris bed may cool sufficiently for MCCI to be arrested before the basemat was penetrated. Physically,

this is possible if heat generated in the melt can be conducted away into the concrete with a delta-T below that required to sustain the concrete decomposition temperature. Success at this header precludes containment overpressure as well, so that if MCCI did not occur then this would also preclude the overpressure failure due to generation of non-condensables. Therefore, end states with success of this header are classified as "no failure".

However, considering the ablation area and the debris temperatures during MCCI, and considering the values calculated previously, the split fraction is assigned a success conditional probability of 1E-02 (failure conditional probability of 0.99).

DET Header: Containment Overpressure Failure due to Incomplete Melt Transfer

For cases with passive flooding and active cooling started later, should any debris be still present in the reactor pit or transfer tube, there is the possibility that the water in these regions would not be cooled by the SAHRS and that boiling and steam overpressurization could occur. Numerous design features of the debris stabilization system make this possibility unlikely. In particular, the concept of the melt plug arrangement itself and the composition of the sacrificial concrete are chosen to condition the core debris/concrete melt mixture properties such that a complete transfer of core debris to the spreading area is assured. There is little data regarding this potential failure mode. Nonetheless, a split fraction conditional probability of 1E-02 for failure has been assigned.

During high pressure CDES sequences, there is a high likelihood of induced failure of the hot leg before vessel failure, which will result in flooding of the reactor pit. Upon vessel failure, there is the possibility that part of the debris will be quenched in the pit and remain there while the remainder of the debris transfers into the spreading area. In this case, independent of the status of SAHRS, there is a risk of overpressurization of the containment because of the continuous boiling of water in the pit. Containment overpressure could occur because the pit is not in the main cooling circuit of the SAHRS and the water level will be maintained at the same level as the spreading area / IRWST, therefore, the pit will constantly be replenished.

The coolability of the corium in the pit is highly uncertain, because the debris will form a very deep pool which may or may not be coolable. For this reason, a large split fraction of 0.5 for non-coolability is assigned.

Summary – Long Term Challenges

The results of the long term challenge evaluation are summarized in Table 19.1-17—Summary of Long Term Challenges Probabilistic Evaluation.

### Level 2 Human Reliability Analysis

The human reliability analysis for the Level 2 PRA follows the same methodology as described in Section 19.1.4.1.1.5 for post-initiator human actions. SPAR-H is a conservative methodology that is appropriate for use when task-oriented HRA methods are not possible, such as is the case for severe accident management. However, the PSF assigned for the Level 2 HRA reflect the more serious circumstances associated with a severe accident. Once into severe accident space, the HRA assigns the PSF for extreme stress (five times nominal value). The PSF assignments for timing and complexity also recognize that additional time is needed for the decision making process and organizational structure of severe accident management. Timing needs and communication complexity increase related to the number of people and organizations involved in the decision. This may include the Technical Support Center (TSC), Emergency Response Center, and executive management.

A key part of severe accident management is the transition from the prescriptive symptom-based EOPs into the more flexible guidelines known as operating strategies for severe accidents (OSSA). The OSSA guidelines are entered when the core outlet temperature reaches about 1200ºF. Exiting the EOPs triggers certain immediate actions such as primary system depressurization, starting LHSI for in-vessel core recovery, containment isolation, and enabling the SAHRS passive cooling line. These immediate actions are universal to all severe accident management strategies and require minimal decision making. Other operator actions credited in the Level 2 HRA involve more decision making and are considered either "on-mitigation path" or "off-mitigation path." On-mitigation path actions include starting SAHRS sprays to reduce containment pressure. Off-mitigation path actions are recovery actions that are complicated by additional failures, or where there may be uncertain benefits. These operator actions require correspondingly more decision making time and communication complexity, which is reflected in the SPAR-H PSF assignments.

The PSF for timing is determined using the SPAR-H equations and comparing the time needed for decision making and action implementation to the total time available until the undesired consequence is unavoidable. In Level 2 the undesired consequence may be reactor vessel failure, containment bypass, or containment failure, and the time available is generally determined from representative MAAP runs.

### 19.1.4.2.1.3 Containment Event Trees

The U.S. EPR Level 2 PRA uses eight CETs. A summary description of each CET is provided in Table 19.1-18—Description of Level 2 Containment Event Trees. These summary descriptions are supplemented by Tables 19C-1 through 19C-8, in Appendix 19C, which provides further details on the headers included in each CET and the input events used. These tables are also supplemented by the Event Tree Figures 19C-1 through 19C-8, which are also presented in Appendix 19C.

The top events included in the CETs address the phenomenological events, the systems, and the human actions credited to mitigate the severe accident. The top events included are those which are expected to have a significant impact on the severe accident progression, meaning that they can affect, directly or indirectly, either the likelihood of containment failure or bypass or the magnitude of the source term. For convenience, the events considered within the CETs are grouped into different time frames. The U.S. EPR Level 2 CETs consider the following timeframes:

- Timeframe 1 (TF1), which considers the period from the onset of core damage up to the time of vessel failure (if this occurs).
- Timeframe 2 (TF2), which considers the period from the time of vessel failure to the start of melt transfer to the spreading area.
- Timeframe 3 (TF3), which considers long term events from the time of melt transfer to the spreading area.

Relevant events considered in timeframe 1 include containment isolation, induced RCS failures, depressurization of RCS by the operators, and hydrogen combustion.

Relevant events in Timeframe 2 include in-vessel steam explosion (failing containment or damaging the reactor pit), melt retention in-vessel, ex-vessel steam explosion (damaging the reactor pit), and loads at vessel failure leading to containment failure (DCH, hydrogen or vessel rocketing).

Relevant events considered in timeframe 3 include melt transfer to the spreading area, initial stabilization of melt ex-vessel, steam overpressure during quenching leading to containment failure, hydrogen combustion, steam overpressurization long term, steam explosion in the spreading area, long term overpressure or basemat failure due to molten core concrete interaction, and sprays for source term mitigation.

The linkage of the CETs to the Level 1 is done with the use of core damage end states, which are described in 19.1.4.2.1.1. The CDES are not, however, directly transferred to Level 2 CETs. Rather, each individual end state is transferred through an intermediate event tree, referred to as CDES link event tree (Table 19C-10 through Table 19C-40 and the corresponding Figure 19C-10 through Figure 19C-40), prior to transfer to a Level 2 CET. The use of these CDES link event trees provides a consistent structure for linking the Level 1 and Level 2 models, allows separation of limited core damage sequences from severe core damage sequences, and also allows some technical aspects of the linked model to be implemented.

Once the incoming sequences from the Level 1 have passed through the CDES link trees they are then transferred to the appropriate CET model. Of the eight CETs used in the U.S. EPR Level 2 PRA at power, seven receive a direct transfer from the CDES

link event trees. The eighth CET, the second stage CET for high pressure sequences, only receives transfers from the first stage CET for high pressure sequences.

Once sequences are transferred to a CET, they generally pass through only that CET and are assigned to a Release Category (RC). The release category assignments are marked on the end of each CET sequence. More detail on RC assignment is provided in the Section below. The exception to the foregoing is the first stage high pressure CET. This CET uses further transfers to other CETs. Three outcomes are possible for sequences in this CET, these being (1) assignment of the end state to a release category, (2) transfer to the low pressure CET, (3) transfer to the second stage high pressure.

### Accident Class Release Categories

Fission product release categories are defined to group accident sequences (end points of the CETs) which have similar release characteristics (source terms). The release categories are defined based on the following attributes:

- Containment Bypass - Bypass sequences are defined as:
  - Interfacing system LOCAs (with no isolation of the break).
  - SGTRs, initiators (single and multiple).
  - SGTRs induced by creep rupture due to high temperature and pressure during the severe accident.
- Time for containment failure to occur - The containment failure timeframes considered in the CET are:
  - TF1 - period from the onset of core damage up to the time of vessel failure.
  - TF2 - period approximately at the time of vessel breach, up to the melt transfer to the spreading area.
  - TF3 - long term, the period from melt transfer to the spreading area.
- Containment Failure Category - The containment failure categories are:
  - For TF1, the failure may be a loss of isolation or a rupture (alpha-mode - failures are grouped as ruptures under this header).
  - For TF2, only a rupture of the containment is possible.
  - For TF3, the failure could be a rupture or a basemat melt through.
  - For bypass sequences, this header separates SGTR sequences from other sequences.

- Melt retained in-vessel - This splits out sequences with and without vessel breach (success or failure of melt retention in-vessel).

- MCCI occurs - This separates sequences having extended MCCI (molten core concrete interaction) from sequences with no MCCI.

- Melt flooded ex-vessel (covered by water).

- Source term mitigated by sprays or scrubbing - Sprays are considered for source term mitigation in all categories with containment failure, except for cases in which the vessel has not breached. This is a simplification, source term calculations assume no sprays in this case.

  – For bypass sequences (SGTR and ISLOCA events) this characteristic represents whether or not the release is scrubbed by an overlying water pool.

The resulting release categories are provided in Table 19.1-19—Release Category Definitions.

### Source Term Definition

The source term represents the release to the environment, as a function of time, for the different isotope groups considered in the model. The source term analysis was performed using the MAAP4.0.7 code, which includes U.S. EPR specific models. In MAAP, fission products are organized into 12 groups as follows:

1. GROUP 1 VAPOR (V): Nobles (Xe + Kr), and Aerosol (A): All non-radioactive inert aerosols

2. GROUP 2 V & A: CsI + RbI

3. GROUP 3 V & A: TeO2

4. GROUP 4 V & A: SrO

5. GROUP 5 V & A: MoO2 + RuO2 + TcO2 + RhO2

6. GROUP 6 V & A: CsOH + RbOH

7. GROUP 7 V & A: BaO

8. GROUP 8 V & A: La2O3 + Pr2O3 + Nd2O3 + Sm2O3 + Y2O3 + ZrO2, NbO2, AmO2, and CmO2

9. GROUP 9 V & A: CeO2 + NpO2 + PuO2

10. GROUP 10 V & A: Sb

11. GROUP 11 V & A: Te2

12. GROUP 12 V & A: UO2

Where: V=vapor, A=aerosol

The source term is the result of the MAAP analysis and presents the fraction of the initial core inventory which is released to the environment as a function of time.

The objectives of the source term analysis are to:

- Characterize the source term associated with each release category.
- Perform analysis to determine the sensitivity of the source term to a number of key variables.

To achieve these objectives, a number of sequences were identified for analysis using MAAP4.0.7. For the first objective, a single representative sequence was chosen for each release category which had a non-zero frequency associated with it in a preliminary version of the CET quantification.

For the second objective, sensitivity cases were identified which investigated:

- Effect of isolation failure break size.
- Importance of SAHRS on source term.
- Effect of seal leakage on source term.

In addition to these cases, an evaluation of the effects of water pool scrubbing during SGTRs was performed.

The source terms are defined for each release category in Table 19.1-20—Source Terms for Each Release Category.

### Large Release Definition

The Level 2 PRA quantifies the frequency and source term of each RC. It therefore provides a comprehensive prediction of release risk. However, for reporting purposes, and to allow comparison with various targets and criteria, it is convenient to quote Large Release Frequency (LRF) as the fraction of CDF predicted to fall into RCs which can be classified as “large”.

The following guidance, adapted from Appendix A of NUREG/CR-6595 (Reference 46) is used to determine whether the release associated with a given release category is “large”:

- Any predicted I, Cs, or Te release above approximately 2.1 to 2.5 percent is classified as “large release”.

- The releases associated with all release categories with containment bypass, containment isolation failure, or containment failure at or before vessel failure are classified as "Large".

Using these criteria and the results of the source term analysis, the following release categories are classified as "large release": RC201 through RC205, RC301 through RC304, RC402 through RC404, RC702, and RC802. Conservatively, RC401 is also included in the LRF.

The conditional containment failure probability is the conditional probability that a core damage sequence will result in a large release. It is calculated as the ratio of LRF to CDF.

RC504 is not classified as LRF even though the release fraction of tellurium (Te) for RC504 in Table 19.1-20 exceeds the value for large release fraction. This is because the release fractions for iodine, cesium, as well as tellurium dioxide and molecular tellurium (TeO2 and Te2) contributors to the Te group in Table 19.1-20 are all more than an order of magnitude below the guidance for "large" release. With such low values for the Iodine, Cesium, and Tellurium species, it is unlikely that off-site consequences would be as great as one mean fatality at one mile.

### Containment Fragility

The Level 2 PRA study identifies, evaluates and quantifies loads on the containment structure that can occur as a result of a severe accident. To assess the probability that a given load will result in failure of the containment structure (also part of the Level 2 study), knowledge of the capacity of the structure to withstand loads is needed. Most containment structures are conservatively designed, and when their capacity is assessed realistically, they are found to have considerable margin above design conditions. It is, for example, often found (even on existing plants) that a containment structure can withstand around two times its design internal pressure before failure would be expected to occur. This capacity information is generally used in the form of a composite fragility curve, which shows the probability of failure at less than or equal to a pressure p, as a function of p. Thus it is a cumulative distribution function, differentiation of which leads to the probability density function. It is important to note that, unlike in design space, a PRA uses best estimate approaches, with consideration of the uncertainties. Thus the median of the fragility distribution represents the best estimate failure pressure, while the uncertainties around this value are represented by the probability distribution. It is also important to realistically characterize any failures, particularly by selecting justified failure modes (rupture), and expected leak or rupture areas. These are used in the source term calculations.

The fragility curve is generated in two steps, described in the following paragraphs:

First, the structural parts of the containment structure are systematically identified. For each structural part, or sub-area, a best estimate structural assessment or analysis of the containment structure is performed, which identifies the important potential failure modes, the expected (best estimate) pressure leading to failure, the location of the failure modes, and the expected failure mechanism (and, therefore, expected break size). In addition, sources of uncertainty are identified and quantified (where possible in the form of distributions). Uncertainties may be due to, for example, material properties, construction practices and analytical/methodological uncertainties. The resulting information is presented for each of the failure modes identified. The values obtained for the U.S. EPR containment structure are shown in Table 19.1-21—Failure Modes and Pressure Capacities of the Containment Six Sub-areas under an Accident Temperature Condition of 309°F.

Second, in the Level 2 PRA it is customary to distinguish between leakage and rupture failure modes of the containment. A leakage failure mode is one where the failure size is such that a rapid depressurization of containment does not occur. The smaller failure size leads to a smaller source term provided subsequent rupture does not occur. Whether rupture subsequently occurs depends on the load, and in particular the pressurization rate of the containment at the time of failure, and on the leakage area. For rupture, it is assumed that the containment breach would stop a gradual pressure increase and would cause a rapid depressurization of the entire containment within two hours. To simulate both leakage and rupture failure modes, the fragility curves for both are needed.

To be in a form directly usable in the PRA, the Level 2 analysts use the results of the structural assessment to generate a "composite fragility curve" (or curves if temperature dependence is important). The fragility curve combines the results from each of the individual failure modes into a single distribution, representing the capacity. The composite curve is shown in Figure 19.1-8—Containment Composite Fragility Curve at 309°F.

To distinguish between leakage and rupture failure modes, two cases are considered:

- A fast pressure rise, where it is typically assumed that a leak failure would not prevent further pressurization (and potential rupture at higher pressure).
- A slow pressure rise, where it may be assumed that a leak failure will prevent further pressurization and so preclude ruptures at higher pressure.

Every section is assigned the most likely failure mode (rupture or leak) based on a comparison with NUREG/CR-6906 (Reference 64). A sensitivity on the classification assumptions is performed to verify that the final analysis is not sensitive to these assumptions. The composite containment fragility curve combines both failure modes. However in the Level 2 PRA, rupture and leak are considered separately when estimating containment failure probabilities given certain loads. The loads are

determined (for different phenomena and for different classes of sequences) in the Level 2 phenomenological evaluations and uncertainties in the loads are considered by representing the loads as probability density functions. More details of the analyses carried out for each phenomenological event are given in Section 19.1.4.2.1.2.

### Level 2 Plant Systems

The Level 2 plant systems that are evaluated in the Level 2 PRA are described below.

*Primary Depressurization System Valves (PDVS)*

RCS depressurization is credited in the Level 2 analysis to prevent RCS failure at high pressure. Depressurization during a severe accident scenario is accomplished via the four Primary Depressurization System Valves (PDSVs). During power operation, the PDSVs remain closed. During transient and accident conditions, the functions of the PDSVs are to:

- Provide RCS heat removal with feed and bleed during transients and LOCA events (Level 1).
- Provide RCS depressurization capability via manual depressurization during severe accidents to prevent core melt and RCS failure at high pressure (Level 2).

Refer to Section 19.1.4.1.1.3 for a description of the PDSV support systems.

*Passive Autocatalytic Recombiners*

This system is discussed in Severe Accident Evaluation, Section 19.2.3.3.2. The Passive Autocatalytic recombiners and gas mixing system are passive systems and do not require supporting systems to operate.

*Core Melt Stabilization System*

This system is discussed in Severe Accident Evaluation, Section 19.2.3.3.3.1. This system is a combination of passive and active devices and requires electrical power and operator action to perform its functions.

*Containment Isolation System*

The containment isolation system is credited in the Level 2 PRA with preventing the release of radioactive fission products by isolation of those lines penetrating the containment that are not required for the operation of accident mitigation and severe accident systems. Systems with piping that penetrates the Containment Building and the valves in the PRA model are listed in the Table 19.1-22—Containment Isolation Valves Assessed in Level 2 PRA.

The following specific safety provisions are provided for the power supplied to containment isolation valves:

- The electric motor-operated CI valves inside containment are supplied from Class 1E 480V buses and are backed up by the two hour batteries, EDGs, and Station Blackout (SBO) diesels in the event of a station blackout.

- The electrical motor-operated valves (MOVs) outside containment are supplied from Class 1E 480V buses normally backed up by the EDGs, and can also be backed up by the SBO diesels in the event of a station blackout. These buses can also be supplied with manual operator action from a severe accident power supply, which is an uninterruptible power supply (UPS) (12 hour batteries). However, the PRA model does not credit the UPS (12 hour batteries for this case).

- The success criterion for the CI function is the closure of at least one valve in each containment release path. CCFs are considered for MOVs and check valves that are identical and fulfill similar functions under similar operational and environmental conditions.

*Severe Accident Heat Removal (SAHRS)*

The SAHRS is credited for the following functions:

- Core Spreading Area Cooling – The SAHRS provides cooling to the core spreading area to stabilize molten core debris in the CMRS.

- Containment Spray Cooling – The SAHRS provides spray cooling for the containment space to prevent containment overpressure due to steaming from the molten core debris in the CMRS.

- Basemat Cooling – The SAHRS provides forced circulation cooling from the IRWST through the SAHRS heat exchanger and through the basemat cooling device for long term decay heat removal from the molten core.

- Containment Atmosphere Scrubbing – The SAHRS provides containment spray for the purposes of source term reduction following a severe accident with the core ex-vessel.

The SAHRS consists of a single train whose primary components are located in Safeguards Building 4. The SAHRS train is composed of a pump that draws suction from the IRWST, a heat exchanger, and three possible discharge pathways. MOVs controlled by the operator from the MCR are used to route the flow from the heat exchanger to one of the following pathways:

- Containment Spray–This path routes flow to the dome spraying system. The dome spraying system is composed of a ring header and spray nozzles located in the dome of the containment. Spray through this header reduces containment pressure, temperature, and airborne fission products. The spray water and the condensate flow back to the IRWST.

- Spreading Area Cooling–This path is used to support an active cooling mode of the spreading area under severe accident conditions.

The initial flooding of the spreading area is the result of a passive actuation of two flooding valves after the operator opens the upstream normally closed MOVs. The melting corium opens the valves as it moves across the spreading area. The spreading area is lower than the normal water level in the IRWST and after the flooding valves are opened, the water will gravity feed from the IRWST to the spreading area to cool the corium.

After this initial flooding is complete, cooling is maintained by switching this path to active cooling. The path is aligned so that the SAHRS pump can pump additional IRWST water through the core spreading area cooling line. Cooling water from the IRWST is pumped through channels in the basemat (underneath) of the spreading area to draw heat away from the cooling core-melt. Steam generated by the core melt cooling condenses in the containment atmosphere and returns to the IRWST.

During backflush operation, the SAHRS pump can be aligned to take suction from the IRWST sump and re-route the excess flow back to the IRWST through a line that bypasses the sump strainers. The SAHRS pump can be aligned to this pathway as in the active cooling mode mentioned above. This allows the SAHRS to pump IRWST water through the SAHRS cooler and back to the IRWST, allowing the SAHRS to cool the IRWST water.

The SAHRS is equipped with a dedicated train of CCWS, which in turn is supported by a dedicated train of ESWS.

### Equipment Survivability

This evaluation addresses the survivability of equipment credited in the CET models under severe accident conditions. During the severe accident, conditions of high temperature, humidity, pressure and radiation are expected inside the containment. Systems that are inside the containment will be exposed to these conditions. There is also the possibility that containment failure could affect the continued operation of systems used for source term mitigation. This may be dependent on the location of containment failure; containment failure at a particular location could have the potential (dependent on the containment failure modes and plant geometry) to cause release of hot gases into equipment rooms.

Since the CET model may include the actuation or continued operation of such systems, it is necessary to assess the likelihood that the systems will operate or continue to operate under these conditions.

The following functions have been identified as requiring evaluation for qualification during severe accident conditions:

- Reactor Coolant System (RCS) depressurization.
- Hydrogen mitigation.
- Melt stabilization.
- Containment heat removal.
- Monitoring activity distribution within the containment and potential releases to the environment.

The review of equipment survivability is documented in Table 19.1-23—Evaluation of Equipment Survivability for Level 2.

The following headers in the CET were also reviewed, but are not relevant for equipment survivability:

- No induced hot leg rupture.
- RCS pressure remains high in small LOCA sequences.
- No reactor pit damage due to lower head failure due to in-vessel steam explosion.
- Reactor pit not damaged by ex-vessel steam explosion.

The review of the CET and assessment of equipment credited in light of plans for equipment qualification for severe accidents has concluded that, with the exception of the hydrogen recombiners, none of the equipment credited in the CET models should be considered affected by the severe accident conditions expected to occur during the progression through the Level 2 CET. Consequential damage to the recombiners due to accelerated flame phenomena is considered in the CET model.

#### 19.1.4.2.2 Results from the Level 2 PRA for Operations at Power

Total at power LRF from internal, fire and flood events is 3.01E-08/yr. This is well below the NRC goal and U.S. EPR probabilistic design goal of 1E-06/yr. The Release Categories and their contribution to the at power LRF and the associated CCFP are shown in Table 19.1-105- U.S. EPR Release Category Contributions to Total LRF from at Power Internal Events, Fire and Flooding

The CCFP from all at power events (internal, fire and flood events) large release sequences is 0.0622.

##### 19.1.4.2.2.1 Level 2 Risk Metrics for Internal Events (LRF, CCFP)

Total LRF from internal events is 1.46E-08/yr. This is well below the NRC goal and U.S. EPR probabilistic design goal of 1E-06/yr. Mean value and associated uncertainty distribution can be found in Section 19.1.4.2.2.7. The number of cutsets contributing

to 95 percent of the internal events LRF is 155,911

The CCFP from all internal events (at power) large release sequences is 0.0608.

#### 19.1.4.2.2.2 Internal Events Core Damage Release Category Results

The Release Categories and their contribution to the internal events LRF and the associated CCFP are shown in Table 19.1-24—Internal Events Release Category Results - Large Release Frequency.

Approximately 73 percent of the LRF for internal events is from Release Category RC702. This Release Category captures containment bypass due to steam generator tube rupture core damage sequences from the Level 1 PRA initiator (random single SGTR initiator approximately 57 percent and pressure-inducted SGTR initiator approximately 4 percent) and thermally creep-induced steam generator tube ruptures (approximately 39 percent) from the Level 2 PRA. Although the Level 2 PRA phenomenological assessments identified certain scenarios in which the probability of a creep induced SGTR was large, the quantification of the Level 2 PRA model shows that the probability of all the circumstances required for these probabilities to be applicable is low. This is because (i) the operators are likely to manually depressurize the RCS before the steam generator tubes are challenged, using either the PSVs or the dedicated primary depressurization system valves, (ii) the tubes are not expected to be challenged in scenarios where there is feedwater to at least one SG (important for seal LOCA cases), (iii) the highest induced rupture probabilities are only applicable in cases where the secondary side of the SGs are depressurized. Other important contributors to the internal events LRF are discussed below:

- The second largest group of release categories (RC201 through RC205) contributes to the internal LRF about 21percent and represents large containment isolation failures. Of these, the two largest contributors are RC203 and RC204 (9 percent and 7percent of the internal LRF respectively). They represent large containment isolation failure with failed in-vessel recovery. RC203 represents scenarios with MCCI and failed SHARS sprays while RC204 represents scenarios without MCCI and successful SHARS sprays.

- The next group contributing to LRF represents containment failure before (RC301 through RC304) or at vessel failure (RC401 through RC404) from hydrogen loads, direct containment heating or vessel rocketing. The largest contributing release category is RC304 with containment rupture before vessel rupture (from SLBI initiator or hydrogen loads) without MCCI and failed SHARS sprays.

- The last LRF contributor represents containment bypass with interfacing system LOCA initiator (about 2 percent of the internal LRF). No credit is taken for scrubbing of these scenarios and all of the CDF sequences are led to LRF.

The main features of interest of the detailed breakdown are that the LRF is dominated by inherent containment bypass (SGTR RC702) or systems failures (containment

isolation failure RC201-RC205) rather than failures related to phenomena (300s, 400s). The containment challenges due to severe accident phenomena are of low frequencies and conditional probabilities. This is indicative of a robust containment response.

The main containment failure release categories that are important in terms of conditional probability (greater than 1percent) are:

- Scrubbed SGTR sequences (RC701) with the top cutset representing multiple induced SGTR initiator. All contributors to RC701 (Scrubbed SGTR sequences) are from steam generator tube ruptures initiators (scrubbing is only credited with SGTR initiators not with creep induced SGTR since a dry secondary is a necessary condition for creep rupture). It is noted that RC701 (where feedwater is available) has a frequency approximately three times that of RC702 (unscrubbed release). It is noted that RC701 is not a large release and requires an operator action to start EFW to steam generator Train 4 where the initiator SGTR is postulated. It can further be observed that (although this has not been credited in the modeling) RC701 would be a slow developing sequence due to the effect of heat removal via the affected SG with feedwater available.

- Small loss of containment isolation (RC206) with a top cutset representing total loss of AC and DC power.

- Long term failure of the spreading area basemat (RC 602 representing), mainly driven by failure of basemat flooding (opening of the MOVs on the IRWST flooding lines) to stabilize the melt ex-vessel as a result of steam explosion due to late melt relocation, the treatment of this phenomenon is very conservative (a probability of failure of the spreading area of 1 given a late relocation with successful passive flooding and a probability of steam explosion of 0.5). RC602 top cutset represents a small LOCA initiator with a total loss of IRWST and dependent operator failure to open the valves for basemat flooding.

- Long term overpressure without MCCI but with failure of SAHRS sprays for source term mitigation (RC504).

The release categories with important contributions to the LRF and conditional containment failure probability are driven by system failures or other characteristics of the incoming Level 1 core damage sequences. These failures are due to containment bypass or loss of all electrical divisions that supply the control power for containment isolation, the MOVs for basemat flooding and the SAHRS sprays, rather than the capacity of the containment to withstand phenomenological challenges.

#### 19.1.4.2.2.3 Significant Level 2 Cutsets and Sequences

The significant cutsets for the internal events Level 2 PRA are illustrated in Table 19.1-25—Level 2 Internal Events Large Release Significant Cutsets. This table provides the top cutsets for each release category contributing to the internal LRF. If there were no cutsets in a release category that contributed greater than one percent of LRF, then the top cutset in the release category is reported, regardless of its

contribution. The columns in the table show: release category, cutset frequency, the basic events in the cutsets and their descriptions, and a sequence description that includes both the Level 1 and Level 2 aspects of the cutset.

As discussed in Section 19.1.4.2.2.2, the important release categories contributing to large release are RC203 and RC702. These release categories are dominated by system failures and other characteristics of the incoming Level 1 sequences, rather than the capacity of the containment to withstand severe accident phenomenological challenges. The top cutsets for each release category contributing more than one percent to the LRF are described below.

**Release Category RC201:**

The top cutset group contributes approximately one percent to the internal events large release. These cutsets involve LOOP sequence where a loss of all 1E 2hr batteries prevents starting of EDGs and results in a loss of all instrumentation. After core damage this sequence leads to a successful depressurization with power supply from the non-safety electrical buses available. Large containment isolation fails due failure to close the initially open leak off system valves due to loss of electrical Divisions 1 and 4 followed by a containment annulus venting failure. In-vessel recovery is successful after power recovery leading to RC201.

**Release Category RC204:**

This cutset group contributes less than one percent to the LRF. The sequence represents a LOOP sequence where a loss of all 1E 2hr batteries prevents starting of EDGs and results in a loss of all instrumentation. After core damage, the sequence leads to a low pressure sequence. Large containment isolation fails due to failure to close the initially open leak off system valves due to loss of electrical Divisions 1 and 4 followed by a containment annulus venting failure. In-vessel recovery phenomenological failure, with sufficient injection after power recovery within 7 hours, no ex-vessel steam explosion occurs and no significant MCCI (debris flooded) with successful opening of the MOVs on the passive flooding lines.

**Release Category RC205:**

This cutset group contributes less than one percent to the LRF. The sequence represents a LOOP sequence where a loss of all 1E 2hr batteries prevents starting of EDGs and results in a loss of all instrumentation. After core damage depressurization is failed due to a loss of electrical Divisions 1 and 4. Large containment isolation fails due to failure to close the initially open leak off system valves due to loss of electrical Divisions 1 and 4 followed by a containment annulus venting failure. No ex-vessel steam explosion occurs and there is no significant MCCI (debris is flooded) with successful opening of the MOVs on the passive flooding lines. SAHRS sprays failed as power is not recovered before 31 hours.

**Release Category RC304:**

This cutset group contributes less than one percent to the LRF. The sequence represents a SLBI initiator with CCF of SAS results and failure to control EFW steam relief and LHSI heat exchanger cooling. SAHR train is in preventive maintenance resulting in a loss of all long term cooling (LTC). After core damage, the sequence leads to containment overpressure failure due to SAHRS sprays failure.

**Release Category RC702 - Cutset 1:**

This cutset group contributes about one percent to the LRF. The sequence represents a pressure induced SGTR initiator with a failure of 2-9 tubes. The operator fails to depressurize and fails to initiate RHR cooling in time to prevent an excessive inventory loss. After core damage, the sequence leads to containment bypass after SGTR and dependent failure of the operator to start EFW on the faulted steam generator to scrub the releases.

**Release Category RC702 - Cutset 2:**

This cutset group contributes about 9 percent to the LRF. The sequence represents a SGTR initiator with the HVAC Train 4 in preventive maintenance. The initiator disables the maintenance HVAC train leading to a loss of HVAC in Safeguard Building 4 and a loss of a running CCW pump. The operator fails to switch to the standby CCW pump resulting in a loss of CH2 and HVAC Train 3. Tube rupture is assumed to be in SG 4 and loss of HVAC 3 and 4 prevents isolation of the affected SG. RHR Train 1 discharge valve was left in the wrong position resulting in failure of 3 RHR pumps and failure to provide the required heat removal. After core damage, the sequence leads to containment bypass after SGTR and failure of EFW on the faulted steam generator to scrub the releases.

**Release Category RC802:**

This cutset group contributes less than one percent to the LRF. The sequence represents ISLOCA initiator from break in MHSI cold leg injection line. After core damage the sequence leads to containment bypass following ISLOCA initiator with unscrubbed releases.

#### 19.1.4.2.2.4 Significant Core Damage End States, Initiating Events, Phenomena and Basic Events

Table 19.1-26—U.S. EPR Core Damage End States Contributions - Level 2 Internal Events shows the distribution of CDES that contribute to LRF.

This table shows that 44 percent of the LRF results from the SG CDES. This contribution arises because of the steam generator tube rupture sequence described in Section 19.1.4.2.2.3. Of the remaining contribution, 20 percent of the LRF comes from

CDES involving Seal LOCA following transient initiators with depressurized steam generators, and 12 percent from core damage sequences involving Seal LOCA with loss of offsite power initiator depressurized steam generators.

Table 19.1-27—U.S. EPR Initiating Events Contributions - Level 2 Internal Events shows the contribution of the internal initiating events to LRF. The largest contributor at 40 percent is random steam generator tube rupture IE SGTR. This contribution arises because of the steam generator tube rupture described in Section 19.1.4.2.2.3. The second largest contributing initiating event is loss of offsite power (IE LOOP, 24 percent). The third largest contributor is loss of component cooling water (IE LOCCW, 23 percent). The fourth largest contributing initiating event is loss of divisional emergency AC (IE BDA, 5 percent); other initiators contribute less than 5 percent to the internal events LRF.

Table 19.1-28 through Table 19.1-31 show the important contributors to the internal events LRF. Importance is based on the FV importance measure (FV ≥0.005), or the RAW importance measure (RAW ≥2).

Table 19.1-28—U.S. EPR Risk-Significant Phenomena based on FV Importance - Level 2 Internal Events shows the risk-significant containment phenomena based on FV importance.

The events L2PH ISGTR-SS2D=Y and L2PH ISGTR-SS0.6D=Y represent creep induced SGTR from high pressure core damage sequences following a Seal LOCA with a 2 inch and 0.6 inch diameter respectively and a depressurized secondary side. These events contribute about 19 percent and 12 percent respectively to the internal LRF and represent a containment bypass leading to a large release (RC702).

The next basic events representing direct containment failure due to a rupture are L2P VECF-FA(H) and L2PH CBV HP. These events represent very early containment failure due to hydrogen flame acceleration (in high pressure sequences) and complete circumferential vessel breach leading to vessel rocketing respectively. Both events contribute less than 1 percent to the internal LRF, however the early hydrogen failure event has the largest RAW value (close to 14) of all phenomenological events.

The event L2PH VECF-FA(H) represents the likelihood of containment failure occurring due to loads from an accelerated flame originating in the lower or middle equipment rooms. These rooms are expected to experience short term transient accumulation of hydrogen during a high pressure core damage sequence, due to hydrogen release thru the PSVs. This event was applied for all high pressure core damage sequences even if the primary circuit depressurizes; this is because the period of vulnerability to ignition and generation of an accelerated flame is expected to be before the time of depressurization. The evaluation of this event includes consideration of the likelihood of continuous burning (rather than accumulation) of

released hydrogen and also takes into account the short term nature of the localized hydrogen peak concentration, because this is reduced in the longer term by the action of the recombiners. Accelerated flames were considered as leading to severe loads on the containment structure even in the absence of deflagration-to-detonation transition. Only limited credit was taken for reduction of the assessed probabilities for mixtures that are close to the concentration limits for flame acceleration.

The event L2PH CBV HP represents the likelihood of containment failure in high pressure sequences from vessel rocketing following a complete circumferential break of the vessel.

Other events appearing as LRF phenomenological contributors (The event L2PH ISGTR-TR=N, The event L2PH CPIHLR-TR, TP=Y, L2PH CP STMEXP, L2PH STMEXP EX=N, L2PH NO CCI, L2PH CCI-DRY) do not represent direct containment failure events. Rather, these represent phenomenological occurrences during the sequences that have an indirect impact on containment performance. The events mentioned represent the probability of intact steam generator tubes, the probability of a hot leg rupture, the conditional probability of ex-vessel steam explosion given a wet pit and the probability of occurrence of corium concrete interactions. Other basic events representing hydrogen combustion loads leading to containment failure have small FV but high raw due to their low probabilities.

Table 19.1-29—U.S. EPR Risk-Significant Phenomena based on RAW Importance - Level 2 Internal Events shows the risk-significant containment phenomena based on RAW importance.

Three events leading to containment failure have RAW values greater than 2, these are:

- L2PH VECF-FA(H): containment rupture before vessel rupture due to hydrogen flame acceleration in high pressure sequences.
- L2PH STM EXP INV LP containment rupture at vessel rupture due to in-vessel steam explosion in low pressure sequences.
- L2PH VECF-H2DEF(H)L containment leak before vessel rupture due to hydrogen deflagration in high pressure sequences.

Table 19.1-30—U.S. EPR Risk-Significant Equipment based on FV Importance - Level 2 Internal Events shows the top risk-significant equipment based on FV importance.

This table shows a strong consistency with the results of the Level 1 analysis contained in Table 19.1-8. This is due to the importance of the electrical and HVAC support systems for the operation of active components that are common to both analyses. HVAC and electrical systems contribute the most to the internal LRF followed by the cooling chains (CCWS and ESWS). Seven components from these systems contribute

more than 10 percent to the internal LRF. Approximately 300 components have RAW values greater than 2 and as high as the 300 range. Most of these components belong to one of the three groups identified as important based on the FV values. The additional components identified as important based on RAW values belong to the SIS system and the ultimate heat sink (which is part of the cooling chain).

Passive SSCs are not represented in the LRF as they perform long term action where phenomena are slowly progressing. For instance the PARs and spreading area structure would be represented in release categories RC500 and RC600 which are not part of the LRF group.

Table 19.1-31—U.S. EPR Risk-Significant Equipment based on RAW Importance - Level 2 Internal Events shows the top risk-significant equipment based on RAW importance.

This table shows consistency with the results of the Level 1 analysis contained in Table 19.1-9.

Table 19.1-32—U.S. EPR Risk-Significant Human Actions based on FV Importance - Level 2 Internal Events and Table 19.1-33—U.S. EPR Risk-Significant Human Actions based on RAW Importance - Level 2 Internal Events show the risk-significant human actions based on FV and RAW importance.

Level 1 operator actions dominate the internal LRF with the three largest contributors being actions related to recovery of room cooling, CCW supply to common header and cross tie of the SBO diesels. All of these actions represent operator failures to perform actions prior to the onset of core damage, rather than being actions related to the failure to perform accident management actions. This reflects the dominance of core damage sequences which represent a severe challenge or bypass of the containment, as discussed in Section 19.1.4.2.2.3, (2) the low reliance of the U.S. EPR design on manual severe accident management measures to prevent large release. The largest contributing Level 2 operator action is OPF-L2-SCRUB-SGTR representing failure of the operator to start EFWS to the faulted SG to scrub radioactive releases. This action contributes about 3 percent to the internal LRF

It can be observed that the main actions considered in timeframes that are relevant for LRF are (a) backup actions for containment isolation, (b) operator entry to the operating strategies for severe accidents (OSSA) and manual depressurization of the RCS. Neither of these actions are single failures from the point of view of preventing large release. Backup of containment isolation is only required if the automatic isolation fails. Depressurization via a hot leg rupture is expected even if a manual depressurization fails, and the U.S EPR containment also shows a good response to high pressure core damage sequences without depressurization, with prevention of large release expected as the most likely outcome even for such sequences.

Most operator actions are relevant for long term mitigation of the containment overpressure, flooding of the basemat and scrubbing of radioactive releases. These actions are not captured in the release categories defining the LRF.

An examination of the operator actions based on RAW values did not show any additional Level 2 operator action as significantly contributing to the LRF.

Table 19.1-34—U.S. EPR Risk-Significant Common Cause Events based on RAW Importance - Level 2 Internal Events shows the risk-significant common cause events based on RAW importance.

This table shows a strong consistency with the results of the Level 1 analysis contained in Table 19.1-12. In the Level 2 results, the HVAC support systems play a large role because of the cooling they supply to the electrical buses that are needed for the highly reliable containment isolation function.

Table 19.1-35—U.S. EPR Risk-Significant I&C Events based on RAW Importance - Level 2 Internal Events shows the risk-significant common cause I&C events based on RAW importance.

SAS CCF has the largest RAW of the I&C systems because the failure probability is low and SAS controls the EFWS water to the SG which is involved in source term scrubbing. Failure of the scrubbing leads to the largest contributor to the internal LRF RC702.

#### 19.1.4.2.2.5 Key Assumptions

For steam line breaks inside containment and failure of three main steam lines to isolate, the Level 1 PRA assumed that additional reactivity control would be required (boron injection) to prevent a return to power and core damage. In the Level 2 PRA it was assumed that such sequences would remain at sufficiently high power for sufficiently long to cause a continuous discharge of steam into the containment, sufficient to overpressure the containment, without the operation of sprays.

Sequences involving containment failure due to loads from an accelerated flame arise from mixture conditions that exceed, for a short time, the limits for potentially flame accelerating mixtures. Accelerated flames were considered as leading to severe loads on the containment structure even in the absence of deflagration-to-detonation transition and only limited credit was taken for reduction of the assessed probabilities for mixtures close to the concentration limits for accelerated flames.

#### 19.1.4.2.2.6 Sensitivity Analysis

The focus of sensitivity studies in support of the Level 2 PRA was on the impact of the phenomenological events modeled in the PRA. In general, sensitivity can be assessed

by considering what the impact on the results, in terms of LRF, would be if the phenomena were sure to occur or sure not to occur. This is an appropriate paradigm for such events, because, generally, it is the case that they do not represent random occurrences (i.e., events that are expected to happen sometimes and not other times) but rather represent events that are expected to have a deterministic, but unknown, outcome. Thus a study of the impact on LRF of setting these events to have probabilities of 0 or 1 provides useful insights. For the purposes of reporting, events are judged to be significant if they can lead to a factor of two increase or decrease in LRF when set equal to 1 or 0.

Since the LRF results are dominated by SGTR sequences discussed in Section 19.1.4.2.2.2, Section 19.1.4.2.2.4, and Section 19.1.4.2.2.5, no individual phenomenological events make a large enough contribution to LRF for these to lead to a significant reduction in LRF when set equal to zero.

The following events can lead to a significant increase in LRF if set equal to 1:

- Hydrogen combustion loads from accelerated flames at high pressure prior to vessel failure leading to containment failure L2PH VECF-FA(H). If assumed to always occur, this event would lead to a 13.9 times increase in the internal LRF.
- The event L2PH STM EXP INV LP (containment failure due to in-vessel steam explosion), would, if assumed to always occur, lead to nearly an 11 times increase in the internal LRF.
- Hydrogen combustion loads from deflagration at high pressure prior to vessel failure leading to containment leak (L2PH VECF-H2DEF(H)L). If assumed to always occur, these events would lead to a 3.8 times increase in internal LRF.

It can be noted that deflagration causing failure of the containment has a small likelihood. Its base probability was assessed with some degree of conservatism - the analysis was based on upper bound (top of range of uncertainty) values for the masses of hydrogen present in containment rather than performing detailed Monte-Carlo simulation as was performed for some other events, and no credit was taken for consumption of hydrogen due to continuous burning.

Similarly, it is also noted that some authors have assessed containment failure due to steam explosion as a physically unreasonable event—refer to NUREG-1524 (Reference 47). The U.S. EPR Level 2 analysis also assessed this as a very low probability event, but with an assessed probability greater than 1E-06, it was not judged to be of sufficiently low probability for it to be removed from the model. Sensitivity to this event arises because, if it is not excluded from the model, it is applicable to a large proportion of core damage sequences.

In addition to the above, sensitivity studies were performed to investigate the induced SGTR contribution and the key factors that reduce its importance to the LRF results.

The two factors identified were FW availability to any SG and operator depressurization; success of either of these functions, included in the CET, avoids the possibility of induced SGTR. It was found that, for the case of internal events, unavailability of primary depressurization had a larger impact on the frequency of RC702 than unavailability of feedwater. However, while the combined impact of both being unavailable had a still larger impact, this was not sufficient to cause a significant (2x) change in LRF for internal events.

#### 19.1.4.2.2.7 Uncertainty Analysis

The results of the uncertainty evaluation for the Level 2 Internal Events LRF will be presented in Figure 19.1-9—U.S. EPR Level 2 Internal Events Uncertainty Analysis Results - Cumulative Distribution for Internal Events LRF.

The basis for the input uncertainty distributions for systems related basic events and operator actions is discussed in Section 19.1.4.1.2.7.

For quantitative evaluation of the overall uncertainty on the LRF, uncertainty distributions were added for the Level 2 phenomenological basic events. These events are identified in the PRA database by use of the prefix “L2PH”.

#### 19.1.4.2.2.8 PRA Insights

The key insights from the Level 2 PRA for internal events are discussed below. For internal events, the LRF is dominated by sequences entering from the Level 1 in which the containment function is already defeated (bypassed) or cannot be restored (isolation failure). These sequences are those discussed in Section 19.1.4.2.2.3.

Despite the above contributors, the CCFP of large release is 0.06 percent, below the NRC goal of 0.1. The conditional failure probability of large release arising from phenomenological challenges is below 0.01. This implies a robust response of the U.S. EPR containment and accident mitigation features for avoiding large releases. Failure of large containment isolation has a conditional failure probability of 0.01 and is dominated by support system failures from the Level 1 sequences.

Other phenomenological challenges were not identified as leading to significant probabilities of large release. In particular, it is noted that while some challenges were assessed as having a significant probability under certain circumstances, they did not show up as important once the probability of these circumstances was taken into account. One example is the phenomena of thermally-induced steam generator tube rupture, which was assessed as having a large probability for two-inch equivalent LOCA events (or seal LOCA of equivalent flow rate) in conjunction with a depressurized secondary side and an absence of feedwater to the steam generators. Sensitivity studies showed that these events would have been visible LRF contributors without the U.S. EPR design provisions for manual RCS depressurization or if the

two-inch LOCA sequences entered Level 2 with feedwater unavailable. However, even combined unavailability of both functions is not sufficient to increase LRF by a factor of two.

The most important systems for the internal events LRF belong to the HVAC and electrical system followed by the cooling chain (from the Level 1 core damage sequences). The HVAC and electrical systems impact containment isolation, passive flooding and SAHRS).

Operator actions are dominated by Level 1 actions. The largest contributor from the Level 2 internal LRF represents a failure of the operator to start EFWS to the faulted SG to scrub radioactive release.

In terms of non-LRF containment failure release categories, RC701, RC206, RC602, and RC504 are important contributors.RC701 represents Level 1 SGTR initiators sequences with available EFW to Train 4 for scrubbing. The sequences entering the Level 2 SGTR CET did not qualify for limited core damage CET (requiring successful Level 2 Feed & Bleed).

RC206 represents containment isolation failure driven by a total loss of AC and DC power due to LOOP initiator and a common cause failure of the safety batteries or a common cause failure of HVAC.

RC602, late basemat failure is dominated by IRWST sump strainers common cause failure or operator action failure to open the MOVs to the passive flooding lines leading to failure of basemat flooding.

RC504, long term containment overpressure failure without MCCI and SAHRS sprays failure, has a frequency representing 2 percent of CDF. Failure of steam control is driven by SAHRS unavailability due to preventive maintenance and failure of LHSI backup including failure to recover power after a LOOP initiator.

### 19.1.5 Safety Insights from the External Events PRA for Operations at Power

#### 19.1.5.1 Seismic Risk Evaluation

Evaluation of the risk due to seismic events was performed using a PRA-based seismic margins approach. Section 19.1.5.1.1 describes this approach and outlines the manner in which it was applied. Section 19.1.5.1.2 summarizes the results obtained from the PRA-based seismic margins evaluation.

### 19.1.5.1.1 Description of the Seismic Risk Evaluation

#### 19.1.5.1.1.1 Methodology

The PRA-based Seismic Margins Analysis (SMA) was performed in accordance with the applicable NRC guidance documents ISG-020 (Reference 60), and SECY-93-087 (Reference 2), and in accordance with the applicable guidance in Part 5 of ASME-ANS Ra-Sa-2009 Level 1 /LRF Standard (Reference 61) as endorsed by Regulatory Guide 1.200 (Reference 63). As discussed in ISG-020 the purpose of a PRA-based seismic margins analysis is to provide an understanding of significant seismic vulnerabilities and other seismic insights to demonstrate the seismic robustness of a standard design. ISG-020 requires that the SMA analysis be performed relative to a Review Level Earthquake of 1.67 times the Safe Shutdown Earthquake (SSE). The PRA-based seismic margin analysis includes the following key elements:

- Define the seismic hazard input (Section 19.5.1.1.2).
- Perform the Seismic Fragility Evaluation (Section 19.5.1.1.3).
- Evaluate the design specific system and accident sequences considering the impacts of the Fragility Analysis (Section 19.5.1.1.4).
- Evaluating the Plant Level HCLPF (Section 19.5.1.1.5).

The U.S. EPR PRA model developed for internal initiating events (Section 19.1.4) and the U.S. EPR PRA Model for Shutdown Initiating Events (Section 19.1.6) provides the framework for addressing potential failures induced by seismic events. These PRA models also provide the primary basis for establishing the seismic equipment list (SEL), which identifies equipment and structures for seismic fragility analysis. Because this assessment is being conducted early in the plant design, fragility assumptions are documented to support seismic design development in the detailed design phase.

#### 19.1.5.1.1.2 Seismic Hazard Input

The Certified Seismic Design Response Spectra (CSDRS) of the U.S. EPR design consists of three European Utility Requirements (EUR) control motions anchored to 0.3 g peak ground acceleration (PGA), and a fourth high-frequency control motion. The vertical EUR control motions are the same as the horizontal EUR motions. The high frequency horizontal (HFH) and the high frequency vertical (HFV) control motions are anchored to 0.21 g and 0.18 g peak ground accelerations, respectively. The horizontal and vertical CSDRS are provided in Figure 3.7.1-1. For the U.S. EPR design, the CSDRS is the safe shutdown earthquake (SSE) per RG 1.208.

The PRA-based seismic margin assessment follows the guidance in SECY 93-087 and demonstrates that there is a minimum seismic margin of 1.67 times the CSDRS for the U.S. EPR design, not including an analysis site-specific of soil effects, which is the

responsibility of the COL applicant, as noted in Section 19.1.5.1.2.4. See Section 3.7.1 for a description of the CSDRS for the certified design. The 1.67 times the CSDRS is referred to as seismic margin earthquake (SME) in design certification.

#### 19.1.5.1.1.3 Seismic Fragility Evaluation

The fragility analysis results in the generation of HCLPF capacities for SSC expressed in terms of PGA. The systems and accident sequence analysis determine the scope of the fragility analysis by specifying a SEL. The SEL establishes the set of SSC for which HCLPF capacities are needed. The SEL is provided in Table 19.1-106. Seismic fragility analysis is based on input from the seismic qualification and analysis described in Section 3.7 and Appendix 3E for structures, and the seismic qualification process described in Section 3.10 for mechanical and electrical components.

For structures on the SEL, HCLPF calculations are performed using a separation of variable method based on the methodology outlined in EPRI TR-103959 (Reference 38). The structural fragility analysis is performed using the seismic qualification and analysis shown in Section 3.7 and Appendix 3E, and using the U.S. EPR CSDRS as seismic input. Seismic analysis and foundation design for the standard plant are performed for multiple soil profiles including high frequency soil profiles as described in Section 3.7.1.3. Fragilities are calculated based on the highest seismic demand for all the soil profiles. The resulting fragilities are characterized by the median capacity, logarithmic standard deviations that account for randomness and uncertainty, and HCLPF capacity. The HCLPF capacity is a measure of a component seismic capacity. The HCLPF capacity is the acceleration below which there is 95 percent confidence that the failure probability is less than 5 percent. This value can be calculated from the median capacity (Am) for the component and two logarithmic standard deviations, accounting for variability due to uncertainty and randomness ($\beta_U$ and $\beta_R$, respectively). This relationship is as follows:

$$HCLPF = A_m \exp [-1.65 (\beta_R + \beta_U)] \quad (A)$$

The assigned structure-related HCLPF are shown in Table 19.1-106. The HCLPF for the structures excludes analysis of site-specific soil effects, which are the responsibility of the COL applicant, as described in Section 19.1.5.1.2.4.

For mechanical and electrical components, the fragility analysis assigns a minimum HCLPF of 0.5 g to support achieving a plant and sequence level HCLPF of 1.67 times the SSE. Based on industry experience, most commercial equipment and distributive systems are inherently rugged as long as they are adequately supported or anchored (Reference 63). To address supports and anchorage, Section 3.10.3 describes a process by which conservatism is introduced into the design in the form of a performance-based factor applied to the qualification process for critical equipment during severe accident scenarios. As described in Section 3.10, the seismic qualification of electrical

and mechanical systems and components conforms to the guidance of Regulatory Guide 1.100; and Section 3.10.1.4 describes the process by which a Required Response Spectra (RRS) is established for the U.S. EPR design.

One of the key elements in establishing seismic margin for systems and components on the SEL is to establish an RRS that is appropriately factored throughout the frequency range. Therefore, to provide further confidence that the assigned generic HCLPFs for systems and components on the SEL are achievable, appropriate RRS multiplication factors will be established prior to equipment qualification based on the guidance provided in Reference 63 and on conservatism in the in-structure response spectra. This additional measure when applied to the qualification process for the systems and components on the SEL provides reasonable assurance that a plant and sequence level HCLPF equal to 1.67 times the CSDRS is achievable.

A COL applicant that references the U.S. EPR design certification will, for equipment on the SEL, confirm that an acceptable seismic margin is achieved through the seismic qualification implementation program. The plant and sequence level HCLPF capacities will be verified by the COL applicant during the PRA verification process, as described in Section 19.1.2.2.

The COL applicant is also responsible for identifying site-specific SSC and their impact on the HCLPF analysis, as described in Section 19.1.5.1.2.4.

#### 19.1.5.1.1.4 Systems and Accident Sequence Analysis

A seismic-margins model was developed from the event trees and fault trees that comprise the model for internal initiating events so that potentially important accident sequences were considered. So that the relationships among seismic failures and other failure modes could be captured, the seismic-margins model also retains random failures and human failure events from the internal events PRA.

**Initiating Events Analysis:**

Initiating events in the at-power and shutdown internal events models were reviewed to determine those events that need to be included in the SMA model and to provide input to the SEL. Where initiating events were not explicitly modeled in the PRA, it was because SSC in the mitigating systems perform the same functions identified in initiating events already modeled and, therefore, have already been considered for inclusion in the SEL. SSC were identified and added to the SEL when their failure would cause the initiating event.

The following summarizes this review of initiating events:

*Transient Initiators and Loss of Offsite Power*

Loss of offsite power (LOOP) is included as a transient initiating event. LOOP is expected to be the dominant contributor to risk from transient initiating events, based on historical PRA insights. Based on U.S. EPR Level 1 PRA results, LOOP is a dominant contributor to risk for internal events. LOOP dominates this category of failures because it disables non-safety equipment and challenges the emergency diesels. Offsite power is expected to have a capacity lower than the SME. Loss of offsite power is assumed to occur for all seismic initiating events in the SMA quantification. This is conservative because if offsite power is available then the safety systems are not dependent on the emergency diesel generators to start, or dependent on the I&C systems to start and load the emergency diesel generators, etcetera. However, it is noted that in some cases the availability of offsite power will make certain scenarios worse. For example, a loss of condenser vacuum ATWS is more limiting than a loss of offsite power ATWS. Where this situation was noted (e.g., on the ATWS scenarios), the importance of the reactor trip function (and maintaining core geometry so that rod drop is ensured) was qualitatively evaluated based on the limiting scenario rather than relying on the occurrence of a loss of offsite power.

*Small LOCA, Medium LOCA, and Large LOCA*

All LOCA initiating events (SLOCA, MLOCA, and LLOCA) are included as seismic initiating events. Equipment that may fail and cause a SLOCA, such as multiple sensing lines, are expected to have a capacity less than the SME. The RCS piping, major RCS components and the associated supports are included on the SEL (so that no major LOCA event would be expected to occur as a result of a seismic event). Nonetheless, it is conservatively considered that a significant LOCA event could occur as a result of a seismic event (as per the requirements of Reference 61). Excessive LOCA (e.g., Reactor pressure vessel ruptures) are not specifically addressed in the SMA analysis, but because major RCS components (e.g., reactor vessel) are included on the SEL, the probability of such an event will be acceptably small (and because the excessive LOCA goes directly to core damage no additional mitigation equipment would be identified from evaluating these events further).

*Steam Generator Tube Rupture*

SGTR initiating events are not considered as an initiating event in the SMA. The components that could fail and result in a SGTR such as the steam generators, the steam generator tubes and associated components are included on the SEL. Additionally the major equipment such as the MSIVs, MSRTs, FWIVs and steamline activity instruments are included on the SEL to provide mitigation capability.

*Secondary System Breaks*

Breaks/Ruptures in the secondary piping are not explicitly modeled as an initiating event because the equipment required to mitigate these events is already required to mitigate other initiating events that are modeled. Leaks in the secondary piping are expected to have a capacity lower than the SME. Plant arrangement is s that leaks in the secondary piping areas do not impact mitigating equipment (e.g., Emergency Feedwater and Safety Injection). Equipment added to the SEL to mitigate the impacts of secondary breaks includes steam generators and piping, feedwater isolation valves, main steam isolation valves, and steam generator pressure signals.

*Failures of Class 1E Structures:*

Structure failures are not explicitly modeled as initiating events because the Seismic Category I structures that contain equipment credited in the PRA, and Category II structures that can impact structures that contain equipment credited in the PRA, are added to the SEL qualitatively. Failure of a structure is assumed to result in failure of the components in that building. For Seismic Category I and II structures on the SEL, failure of the structure is assumed to lead directly to core damage.

*Interfacing Systems LOCAs*

Interfacing system LOCAs (ISLOCA) are modeled as a shutdown SMA initiating event because failure modes were identified whereby a seismic event could cause an interfacing system LOCA (e.g., rupture of the RHR piping in the Safeguard Building for an in-service RHR train, or the letdown piping downstream of the low pressure reducing station could fail and the isolation valves could fail to close). For the at-power PRA, the only interfacing system break that was identified as being potentially caused by a seismic event was a letdown line break (downstream of the class break where the piping is non-seismically qualified). The letdown line isolation valves are included on the SEL to protect against this at-power initiating event. Additionally, the coolant purification isolation valves from the RHR trains to the CVCS (JNA30AA004, JNA30AA103; JNA40A004, JNA40AA103) are included on the SEL to provide a means to isolate flow through the low pressure reducing station.

*Shutdown Initiating Events*

Initiating events in the shutdown internal events model were also reviewed to determine those events that need to be included in the PRA model and to provide input to the SEL.

The following initiating events are therefore considered in the Shutdown SMA:

Loss of Residual Heat Removal (RHR) – Loss of RHR is modeled as an initiating event.

LOCA in Shutdown – LOCA in Shutdown is modeled as an initiating event (both small break and large break LOCA are considered in the analysis).

Uncontrolled Level Drop (ULD) – ULD is considered as a potential shutdown initiating event in the SMA. The coolant purification isolation valves from the RHR trains to the CVCS (JNA30AA004, JNA30AA103, JNA40A004, JNA40AA103) are included on the SEL to provide a means to isolate flow to the low pressure reducing valves (including consideration of the possible rupture of the letdown piping downstream of the seismic class break).

Interfacing System LOCA – ISLOCA RHR LOCA during shutdown operation is specifically modeled as an SMA initiating event. Equipment added to the SEL includes the Low Pressure Reducing Station Letdown Isolation Valves.

Based on this review, the SMA model includes the following initiating events:

- Seismic LOOP.
- Seismic SLOCA.
- Seismic MLOCA.
- Seismic LLOCA.
- Seismic Loss of RHR in Shutdown.
- Seismic LOCA in Shutdown.
- Seismic ULD in Shutdown.
- Seismic ISLOCA in Shutdown.

Each of these initiators was quantified using the internal events event tree (from Appendix 19A for the at-power PRA or Appendix 19B for the Low Power Shutdown PRA). The SMA model is evaluated (quantified) with the seismic initiating event frequency set to 1.0. For the at-power model, the initiating event frequencies (IE LOOP, IE SLOCA, IE MLOCA and IE LLOCA) are directly set to 1.0. For the shutdown initiating events, the initiating event frequencies are set to 1, and additionally Boundary Condition Sets are utilized such that each seismic initiating event of interest is assumed with a probability of 1.

### Plant Response and Mitigation Systems Review

Accident responses in the at-power and shutdown PRA models were used to develop the SMA model and the resulting SEL.

### SMA Simplifying Assumptions and Modeling Seismic-Induced Failure of Non-Seismic Components

- All systems that depend on normal AC power such as main feedwater, main condenser, Startup and Shutdown System (SSS) pump and their support systems are set to failure in the SMA analysis by failing the offsite power supply. In the at-power model, this is accomplished by setting house event PWR and basic event LOOP24+REC to true (additionally, in the IE LOOP quantification, it is necessary to set REC OSP 1HR, and REC OSP 2HR to true to prevent power recovery from being considered in the LOOP event tree analysis). In the Shutdown model, it is accomplished by setting house event SD and basic event SD LOOP24+REC to true.

- All SSC that are not on the SEL with a commitment to maintain their function for the Review Level Earthquake (1.67 * CSDRS = 0.5g pga) are set to failure in the SMA analysis. (Category II seismic equipment on the list is assumed to functionally fail, but is also assumed not to result in failure of any adjacent seismic category I SSC). Seismic categories were determined based upon Table 3.2.2-1.

### Non-Seismic Systems\Components that are Important to the Level 1 PRA

- Chemical and Volume Control System – CVCS is not credited in the SMA for the purposes of supplying flow to the RCS. The coolant purification isolation valves from the RHR trains to the CVCS (JNA30AA004, JNA30AA103; JNA40A004, JNA40AA103) and the associated category I piping are included on the SEL to provide a means to isolate flow through the LP Reducing Valves. CCW is credited for RCP thermal barrier cooling, and medium head safety injection (MHSI) / low head safety injection (LHSI) are credited for RCS Inventory control. Additionally, auxiliary pressurizer spray is not included nor is it required to mitigate a seismic event.

- SBO Diesels – SBO Diesels are not credited in the SMA. Because the EDGs are the emergency power supply that are designed to withstand seismic forces, the EDGs are the emergency power source that is credited in the SMA analysis (and failure of all 4 EDGs due to random causes is very unlikely). In some seismic PRAs, the results show these backup power supplies have reduced the risk associated with non-seismic random failures of emergency diesels subsequent to lower level earthquakes (higher frequency) that cause a LOOP. Because the U.S. EPR design has four EDGs, the probability of failure because of random causes (non-seismic failure) is less likely.

- Primary Depressurization System (PDS) Valves – PDS valves are not credited in the SMA. These valves are powered by non-seismic AC/DC power supplies located in non-seismic buildings.

- Severe Accident Heat Removal System (SAHRS) – SAHRS and the Closed Cooling Water support to SAHRS are not credited in the SMA. SAHRS depends on electrical equipment in the non-seismic conventional switchgear room.

- Process Information Control System (PICS) – PICS is not credited in the SMA. Operator displays and digital controls and screens in the main control room are not Seismic Category I, but certain portions may be qualified as Seismic Category I.

- Non-Safety Batteries – Non-safety batteries (12 hour and 2 hour) in the Switchgear Building were not credited by failing the buses they supply (with LOOP guaranteed, this effectively fails the PDS valves and the RCP Stand Still Seal System).

- RCP Motors – Oil Collection System – This system is not credited in the SMA. The fire portion of the PRA implicitly credits this system and screens out fires in this system and fires in containment in general.

- Fire Water Distribution System (FWDS) and Sprinkler System – These systems are not credited in the SMA. Fire protection piping in the vicinity of safety-related equipment will be required to maintain structural integrity during a seismic event.

- Non-Class 1E Electrical – Non-class 1E electrical systems are not credited in the SMA.

- Process Automation System (PAS) – PAS is not credited in the SMA.

- Diverse Actuation System – DAS is not credited in the SMA.

- Demineralized Water Distribution System (DWDS) – This system is not credited in the SMA. Refilling from the DWDS requires an operator action, and all operator actions are assumed to fail after a seismic event.

- Safeguard Building Ventilation System (SAC) – The SAC maintenance trains are not credited in the SMA. The maintenance train fans as well as the Operational Chilled Water Chillers that supply the cooling are powered from a non-class IE power supply.

- Certain Equipment Identified as Seismic Category II is included on the SEL where significant seismic interaction issues were identified. This is done when potential system interaction issues are identified. Examples include the Refueling Machine or the polar crane toppling off its rails, or an adjacent structure failing in a manner that an adjacent safety-related structure may be compromised.

- Offsite power – Offsite power is assumed to be lost and remain unavailable following a seismic event, and the offsite power non-recovery probabilities are set to true in the LOOP analysis. Additionally, the EDG mission time has been set to 24 hours, consistent with the standard PRA mission time of 24 hours. Although longer EDG mission times could be postulated, the results of this analysis (identifying SEL equipment, and identifying the SSC most important to seismic accident sequence mitigation) are insensitive to the assumed EDG mission time.

### Evaluation of Safety Functions

The Major safety functions considered in the SMA accident sequence analysis are described below:

*Reactivity Control (Reactor Trip)*

The following equipment is included on the SEL and required to operate to support the scram function:

- Reactor internals (do not prevent rod drop).
- Control rods (drop into the core).
- Fuel assemblies (do not prevent rod drop).
- Reactor protection system (RPS) instrumentation, input signals, logic and cabinets.
- RPS I&C power supplies.
- Reactor Trip Breakers.

ATWS events are considered as a potential at-power initiating event in the SMA analysis. The following equipment is included on the SEL to provide for ATWS mitigation:

Pressurizer Safety Valves (PSV) are required to operate following an ATWS event to mitigate the RCS pressure increase. Therefore, the PSVs are included on the SEL.

CVCS and EBS can be used to mitigate ATWS. CVCS is not included on the SEL because the system is non-seismic category. This is not a concern because the EBS pumps are Seismic Category I and supplied with emergency power. The EBS system, including supporting systems is included on the SEL.

The remaining systems and functions in the ATWS model (e.g., secondary cooling, reactor makeup and containment heat removal) are addressed below for their respective functions.

*Secondary Cooling Emergency Feedwater, Main Steam Relief Valve, Main Safety System Valve*

As described in the initiating event analysis, the steam generator and connected piping systems, including isolation valves have been included in the SEL. Also, as described above, the SSS, main feedwater, and condenser systems are not available as they depend on offsite power and are non-seismic. The following remaining Seismic Category I systems are included in the SMA model and SEL:

- Four EFW trains and their support systems including auto-actuation.

- Four MSRV trains (one on each SG) and their support systems including auto-actuation.
- Eight MSSV (two on each SG).

The above systems alone ensure a success state in the at-power PRA if there is no LOCA. Makeup to the EFW pools is non-seismic and the demineralized water makeup pumps are powered by normal AC power. However, there is enough EFW storage capacity to support the PRA success criteria because the RCP pumps are tripped on a LOOP. There is an operator action to isolate a leaking EFW pool supply, but the probability of this failure mode is low. Although the internal events PRA does not model Residual Heat Removal (RHR) shutdown cooling as a long term alternative to EFW secondary cooling, the four trains of Low Head Safety Injection (LHSI) equipment and their supports systems are included in the SMA model and on the SEL.

*RCP Seal Cooling*

RCP seal cooling is included in the SMA model and included on the SEL to provide a means to maintain cooling to the RCP seals (and thereby maintain the integrity of the RCS). RCP seal injection with CVCS is assumed to be lost because of the seismic event (because the charging pumps are non-class powered). Therefore, thermal barrier cooling with CCWS is required following a seismic event to protect the RCP seals. To maintain the RCP thermal barrier cooling function following a seismic event, components necessary to maintain CCWS thermal barrier cooling are included on the SEL

*Primary Feed & Bleed*

Feed and Bleed Cooling is included in the SMA model to provide accident mitigation in the event that secondary cooling is unavailable. The following equipment is included on the SEL to provide for Feed and Bleed capability:

- Three PSVs opening on demand and their support equipment.
- Safety injection signal (I&C) and supporting equipment.
- Four Medium Head Safety Injection (MHSI) trains and their support systems.
- Four Accumulators and associated MOV and support equipment.
- Four LHSI trains and their support systems (feed and In-Containment Refueling Water Storage Tank (IRWST) cooling).

The following operator action is required:

- Initiate Feed and Bleed - Although SIS occurs automatically when these bleed valves are opened, it is assumed the operators also start the pumps by procedure before opening the valves.

*SLOCA Considerations*

The SSC required to mitigate a SLOCA is similar to the SSC identified for the transient accident sequence. The success criteria are slightly different, but since F&B was included in the transient accident response model most of the equipment required for SLOCA has been identified. The following additional equipment was identified for inclusion in the SMA model and SEL:

- Actuation of Safety Injection and partial cool down (PCD). PCD actuates and opens MSRV trains at a lower pressure to allow MHSI makeup to the RPV.

***MLOCA and LLOCA Considerations***

The systems and components necessary to mitigate a MLOCA or LLOCA are similar to the equipment required to mitigate the small LOCA (although secondary cooling is not required, and accumulators are required to mitigate larger breaks).

***CVCS Letdown (potential loss of inventory path)***

The charging pumps and the associated piping outside of containment are not seismically qualified; therefore, charging was not credited in the SMA. However, the CVCS letdown isolation valves are Category I and are credited in the SMA as a means to prevent an uncontrolled loss of inventory. This loss of inventory could be through the containment isolation valves in the case of an abnormal alignment or break during at-power operations, or through the low pressure reducing station during shutdown.

*Stuck Open PSV (potential loss of inventory)*

Normally, the PSVs are not challenged. Therefore, the possibility of their challenge and then the subsequent failure to close is unlikely and not modeled, except in the case of ATWS and for a loss of RHR during plant operating states (POS) C. The same equipment required to mitigate a small LOCA would mitigate a st**u**ck open PSV.

*Supporting Structures*

Major structures not included above where failure could impact Level 1 SSC on the SEL are added qualitatively and include:

- Nuclear Auxiliary Building.
- Access Building.

- Turbine Building.

*Components Required to Support Effective Operations Control*

To support survival of the operators and their ability to mitigate a seismic event, the following SSC are added to the SEL

- Control room and ceiling.
- Control room emergency ventilation.
- SICS.
- Radiation Monitoring Sensors, Skids, Cabinets.

### Modeling of Seismic Induced Failures

System fragility basic events were added to the model with a probability of 0.1. The same basic event is used for all trains to conservatively correlate seismic failure as a common cause for identical equipment. Fragility basic events were added for the following:

- AC Power (all 4 emergency switchgear trains 31/32/33/34 BDA).
- Accumulators (all 4 trains).
- 1EUPS (the 4 Class 1E Uninterruptible power sources including the inverters and the BRA buses).
- DC Power (the 4 Class 1E Batteries and the associated DC buses).
- CCWS (all 4 trains).
- EBS (both trains).
- EDG (all 4 emergency diesels).
- EFW (all 4 trains).
- ESWS (all 4 trains).
- I&C (all 4 divisions).
- LHSI (all 4 trains).
- MHSI (all 4 trains).
- MSRT (all 4 SGs).
- PSRVs (all 3 trains).

- Reactor Internals (RT failure).
- SAC (all 4 trains and the QKA trains).
- Seal LOCA (all 4 RCPs).

### Seismic Equipment List (SEL)

A list of SSC has been developed based on the SMA model development in the previous section using the internal events PRA model for at-power and shutdown operations. The equipment credited in the SMA for accident mitigation, is included on the SEL (Table 19.1-106). In addition, P&IDs, electrical one-line diagrams, plant arrangement drawings and other plant systems descriptions were reviewed so that highly reliable passive components that may not be explicitly modeled in the PRA are identified. In accordance with Section 5.1.1 of ISG-020 (Reference 60), equipment important to maintain containment integrity is also included on the SEL (Table 19-106). The SEL provides the list of SSC for which fragility analysis is required to determine plant-level HCLPF.

### Containment Performance

An evaluation of containment performance is included so that the appropriate Level 2 SSC are included on the SEL as required by Section 5.1.1 of ISG-020 (Reference 60). The following SSC are included in the SEL:

- Reactor Building, including Penetrations (containment).
- Containment Isolation valves and supporting equipment.
- Core Melt Retention Structure (the melt discharge channel is Seismic Category II, the remainder of SSC are non-seismic).
- Passive flooding line to the core melt stabilization system cooling structure up to and including MOV JMQ42AA004/0006 (the piping line must maintain structural integrity such that IRWST inventory is not depleted).
- Combustible Gas Control System: The Passive Autocatalytic Recombiners and the associated foils and Dampers are included on the SEL list, and will be designed and constructed to maintain a minimum HCLPF of 0.5g pga. The PARS are included on the SEL based on consideration of their importance in maintaining containment integrity following a severe accident.

### Low Power and Shutdown

The LPSD configurations, models, and systems were evaluated to determine whether any components should be added to the SEL. The Shutdown PRA model (fault trees and event trees) was utilized to identify the systems, structures, and components (SSC) that would be required to mitigate a seismic event that occurs during shutdown

operation. The Shutdown PRA model (described in Section 19.1.6) addresses the various Plant Operating States (POS) that occur from Shutdown into Refueling and back to Startup (transition from State C into refueling and back to startup. Each transition POS that differs significantly from normal at-power operation is evaluated for risk in the Shutdown PRA, and each of these shutdown operating states is evaluated in the SMA. POS A and B are covered by the at-power PRA. Many of the same systems and components identified for power operation are also modeled in the LPSD model. A key difference is that loss of LHSI in the RHR mode of operation is a new initiating event, but this system is already included on the SEL. Similarly, loss of offsite power is an important initiating event, but it also has been identified as an important initiator for power operation. However, there are SSC that need to be added to the SEL based on this evaluation as summarized below:

- Reactor Cavity and connected pools (both empty and full).
- Fuel Transfer Tube and Gate Valve.
- Refuel Gates.
- Refueling Machines and Cranes (must not tip over onto fuel assemblies).
- Polar Crane (e.g., must not tip over, drop heavy loads).
- Spent Fuel Pool.
- Spent Fuel Pool Cooling System and supporting equipment.
- Pressurizer vent valves (10JEF10AA501 and 10JEF10AA502).
- The coolant purification isolation valves from the RHR trains to the CVCS (JNA30AA004, JNA30AA103; JNA40A004, JNA40AA103).

### Relay Chatter

Generally, it is expected that solid state relays are used to support the operation of equipment credited on the SEL. Solid state relays are inherently immune to chatter. Electro-mechanical relays, where used, are analyzed as part of the HCLPF capacity determination.

### Random Failures and Human Actions

As required by Section 5.2.3 of Reference 3, the U. S. EPR SMA considers both random failures and human errors. Because the SMA uses the event tree models and fault tree models from the PRA (both the at-power models and the Shutdown models), random failures are considered just as they are in the Internal Events analysis and in the Shutdown PRA analysis. Operator Errors were conservatively set to a value of 1.0 in

the SMA analysis so that required operator actions are identified in the analysis. No credit is taken for any recovery actions associated with seismic failures.

### Summary of the U.S. EPR SMA Approach

The U.S. EPR Seismic Margins Analysis is performed in accordance with the ISG-020 guidance (Reference 60) for performing a PRA-Based Seismic Margins Analysis. ISG-020 endorses Part 5 of the 2009 ASME/ANS PRA Standard (Reference 61) in guiding the SMA approach. The Systems analysis portion of the SMA was therefore performed in accordance with the applicable requirements of 5.2-3 of the 2009 ASME/ANS PRA standard:

- It is conservatively assumed that a seismic event will cause one or more events requiring reactor shutdown including:
  - Loss-of-coolant accidents of various sizes and in all relevant locations.
  - Transients, of which loss of off-site power (LOSP) is usually the most important.

  In the U.S. EPR approach, it is conservatively assumed that LOCAs of various sizes may be induced concurrent with a loss off offsite power and a failure of all equipment not included on the SEL.
- The event trees and fault trees from the internal-event at-power PRA model and from the Low Power Shutdown PRA are used directly in the SMA as the basis for evaluating the seismic accident sequences.
- The PRA-based SMA models consider seismically induced failures as well as random (seismically independent) failures and human errors that are required for accident mitigation.
- System recoveries credited in the internal events model that may not be feasible following a major earthquake are not credited in the SMA model (e.g., nonrecovery of offsite power has been conservatively set to 1 for seismic events, and the diesel generator mission time was increased to 24 hours).
- Seismic related failures are assumed to be non-recoverable.
- The PRA accident sequence analysis and the associated systems analysis was used as the primary input for developing the seismic equipment list.

All (post-accident) human error probabilities have been conservatively set equal to 1.0 in the SMA model, so that human actions required to mitigate seismic induced accident scenarios will be highlighted. The purpose of the SMA is to identify those seismic failures, human errors and random failures that are of primary importance to the seismic risk. It is not the purpose of the SMA to quantitatively estimate the seismic

risk (nor is this any feasible, since in design certification, there is no single seismic hazard that would apply to all possible sites).

The solution of the integrated fault-tree and event-tree models to evaluate the seismic margin is addressed in Section 19.1.5.1.2.

#### 19.1.5.1.1.5 HCLPF Sequence Assessment

The seismic margin assessment evaluates the impact of seismic initiators by determining whether there is adequate margin. This is done by searching for scenarios in which combinations of seismic failures, random events, and failures of human actions could result in an effective seismic capacity less than the SME.

To make this evaluation, seismic failures were added to the fault-tree models developed for internal initiating events, as discussed in the previous section.

The "MIN-MAX" method of evaluating accident sequences at the cut-set level was used to assess the plant-level HCLPF capacity. The MIN-MAX method assesses the accident sequence HCLPF by taking the lowest HCLPF capacity for components analyzed under OR-gate logic and the highest HCLPF capacity for components analyzed under AND-gate logic. Random component failures and human actions are also considered in the evaluation.

The product of this evaluation is identification of the structures and components that arise in the core damage cutsets and that limit the plant-level HCLPF capacity.

### 19.1.5.1.2 Results from the Seismic Risk Evaluation

#### 19.1.5.1.2.1 Risk Metrics

The PRA-based seismic margin assessment investigated the margin incorporated into the U.S. EPR design. This entailed evaluating the plant-level HCLPF, and comparing it to the SME, which is defined as a factor of 1.67 times the design-basis SSE. That is, the assessment focused on identifying any potential vulnerabilities in the design, defined as components that would not meet the criterion of 95 percent confidence that the probability of failure would be less than 5 percent at the SME. This requirement has been met as described below.

#### 19.1.5.1.2.2 Significant Initiating Events and Sequences

##### Summary of the At-power SMA results

At-power event trees that were quantified to support the SMA analysis are included in Appendix 19A. The at-power event trees quantified to support the SMA analysis include LOOP, ATWS, SLOCA, MLOCA, and LLOCA. The at-power PRA event trees as were utilized directly to perform the SMA accident sequence quantification for each

of these initiating events. The SMA cutsets are reviewed to identify those combinations of seismic failures, random failures and operator error that are most limiting with respect to seismic risk. Since at this stage of the design, detailed fragility evaluations are not available for equipment on the SEL, the SSC on the SEL have been assumed to have a HCLPF greater than or equal to 0.5g. Since there is no differentiation of HCLPF for the various components on the SEL, there is no effort to conclude that certain seismic failures are more likely than others. Rather, since all components on the SSC have the same assumed HCLPF, the limiting seismic cutsets are those cutsets containing the fewest seismic failures. By examining cutsets greater than 1E-3 all cutsets with 3 or less seismic failures are identified (recall that each seismic failure event is assigned a value of 0.1). The at-power SMA cutsets are summarized in Table 19.1-37.

### SMA At-power LOOP Sequences

The LOOP SMA cutsets are included in Table 19.1-37 and the most limiting sequences from an SMA perspective are summarized below:

Single-element seismic sequences: Seismic failure of AC power cabinets, I&C cabinets, EDGs, DC Buses (including Batteries), ESW, and Class 1E UPS represent single-element cutsets

Cutsets with combinations of seismic failures and random failures:

- Seismic failure of CCWS and failure of the RCP seals due to random failure.
- Seismic failure of EFW, failure of one EDG train.

Cutsets with combinations of seismic failures and human actions:

- Seismic failure of EFW and operator failure to start feed and bleed.
- Seismic Failure of either SB HVAC or SCWS and operator failure to open doors and align portable ventilation.
- Seismic failure of reactor trip (due to either reactor trip failures or due to core geometry issues) and operator failure to start Emergency Boration.
- Seismic failure of I&C (either due to I&C seismic failure, or seismic failure of the I&C power supply) and failure to manually trip reactor.

### SMA at-power LOCA Sequences

The LOCA SMA cutsets are included in Table 19.1-37 (for SLOCA, MLOCA and LLOCA initiating events) and the most limiting from an SMA perspective are summarized below:

Single-element seismic sequences:

- Seismic failure of AC power cabinets, I&C cabinets, EDGs, DC Buses, ESW, HVAC, CCWS, Class 1E UPS, or LHSI represent single-element cutsets. For large LOCA, the Accumulators represent an additional single element seismic sequence.

Cutsets with combinations of seismic failures and random failures or operator actions:

- Seismic failure of EFW or MSRT; and failure of one EDG train.
- Seismic failure of EFW or MSRT; and operator failure to start feed and bleed.
- Seismic Failure of SB HVAC (either SAC or SCWS) and operator failure to open doors and align portable ventilation.
- Seismic failure of MHSI and operator failure to initiate fast cooldown.

MLOCA and LLOCA cutsets were also inspected and the results are also included in Table 19.1-37. The SSCs and operator actions important to mitigating MLOCAs and LLOCA are similar to the equipment required to mitigate SLOCAs, with the primary exception that the accumulators are identified as an additional single-element cutset for the LLOCA initiating events.

Seismic failures of key structures that house safety-related systems are also considered as events that are assumed to result in core damage. All Structures housing equipment included on the SEL are included on the SEL so that equipment operation is not compromised because of building failure

### Summary of the Low Power Shutdown SMA results

The Shutdown events trees from the Low Power Shutdown Analysis were used directly for the Shutdown SMA Analysis. The Shutdown event trees were obtained directly from the Low Power Shutdown PRA model (Section 19.1.6 and Appendix 19B). The Shutdown SMA cutsets are reviewed to identify those combinations of seismic failures, random failures, and operator error that are most limiting with respect to seismic risk. Because at this stage of the design, detailed fragility evaluations are not available for equipment on the SEL, the SSC on the SEL have been assumed to have a HCLPF greater than 0.5g. Because there is no differentiation of HCLPF for the various components on the SEL, there is no effort to conclude that certain seismic failures are more likely than others. Rather, since all components on the SSC have the same assumed HCLPF, the limiting seismic cutsets are those cutsets containing the fewest seismic failures. By examining cutsets greater than 1E-3, all cutsets with 3 or less seismic failures are identified (recall that each seismic failure event is assigned a value of 0.1). The Shutdown SMA cutsets are summarized in Table 19.1-37.

Shutdown SMA single-element seismic cutsets are summarized below:

- For various shutdown POS initiators, single element seismic cutsets include AC power cabinets, instrumentation and controls (I&C) cabinets, emergency diesel generators, Class 1E DC Buses or Batteries, and essential service water.

- For a seismic LOCA or uncontrolled level drop in POS C, seismic failure of component cooling water (event component cooling water system) represents a single element cutset.

- For a seismic LOCA in POS C, seismic failure of LHSI is a single element cutset.

Shutdown SMA cutsets with combinations of seismic failures and random failures are summarized below:

- For loss of RHR in POS C, seismic failure of CCWS and failure of the RCP seals due to random failure.

- For seismic LOCA or an uncontrolled level drop in POS C, seismic failure of MHSI and any EDG fails due to random failures.

Shutdown SMA cutsets with combinations of seismic failures and human actions are summarized below:

- For POS C, D and E loss of RHR or LOCA initiating events, seismic failure of SB HVAC (either SAC or SCWS) and operator failure to open doors and align portable ventilation.

- For seismic loss of RHR in POS D, seismic failure of CCWS and operator failure to start LHSI.

- For seismic LOCA or uncontrolled level drop in POS C, seismic failure of either emergency feedwater (event EFW) or main steam relief train (MSRT), combined with operator failure to restart RHR after a LOCA, and operator failure to start feed and bleed.

- For seismic LOCA or uncontrolled level drop in POS C, seismic failure of MHSI and failure to initiate feed and bleed using LHSI.

- For seismic LOCA or uncontrolled level drop in POS C, seismic failure of class 1E UPS and failure to restart RHR.

- For seismic LOCA in POS D or E, seismic failure of CCWS and operator failure to start LHSI.

- For seismic uncontrolled level drop in POS D, seismic failure of either CCWS or MHSI, and Failure to start LHSI.

Shutdown SMA cutsets with combinations of seismic failure, random failures, and human actions are summarized below:

- For POS C, seismic failure of CCWS or LHSI results in loss of RHR, any DG fails due to random causes (results in failure of feed and bleed due to loss of power to at least 1 PSRV) and failure to supply the EFW in the failed train to an operating EFW pump results in late failure of EFW.

- For POS C, seismic failure of CCWS results in loss of RHR, EDG1 fails due to random causes, and failure to align portable ventilation in Safeguards Building 2.

- For seismic LOCA in POS C, seismic failure of EFW or MSRT, failure of train of power, and operator failure to restart RHR after a LOCA.

- For POS C a seismic LOCA or an uncontrolled level drop, with seismic failure of EFW or MSRTs, concurrent with failure to restart RHR after the initiating event (uncontrolled level drop or LOCA) and 1 EDG fails due to random causes.

- For an uncontrolled level drop in POS Cbd, seismic failure of LHSI, any EDG fails due to random causes, and failure of the operators to align the EFW inventory from the failed EFW train results in late failure of EFW.

- For an uncontrolled level drop in either Cbd or Dud, seismic failure of 1EUPS, random failure of EDG3 and failure of the operator to locally isolate the low pressure reducing station.

- For an uncontrolled level drop in either Cbd or Dud, seismic failure of 1EUPS, random failure of EDG4 and failure of the operator to locally isolate the low pressure reducing station and operator failure to align portable ventilation.

- For an uncontrolled level drop in Dud, seismic failure of CCW, random failure of EDG4 and failure of the operator to locally isolate the low pressure reducing station and operator failure to align portable ventilation.

Shutdown SMA RHR LOCA cutsets are summarized below:

- RHR piping fails (assumed in initiating event) and operator failure to isolate the LOCA (automatic isolation is non-seismic).

- RHR piping fails (assumed in initiating event) and DC fails (results in loss of power to all RHR isolation valves).

- RHR piping fails (assumed in initiating event), seismic failure of Class 1EUPS, and random failure of the EDG in the train with the ruptured RHR piping (results in loss of power to all RHR suction isolation valves).

Shutdown SMA Cutsets with no seismic failures (combinations of random failures and/or operator errors only):

- An uncontrolled level drop via the low pressure reducing station, automatic isolation of the ULD fails due to the seismic event (since the automatic isolation signal is dependent on non-seismic I&C), and operator fails to manually isolate the leak.

- In POSs Cau and Cbu when only RHR pumps 2 and 3 are assumed initially operating, random failure of the two EDGs supplying the operating RHR pumps results in loss of the running RHR, and operator failure to start standby RHR trains fails the standby RHR (EFW fails due to loss of power to MSRTs and Feed and Bleed fails due to loss of power to one or more PSRVs).

- Seismic LOCA or Uncontrolled level Drop in POS C, one EDG fails due to random causes, operator fails to restart RHR pumps, and operator failure to crosstie EFW inventory from the failed train results in late failure of EFW.

- Seismic LOCA or Uncontrolled level Drop in POS C, one EFW fails due to random causes, operator fails to restart RHR pumps, and operator failure to crosstie EFW inventory from the failed train results in late failure of EFW.

- Seismic LOCA or Uncontrolled level Drop in POS C, (EDG1 or EDG2 fails due to random causes) AND (EDG3 or EDG4 fails due to random causes), and operator fails to restart RHR pumps.

- Seismic LOCA or Uncontrolled level Drop in POS C, EDG1 and EDG2 fails due to random causes, and operator fails to restart RHR pumps.

- An Uncontrolled Level Drop in POS C or D, EDG3 and EDG4 both fail due to random causes, and operator fails to locally isolate the low pressure reducing station and also fails to align portable HVAC.

#### 19.1.5.1.2.3 Significant Functions, SSC, and Operator Actions

**Summary of the Limiting At-Power SMA Functions and SSC**

The results of the at-power SMA demonstrate that the plant-level HCLPF is equal to or greater than 1.67 times the CSDRS (provided the HCLPF commitments in Table 19-106 are achieved). The following SSC are limiting in determining the plant-level HCLPF capacity:

- The class 1E electrical distribution power cabinets.

- DC – Class 1E Batteries and associated DC Buses.

- Component cooling water system (CCWS).

- Emergency diesel generators.

- Emergency feedwater.

- Essential service water.

- Instrumentation and controls (I&C) cabinets.

- Low head safety injection (LHSI).

- Main head safety injection (MHSI).
- Accumulators (ACC).
- Main steam relief train (MSRT).
- Class 1E UPS – Class 1E Inverters and associated BRA buses.
- Safeguards Building (SBs), heating, ventilation, air conditioning (HVAC) – The safety chilled water System (SCWS) and SB ventilation system electrical division (SAC).
- The associated structures housing this equipment (e.g., the Safeguards Buildings, the Emergency Power Generating Buildings, and the Essential Service Water Pump Buildings).
- Reactor Trip (and maintenance of core geometry such that rod drop is not impeded).

### Summary of the Limiting Low Power Shutdown SMA Functions and SSC

The results of the Low Power Shutdown SMA demonstrate that the plant-level HCLPF is equal to or greater than 1.67 times the CSDRS (provided the HCLPF commitments in Table 19-106 are achieved). The following SSC are limiting in determining the plant-level HCLPF capacity:

- AC – The class 1E electrical distribution power cabinets.
- DC – Class 1E Batteries and associated DC Buses.
- EDGs.
- Component cooling water.
- EFW.
- Emergency service water.
- I&C cabinets.
- Class 1E UPS – Class 1E Inverters and associated BRA buses.
- MSRTs.
- Safeguards Building (SB) heating, ventilation, air conditioning (HVAC) (safety chilled water and SB ventilation system electrical division).
- LHSI/RHR.
- MHSI.

- Low pressure reducing station valves.
- The associated structures housing this equipment (e.g., the Safeguards Buildings, the Emergency Power Generating Buildings, Essential Service Water Pump Building, and the Fuel Building).
- Reactor Trip (and maintenance of core geometry such that rod drop is not impeded).

*Significant Operator Actions*

A number of operator actions are identified in the SMA results (Table 19.1-37) as being important to mitigating seismic accident sequences:

- Isolate the Low Pressure Reducing Station in the event that a seismic event occurs when the low pressure reducing station is in service (automatic isolation is a non-safety function).
- Isolate any RHR LOCA that occurs outside containment: In the event that the seismic category 1 RHR piping fails due to the seismic event, operator action is required to manually isolate the break (automatic isolation is a non-safety function).
- Feed and Bleed: This operator action is required within about 2 hours after a seismic LOOP if it is assumed that EFW fails at time zero. This allows for sufficient time to perform the action, even allowing for the fact that operator response may be degraded due to the seismic event. Feed and Bleed is also required after a LOCA during POS C and for SLOCA and MLOCA when secondary cooling fails.
- Fast Cooldown: Given a LOCA with MHSI failure, the operators would initiate a fast cooldown to allow LHSI injection with accumulators.
- Ventilation Recovery: Operator action is credited to open doors and align portable ventilation following a failure of SAC or QKA to maintain temperatures in the Safeguards Building that will support operation of the vital equipment. More than 4 hours is required before any critical equipment reaches temperatures that would compromise equipment functionality.
- EBS Start for an ATWS event: This operator action is assumed to be required in less than 30 minutes.
- RHR Restart after a LOCA in POS C: The RHR pumps may be required to trip on a LOCA due to low coolant level, therefore requiring a manual restart. Additionally if a significant LOCA occurs during shutdown, operator action may be required to manually trip the pumps (the LHSI pump trip on low RCS level is a non-safety function).
- LHSI Start after a loss of RHR in POS D: Provides inventory control after a loss of RHR during mid-loop.

- LHSI Start after a LOCA in POS D or E: Provides inventory control after a LOCA during POS with LHSI pumps not aligned for RHR.

- Open EFW suction crosstie valves to allow EFW inventory in EFW trains that are failed or unavailable to be utilized by EFW trains that are available (OPF-EFW-6H): There is ample time to perform the required action (greater than 6 hours when one train of EFW is available, and greater than 12 hours when 2 trains of EFW are available).

#### 19.1.5.1.2.4 Key Assumptions and Insights

Assumptions and insights from the PRA-based seismic margin assessment are as follows:

- Plant level HCLPF – Based on the seismic margin assessment, it is concluded that the U.S. EPR HCLPF capacity will be equal to or greater than 1.67 times the CSDRS (0.5g pga). This conclusion is dependent on achieving the HCLPF commitments in Table 19.1-106 and additional activities after Design Certification as discussed in ISG-020.

- Seismic PRA model – The SMA analysis considers seismically induced LOOP, SLOCA, MLOCA, LLOCA, ATWS, and various shutdown initiating events. Equipment and structures that are not seismically qualified are not credited in the model. This treatment is judged conservative for a seismic margin assessment because of inherent seismic capacity and ruggedness that exists in non-seismic structures and equipment.

- The operator is important in protecting against a seismic event in shutdown conditions when the low pressure reducing station is in service (especially in reduced inventory conditions such as mid-loop). The automatic signal that closes the reducing valves on low RCS level is a non-safety signal, and the valves that are typically utilized to control letdown flow through the low pressure reducing station (the low pressure reducing station valves) are provided with a power supply that is not seismically qualified such that a significant seismic event will require operator action to isolate the LP reducing station, and will disable the equipment that is typically utilized to isolate low pressure reducing station flow. Therefore, a seismic event could both cause an uncontrolled level drop event, result in failure of the I&C control signals (the low RCS level signal that automatically closes the low pressure reducing valves is a non-class signal), and significantly degrades the ability of operations staff to respond to the event.

A COL applicant that references the U.S. EPR design certification will confirm that the U.S. EPR PRA-based seismic margin assessment is bounding for their specific site, and will update it to include site-specific SSC and soil effects (including sliding, overturning liquefaction and slope failure).

#### 19.1.5.1.2.5 Sensitivities and Uncertainties

Uncertainties are taken into account explicitly in the fragility development and in evaluating non-seismic failures of equipment. Because the seismic margin assessment is primarily qualitative, no sensitivity studies are conducted.

### 19.1.5.2 Internal Flooding Risk Evaluation

#### 19.1.5.2.1 Description of Internal Flooding Risk Evaluation

##### 19.1.5.2.1.1 Methodology

Based on good spatial separation between safety buildings containing safety trains in the U.S. EPR design, a bounding internal flooding analysis method is used to evaluate risk from the internal flooding events. The aim of this bounding analysis is to show that the CDF/LRF, as a result of a more detailed internal flooding evaluation, will not change the conclusion that the overall CDF/LRF meets the U.S. EPR design objective.

The bounding internal flooding analysis method implies that the floods are analyzed for the entire building, that the worst PRA scenario resulting from the failure of all SSC in the building is modeled, and that the total building flooding frequency is applied to that scenario. Based on this approach, for each building containing SSC credited in the PRA, the internal flooding evaluation is performed in the following steps:

- Calculate flooding frequency based on the flooding sources and piping segments. Where detailed design information is not available, use conservative estimates of flooding frequency from available industry references.
- Analyze possible flooding scenarios for each location and, based on the PRA model, select the worst scenario.
- Apply the total building flooding frequency to the worst scenario, and calculate the corresponding CDF and LRF.

##### 19.1.5.2.1.2 Internal Flooding Frequencies

**Locations Selected for Internal Flooding Risk Evaluation**

The eight U.S. EPR buildings that contain SSC credited in the PRA analysis, and are selected for internal flooding risk evaluation, are listed below:

- The four SBs.
- The Fuel Building (FB).
- The Reactor Building (RB) annulus.

- The ESW Pumphouses.
- Turbine Building (TB).

SWGR Building and EPGBs, which also contained SSC credited in the PRA analysis, are screened out from the flooding analysis, based on the following: SWGR Building does not contain significant flooding sources; a flood in an EPGB is not likely to cause an initiating event, and it would only disable the corresponding EDG.

The principal protective measure for these buildings is physical separation. Below elevation +0 feet, division walls provide separation and serve as flood barriers to prevent floods from spreading to adjacent divisions. These division walls are watertight, have no doors, and have a minimal number of penetrations. Water is directed within one division to an elevation below, where it is stored. Above elevation +0 feet, a combination of watertight doors and openings for water flow to the lower building levels prevent water ingress into adjacent divisions. In SBs only the ESW system contains enough water to rise to the +0 elevation, and potentially propagate to the adjacent SB. Safety sensors in the sumps are installed to ensure a prompt trip of the affected ESW pump. Propagation between buildings through a backflow from the drain collection headers is also not visible because the sump pumps discharge lines from all four SBs are independently routed to the waste collection tank in the Radwaste Building.

Buildings that have a physical connection (door) are analyzed together. The connections exist between the FB and SB 1 and SB 4, and between RB annulus and SB 2 and SB 3. These connections are taken into account when developing flooding scenarios, as defined in Section 19.1.5.2.1.3.

### Flooding Frequencies for the Selected Locations

In developing flooding frequencies, all plant systems that transport fluid through a selected location are considered as potential flood sources. For each selected location, the following flooding sources were considered in the analysis:

- Equipment (e.g., piping, valves, pumps, tanks or pools) in the location.
- Plant external sources of water (i.e., ultimate heat sink reservoirs), that are connected to the location through some system or structure

In-leakage from the other flood locations (e.g., back flow through drains, doorways, etc) was not considered based on the spatial separation between buildings, as discussed above.

Sources of information for identifying the flood sources within each flood area of the plant included the following:

- The Plant-Specific Spatial Database.
- General Arrangement Drawings.
- Piping and Instrumentation Diagrams.
- Design Basis Flood Calculations.

The method chosen to evaluate internal flooding frequencies for the locations/ buildings selected above is based on the EPRI TR-102266 Pipe Failure Study (Reference 40). This method gives a pipe break frequency based on the number of the pipe segments for different sizes of pipes and for different systems. In the design certification phase PRA, sufficient information is only available to calculate the internal flooding frequency based on the piping segments, because information on the length of the piping or the number of welds is not available at this time. Therefore, for each building selected above, the flooding frequency is calculated based on the number of pipe segments as determined by the piping and instrumentation diagrams (P&ID). Both operating systems and standby systems (including the fire water system) were considered in the evaluation. The systems were chosen based on their flooding potential; only systems with the potential to cause a significant flooding event were selected. A significant flooding event is defined for a given building as an event that results in a flood level of more than one foot in any room of that building. Main feedwater (MFW) and main steam (MS) pipes in the MFW/MS valve rooms on the top of SB 1 and SB 4 are not considered as flood sources in these buildings, because these floods do not have a potential to affect any other location inside the building. These pipe breaks are also evaluated as a part of the high energy line break (HELB) analysis.

The TB also houses SSC that are credited in the PRA analysis. No P&IDs are available yet for the systems located in the TB; therefore, a generic flooding event frequency is used. It is taken from NUREG/CR-2300, PRA Procedures Guides, (Reference 41).

The U.S. EPR locations selected for the flooding analysis and corresponding flooding frequencies are defined in Table 19.1-38—Changes in U.S. EPR Flooding Scenarios and Frequency Calculation. The same uncertainty distributions (lognormal, with error factor of 5) are used as in the flooding frequency source document.

These distributions are shown associated with the flooding scenario frequencies, which will be discussed in the next section (see Table 19.1-39—Flooding Scenarios Description and Frequency Calculation).

#### 19.1.5.2.1.3 Flooding Scenarios

For each location/building selected for the flooding analysis, the worst flooding scenario is defined, assuming that all mitigating equipment at the location is lost. Other effects of pipe breaks, like jet impingement, spray, pipe whip, or humidity, were

not specifically evaluated because all equipment at a location is considered failed. The frequency of the selected flooding scenario is estimated based on the building flooding frequencies as defined in Table 19.1-38

The scenarios defined for each area are described in Table 19.1-39. Table 19.1-39 gives the flooding scenario identifiers and descriptions, summarizes the effects the flood has on mitigating systems and gives the scenario frequencies with the basis for their calculation.

Flooding scenarios are quantified using the same fault tree and event tree logic used in the Level 1 internal events evaluation. Mitigating systems that are assumed to be unavailable in a flooding scenario are disabled in the fault tree for this specific scenario.

One of the more complex scenarios for which its own event tree is developed, as presented in Appendix A, is the flood in the RB annulus. In this scenario, different operator actions are credited to isolate a pipe break before a significant flood level occurs, depending on the status of the normally closed isolation fire water distribution systems (FWDs) MOVs and the size of the break. Unisolated flooding inside the RB annulus could reach the level of the electrical penetrations to the containment, Control and power cables pass through the annulus in air-tight conduits. They enter the containment through the connection boxes, whose ability to withstand the effects of flooding is not known. In this evaluation, given that no specific information is available, it was conservatively estimated that, if flooded, the connection boxes to the containment would fail and the connection with the containment, including all instrumentation, would be lost and core damage is assumed. A successful isolation is analyzed as a flooding in the adjacent buildings SB2 and SB3 by considering a possibility that the doors between the RB annulus and SB 2 and SB3 could fail open at a certain flood level. No credit is given for the doors holding under a water pressure. If propagation occurs, the safety systems in the adjacent buildings are considered failed.

#### 19.1.5.2.2 Results of Internal Flooding Evaluation

##### 19.1.5.2.2.1 Risk Metrics

The total CDF from internal flooding events is 6.1E-08/yr, less than 1E-07/yr. This is well below the NRC goal of 1E-04/yr (SECY-90-016, Reference 30) and the U.S. EPR probabilistic design goal of 1E-05/yr. Mean value and associated uncertainty distribution can be found in Section 19.1.5.2.2.7.

##### 19.1.5.2.2.2 Significant Initiating Events

The significant flooding initiating events modeled (flooding scenarios) and their contribution to the internal flooding CDF are given in Table 19.1-40—U.S. EPR

Initiating Events Contributions - Level 1 Internal Flooding (Contributing More than 1% to Internal Flooding CDF). Only those initiating events that contribute more than one percent to the total flooding events CDF are listed in the table. All flooding initiating events and their contributions are illustrated in Figure 19.1-12—U.S. EPR Initiating Event Contributions - Level 1 Flooding. As can be seen from Table 19.1-40 and Figure 19.1-12, the flood contained in the annulus dominates the internal flooding CDF. Although this scenario has a low frequency, it is conservatively modeled as directly resulting in core damage if the connection boxes to the containment fail as a result of the flood.

The next biggest contributor to the flooding risk is a flood in SB 1 or SB 4 that extends to the FB. This flood is divided into three categories: floods caused by a break in SIS piping (the second largest contributor) or the emergency feedwater system piping (the fourth largest contributor) and floods caused by a break in any other system (the largest contributor). All of these pipe breaks are assumed to disable one division of all safety systems, and the manual cross connection of the EFW tanks (the tanks make-up would be required). The important contribution of those specific buildings could be attributed to the PRA modeling assumption on the initially running CCW trains, and on the location of the CCW switchover valve, so that a flood in SB 1 or SB 4 could disable one CCW common header. In addition, breaks in the SIS piping (larger than 2") could also disable IRWST function by draining its inventory outside containment and disabling any safety injection or feed and bleed actions.

The next biggest contributor to the flooding risk is a flood contained in the annulus. Although this scenario has a low frequency when considering isolation failure, it is conservatively modeled to directly result in core damage if the connection boxes to the containment fail as a result of the flood.

The TB flood relatively high contribution could be mainly explained by the high flood frequency. All other flooding scenarios contribute less than one percent to the total flood CDF.

#### 19.1.5.2.2.3 Significant Cutsets and Sequences

The top 100 cutsets from the RS output for quantification of the flood CDF are evaluated in detail. Cutset contributions to the internal flooding CDF are relatively evenly distributed; only the first nine cutsets contribute more than one percent. The number of cutsets that contribute to 95 percent of the flooding CDF is larger than 30,000.

The significant cutsets for the internal floods are shown in Table 19.1-41—U.S. EPR Important Cutsets - Level 1 Flooding (Top 100 Events). In this table, the first 100 cutsets are grouped based on the associated initiating event and on their similar impact on mitigating systems. The corresponding sequence in the event tree is identified for

each group. The table indicates, for each group, its number, the number of cutsets in the group, the total CDF of the group, its percentage contribution to the total flooding CDF (contribution of the group itself and cumulative contribution), a representative cutset and the description of the sequence of events. As shown in Table 19.1-41, the top 100 cutsets are grouped into 17 groups, representing over 40 percent of the flooding CDF. These groups are discussed below:

Groups 1, 2, and 3 in Table 19.1-41 represent cutsets that account for approximately 20 percent of the internal flooding CDF. These groups describe: the floods due to a SIS pipe break in SAB4 that fall IRWST (all injection and feed and bleed function) and all division 4 pumps. In Group 1, the flood is followed by a loss of CCW CH2 and subsequent RCP seal LOCA leading directly to the core damage, because of the injection failure. In Group 2, the flood is followed by a PAS failure disabling MFW/ SSS, and an failure to make-up to the EFW tanks (manual EFW crosstie, and feed and bleed are disabled by the flood). In Group 3, the flood is followed by a PS system failure, disabling MFW/SSS full load isolation. Operator error to control EFW/MSRT leads to a total loss of secondary cooling and core damage, because the flood disabled feed and bleed.

Groups 4, 5, 6 and 7 in Table 19.1-41 represents cutsets that account for approximately 15 percent of the internal flooding CDF. These groups describe the floods due to a FWDS pipe break in annulus which, if not isolated, would fail the connection boxes to the containment and lead to core damage. The difference between these four groups is in the manner and timing isolation has failed, as described in Table 19.1-41.

Groups 8 and 9 represent the RCP seal LOCA sequences following a flood in the SB 1 or SB 4 including the FB. A flood in SB 1 or SB 4 could directly lead to a loss of CCW CH2 and consequently in a loss of seal cooling to RCPs if, at the time of the accident, TB cooling is supplied from the CCW header (the seal injection is disabled because of the flood propagation to the FB, which hosts the CVCS). A failure to isolate seals for one of those two RCPs leads to a seal LOCA with an assumed probability of 0.2. The mechanism by which mitigation of the seal LOCA is failed differs slightly between these groups. It involves either a failure of long-term cooling of the IRWST by the LHSI heat exchanger that require start of the standby CT fans (the SAHRS is unavailable due to the flood), or failure of secondary heat removal. In Table 19.1-41, which accounts for the top 100 cutsets, seal LOCA sequences represent around 20 percent of the flooding CDF. Overall, a consequential seal LOCA accounts for about 65 percent of the flooding CDF.

Groups 10, 15 and 17 represent the sequences following a flood in one of the Safeguard Building that disables one of the EFW trains and manual crosstie between EFW tanks. This flood is followed by a PAS failure disabling MFW/SSS. Dependent operator actions to refill EFW tanks or to start feed and bleed lead to a total loss of core cooling and core damage.

Groups 11 and 16 represent the sequences following a flood in one of the Safeguard Building that disables one of the safety divisions. This flood is followed by a consequential LOOP and failure of EDGs supporting other divisions.

Groups 12, 13 and 14 represent sequences with a loss of all feedwater and an operator failure to initiate feed and bleed. A flood in the TB disables the MFW and the SSS, followed by an independent failures of EFW pumps and failure of feed and bleed in Groups 12 and 13, and a failure of total steam removal in Group 14.

The important CDF sequences for internal floods are presented in Table 19.1-128—U.S. EPR Important Sequences – Level 1 Flooding Events (Contributing more than 1% to the Total CDF). The "important" CDF sequences are defined as those sequences with a sequence frequency greater than one percent of total at-power CDF, as presented in Section 19.1.8.1. For each sequence, Table 19.1-128 gives corresponding event tree, sequence number, event tree sequence identifier, the sequence frequency, and a brief description. It also connects the sequence to the corresponding cutset group in Table 19.1-41, which gives a more detailed description of the sequences.

#### 19.1.5.2.2.4 Significant SSC, Operator Actions and Common Cause Events

Table 19.1-42 through Table 19.1-48 show the important contributors to the internal flooding CDF. Importance is based on the FV importance measure (FV ≥0.005), or the RAW importance measure (RAW ≥2).

Table 19.1-42—U.S. EPR Risk-Significant Components based on FV Importance – Level 1 Internal Flooding shows the top risk-significant SSC based on the FV importance measure. The ESW pump trains 2 and 3 have the highest FV. This could be explained by an overall high contribution of the consequential RCP seal LOCA sequences that follow a flood in a SB that require a switchover to standby CCW/ESW train, and a long-term cooling by LHSI heat exchangers.

Table 19.1-43—U.S. EPR Risk-Significant Components based on RAW Importance - Level 1 Flooding shows the top risk-significant SSC based on the RAW importance measure. The two most important components are two uninterruptible power supply switchboards that play an important role in preventing and mitigating RCP LOCAs. The RCP pump breakers and the thermal barrier safety valves are also important in prevention of the RCP LOCA, while components related to the MFW/SSS operation are important for the mitigation of all transients, given that a manual EFW tanks crosstie is likely to be disabled by a flooding event.

Table 19.1-44—U.S. EPR Risk-Significant Human Actions based on FV Importance - Level 1 Internal Flooding shows the risk-significant human actions based on the FV importance measure. Operator action to trip RCPs on a loss of bearing cooling has the highest FV. This could be explained by an overall high contribution of the consequential RCP seal LOCA sequences that follow a flood in a SB. This action is

followed in importance by three operator actions related to isolation of the FWDS breaks in annulus. The other important operator action based on the FV is the failure to recover room cooling locally following a loss of ventilation. The high importance of that action reflects the importance of ventilation dependencies in the plant risk in general.

Table 19.1-45—U.S. EPR Risk-Significant Human Actions based on RAW Importance - Level 1 Internal Flooding shows the risk-significant human actions based on the RAW importance measure. The most important operator action based on the RAW value is the operator failure to isolate a FWDS break in the annulus.

Table 19.1-46—U.S. EPR Risk-Significant Common Cause Events based on RAW – Level 1 Internal Flooding shows the risk-significant common-cause events based on the RAW importance measure. In addition to the common cause failure of the safety batteries that is important for the consequential LOOP scenarios, the other important common cause events are (i) common cause failure to close FWDS isolation MOVs, important for the flood in annulus, and (ii) various common cause events disabling safety injection, important for the RCP LOCA mitigation.

Table 19.1-47—U.S. EPR Risk-Significant Common Cause I&C Events based on RAW Importance - Level 1 Internal Flooding shows the significant common-cause I&C events based on the RAW importance measures. As illustrated in this table, I&C common-cause events (I/O module, software, sensors, computer processors, or SAS) have a high RAW. This is because a CCF of the signals could contribute to an actuation or control failure of safety systems such as EFWS or SIS. The most important common cause I&C failure is the CCF of all four trains of SG level sensors on all four SGs, which fails the EFWS actuation function in both the protection system and the DAS.

Table 19.1-48—U.S. EPR Risk-Significant PRA Parameters - Level 1 Flooding shows the significant modeling parameters used in the analysis, the significant preventive maintenance performed on the various trains, and the significant LOOP-related basic events. The significance is determined based on either the FV or RAW importance measure, as defined above. This table illustrates a high significance (a high FV) of the parameters modeling the probability of an RCP seal LOCA occurring given a loss of seal cooling. LOOP-related events (a LOOP during 24 hours, or a consequential LOOP) also show a high significance (a high RAW).

#### 19.1.5.2.2.5 Key Assumptions

Some of the key PRA assumptions related to the modeling of internal flooding events are listed below:

- Because of incomplete information on equipment and piping locations, it is assumed that a flood in any building will fail all equipment in this building.

- It is assumed that a flood in SB 1 or SB 4 would propagate to the FB, and vice versa. The door that separates those buildings is supposed to withstand a three-foot water column; it is conservatively assumed that any flood will cause it to fail.

- A flood in an SB is assumed to affect the CCW switchover valves. This is a conservative assumption, since those valves are located exactly at ground level, while all flooding events considered are contained below ground level.

- Floods caused by a break in a system with very large flooding potential (ESWS or DWS) are assumed to be contained below ground level of the affected buildings (SB or FB). This is a reasonable assumption since those systems are automatically isolated if the building sump detects a large flooding event. Moreover, extensive time is needed to flood a building up to ground level, so operator isolation is likely to succeed if automatic isolation failed.

- Flood from SIS piping larger than 2" is treated as a separate flooding scenario and postulated to drain the IRWST outside containment leading to suction failure for all four SIS trains. Smaller SIS piping breaks (less than 2") are included in the FLD-SAB14 FB flood scenario.

- Containment Annulus is structurally designed to withstand pressure if it were filled with water up to the 0.0' level. No information about the structural capacity of the annulus with a flood above ground level is available at this time. However, the doors connecting the annulus area to safeguard buildings 2 and 3 are located at ground level and are designed for a 3 ft level flood. It was assumed that the doors will fail before the concrete structure relieving the pressure on the walls. Flood scenarios above ground level are conservatively assumed to lead to both: (1) propagation to safeguard buildings 2 and 3 (resulting from doors failure) and to (2) penetrations failure in the annulus resulting in a total loss of communication between the containment and the main control room (see the assumption below).

- The probability that the connection boxes of the electrical penetrations that run through the annulus will fail if submerged is estimated to be 1. The guaranteed failure is assumed because of a limited state of knowledge regarding the design of those penetrations. This assumption has a high importance, because the failure of the penetrations is assumed to lead directly to core damage.

- Operator action “OPF-TB CH SO” which considers operator action to switch RCP thermal barrier cooling to the alternate CCW header, is only credited for certain flooding events (FLD-EFW and FLD-SIS) where it has been judged that adequate time is available to perform the action before thermal barrier cooling is lost from the in-service common header.

#### 19.1.5.2.2.6 Sensitivity Analysis

A sensitivity analysis was performed to evaluate the impact of a series of the PRA modeling assumptions on the flooding CDF, including the above assumptions specific for the internal flooding analysis.

The sensitivity results are shown in Table 19.1-49—U.S. EPR Level 1 Flooding Events Sensitivity Studies. Several insights can be drawn from the sensitivity cases analyzed.

Most of the cases studied in Section 19.1.4.1.2.6 for internal events are also analyzed. It allows for a comparison of the impact of the same parameters on the internal events CDF and the flooding CDF. The flooding CDF is very sensitive (somewhat less than internal CDF) to parameters such as HEPs, common cause factors, and HVAC recoveries. The flooding CDF shows a lower sensitivity to assumptions on offsite and onsite power. However, the flooding CDF shows a higher sensitivity to modeling assumption on an RCP seal LOCA probability. This could be explained by the importance RCP LOCA scenarios play in the flooding CDF. The flooding CDF also shows higher sensitivity to the preventive maintenance assumption: having one train in the maintenance for all year. This is because a flooding event is assumed to disable one train itself, and with this assumption two divisions will be lost.

The impact on the CDF of the assumptions specific for the flooding events modeling is also studied; the assumption on the flooding impact on the CCW switchover valve shows a moderate impact on the flooding CDF. This is because without an impact on the CCW switchover valve a single flooding event would not result in a loss of CCW common header and a challenge to the RCP motor or thermal barrier cooling.

#### 19.1.5.2.2.7 Uncertainty Analysis

The results of the uncertainty evaluation for the Level 1 Flooding Events CDF are presented in Figure 19.1-13—U.S. EPR Level 1 Internal Flood Events Uncertainty Analysis Results - Cumulative Distribution for Flood Events CDF.

The uncertainty results are summarized below:

- CDF Internal Flooding Events Mean Value: 7.5E-08.
- CDF Internal Flooding Events 5 percent Value: 7.5E-09.
- CDF Internal Flooding Events 95 percent Value: 2.4E-07.

This ninety-fifth percentile CDF value is more than two orders of magnitude below the NRC goal of 1E-04/yr.

Uncertainty on the Level 1 Flooding PRA results is quantified using a process similar to that described for the internal events in Section 19.1.4.1.2.7. Parametric uncertainty was represented by selecting an uncertainty distribution for each parameter type including flooding initiating events, as described in Section 19.1.4.1.2.7.

#### 19.1.5.2.2.8 PRA Insights

The largest contributor to the flooding CDF is the flood in the SB1 or SB4, which accounts for approximately 50 percent of the overall flooding CDF. The risk from this flood is dominated by the seal LOCA scenarios, because this flood could cause a complete loss of motor cooling to two of the RCPs or, 50 percent of the time, a complete loss of seal cooling to all RCPs. Given a loss of seal cooling, a single failure in the isolation of the RCP seals could result in a seal LOCA with a probability estimated to be 0.2. Seal LOCA sequences contribute to more than 65 percent of the flooding events CDF.

The second largest contributor to the flooding CDF is the flood in the SB4 due to SIS pipe break. It accounts for almost 25 percent of the overall flooding CDF. This high contribution to the flood risk is related to disabling of the IRWST tank, and impacting numerous mitigating functions.

The next largest contributor to the flooding CDF is the flood in the annulus. It accounts for over 15 percent of the overall flooding CDF. This high contribution to the flood risk highlights a vulnerability to annulus pipe break events. It is also the result of conservative assumptions made due to the lack of the detailed design of the annulus electrical penetrations.

Even though several conservative assumptions were made in the analysis, the total risk from flooding events is low with a CDF of less than 1E-07/yr. This illustrates the robustness of the U.S. EPR design and the good spatial separation of the safety trains.

### 19.1.5.2.3 Level 2 Risk Metrics for Flooding Events (LRF and CCFP)

Total LRF from internal flooding events is 8.2E-09/yr. This is well below the NRC goal and U.S. EPR probabilistic design goal of 1E-06/yr. Mean value and associated uncertainty distribution can be found in Section 19.1.5.2.3.6. The number of cutsets contributing to 95 percent of the internal flood LRF is 3,504.

The CCFP from all flooding (at power) large release sequences is approximately 0.14.

#### 19.1.5.2.3.1 Flooding Events Core Damage Release Category Results

The Release Categories and their contribution to the flooding events LRF and the associated CCFP are shown in Table 19.1-50—Level 2 Flooding Events Release Category Results - LRF.

LRF for flooding events is less than 56 percent of the internal events LRF. Approximately 95 percent of the flooding large release is from Release Category RC802. RC802 captures containment failure before vessel failure and these flood-initiated failures are primarily due to SIS flood initiator. The initiator causes SIS pipe

break with loss of SIS IRWST suction in all four divisions and opens a path from inside containment to the safeguard building. Although a factor of 0.5 is used to model SIS piping under water from the flooding event, this scenario dominates the flood LRF. Other important contributors to the internal events LRF are discussed below:

- The second largest contributor is release category RC702 (3 percent of flood LRF) representing creep-induced SGTR from high pressure transient or small LOCA initiators leading to high pressure core damage with a depressurized secondary side.

- The third contributor comes from containment isolation failures mainly RC203 (1.2 percent of flood LRF) with failed vessel, ongoing MCCI and failed SAHRS sprays). The top cutsets for this release category are dominated by the annulus flooding initiator with operator failures to isolate the fire water distribution system and flooding in Safeguard Building 4 initiator with a random failure of electrical Division 1. Sequences from both initiators progress into a hot leg rupture.

The residual LRF is made up of phenomenological challenges which have a small potential of leading to bypass (due to localized destructive hydrogen combustion modes) of the containment.

Other containment failure release categories with a conditional probability greater than 1 percent are:

- Long term containment failure due to basemat failure, without debris flooding, without containment sprays (RC602); this release category is dominated by initiator flood in annulus as it fails all operator actions to start SAHRS and open the basemat flooding lines,

- Scrubbed interfacing system LOCA (RC801) as 0.5 of the SIS flood in the safeguard building is scrubbed corresponding to 0.5 of the CDF from this initiator.

- Long term overpressure without MCCI and failure of sprays for source term mitigation (RC504). This release category is dominated by failure of LHSI injection used as backup to SAHRS (failed by the flood initiator in Division 4 for active flooding and long term steam control.

- Small containment isolation failure (RC206) dominated by flood in annulus initiator with failure of all signals for containment isolation.

#### 19.1.5.2.3.2 Significant Level 2 Flooding Events Cutsets and Sequences

The significant cutsets for the flooding events Level 2 PRA are described in Table 19.1-51—Level 2 Flooding Events Large Release Significant Cutsets. In this table, the top cutsets contributing more than one percent LRF are listed. If there is no cutset in a release category that is greater than one percent of LRF, then only the top cutset in the release category is reported, regardless of its contribution. The columns in the table show: release category, cutset frequency, the basic events in the cutsets

and their descriptions, and a sequence description that includes a description of both the Level 1 and Level 2 aspects of the cutset.

The flooding events LRF is dominated by SIS flooding sequences. Important cutsets that contribute one percent or more to large release for internal events are described below.

**Release Category RC802 – Cutset 1:**

This cutset contributes approximately 67 percent to the flooding events LRF. The sequence represents a flood initiator due to a SIS pipe break in Safeguard Building 4 failing IRWST and all Division 4 pumps. A loss of the running CCW pump (Division 4), with the standby CCW pump (Division 3) in preventive maintenance, leads to a loss of CCW CH2 and a loss of cooling to RCP pumps 3 and 4 motor bearings. Failure to trip either pump, automatically (priority module failure) or manually (operator failure) leads to a RCP seal LOCA, which cannot be mitigated without the IRWST (failure of all injection). After core damage, containment is bypassed due to the break in the SIS piping outside of containment. The break is not considered submerged in 50 percent of the cases leading to a large release, since 50 percent of the piping is above the flood water.

**Release Category RC802 – Cutset 2:**

This cutset contributes approximately 6.9 percent to the flooding events LRF. The sequence represents a flood due to a SIS pipe break in Safeguard Building 4 failing the IRWST and all Division 4 pumps. The loss of the condensate system/turbine bypass fails MFW, SSS in PM. Failure of DWDS makeup results in inadequate EFW inventory and leads to core damage. After core damage, containment is bypassed due to the break in the SIS piping outside of containment. The break is not considered submerged in 50 percent of the cases leading to a large release, since 50 percent of the piping is above the flood water.

### 19.1.5.2.3.3 Significant Flooding Events CDES, Initiating Events, Phenomena and Basic Events

Table 19.1-52—U.S. EPR Core Damage End States Contributions - Level 2 Internal Flooding shows the distribution of core damage end states that contribute to LRF.

The core damage end states contributing above 1 percent to LRF for flooding events all involve high pressure core damage sequences in addition to the interfacing system LOCA CDES. 95 percent of the frequency is associated with ISLOCA end state (IS), about 3 percent of the frequency comes from transient type end states, TRANN (transient end state from flood in annulus) and TR CDES. Seal LOCAs with and without the secondary side depressurized (SS and SSD) account for about 1.5 percent of LRF.

Table 19.1-53—U.S. EPR Initiating Event Contributions - Level 2 Internal Flooding shows the contribution of the flooding initiating events to LRF.

The internal floods LRF is dominated by a single initiator FLD-SIS (95 percent) representing SIS pipe break in Safeguard Building 4 and a loss of IRWST inventory. All contributions from this initiator lead to release categories RC801 (if the release is scrubbed) and RC802 (if the release is unscrubbed). The two other initiators contributing more than 1 percent each are:

- Flood in reactor building annulus FLD-ANN.
- Flood in Safeguard Building 1 or 4 including the Fuel Building FLD-SAB14 FB.

The annulus flood FLD-ANN leads to high pressure transient core damage sequences characterized by CDES TRANN. These sequences are likely to lead to creep induced SGTR if the secondary side is depressurized. Although this initiator leads to a complete failure of signals in the containment, outboard containment isolation is still possible with manual actions.

Tables 19.1-54 through 19.1-57 show the important contributors to the internal flooding LRF. Importance is based on the FV importance measure (FV ≥0.005), or the RAW importance measure (RAW ≥2).

Table 19.1-54—U.S. EPR Risk-Significant Phenomena Based on FV Importance - Level 2 Internal Flooding shows the risk-significant containment phenomena based on FV importance.

The basic events for phenomenological events contributing more than 1 percent to the internal LRF are discussed below:

- The event L2PH ISGTR-TRD=Y contributes 2 percent of the LRF. This event represents a direct containment bypass with induced SG tube rupture from high pressure transient sequences with the secondary side depressurized. This event represents a containment bypass leading to a large release (RC702).
- The event L2PH CCI-DRY contributes 1 percent of LRF. This event represents cases with dry spreading area (debris not flooded with significant MCCI) and appears in all RC203 cutsets (which itself contributes about 1.2 percent of the LRF). The remaining contribution comes from release categories with ongoing MCCI. This event does not represent a direct containment failure but rather characterizes the top contributing sequences to the LRF.
- The event L2PH ISGTR-TR=N contributes to approximately 1 percent of the LRF. This event represents high pressure core damage sequences without SGTR and the secondary side pressurized. This event does not represent a direct containment failure but rather characterizes the top contributing sequences to the LRF.

- The event L2PH CP STMEXP and L2PH STMEXP EX=N each contribute approximately 1 percent of the LRF. These two events represent the probability of ex-vessel steam explosion given a wet pit and no pit failure following steam explosion. These events are modeled under an AND gate and would appear in the same cutsets. This event does not represent a direct containment failure but rather a phenomenological occurrence during the sequences that have indirect impact on containment performance.

- Events L2PH CPIHLR-TR, TP=Y, L2PH ISGTR-SS2D=Y each contribute 1 percent of the LRF. The first event does not represent a containment failure while the second event represents direct containment bypass via induced SGTR.

Other events each contributing 1 percent to the flood LRF characterize the top contributing sequences and do not represent direct containment failure.

Table 19.1-55—U.S. EPR Risk-Significant Phenomena based on RAW Importance - Level 2 Internal Flooding shows the risk-significant containment phenomena based on RAW importance.

The insights from this table are discussed in the Sensitivity Analysis section below.

Table 19.1-56—U.S. EPR Risk-Significant Equipment based on FV Importance - Level 2 Internal Flooding shows the risk-significant equipment based on FV importance.

Table 19.1-57—U.S. EPR Risk-Significant Equipment based on RAW Importance - Level 2 Internal Flooding shows the risk-significant equipment based on RAW importance.

These tables shows a strong consistency with the results of the Level 1 analysis contained in Table 19.1-42 and Table 19.1-43. This is due to the importance of the electrical and HVAC support systems for the operation of the active components that are common to both analyses. The RCS system, and more specifically, the reactor coolant pumps trip failure is the largest contributor to the flood LRF. This is due to the SIS break initiator that floods the pump room in Safeguard Building 4 (with CCWS train 3 unavailable) leading to a loss of the common header cooling to the RCP seals. The resulting seal LOCA cannot be mitigated as all injection is failed following IRWST inventory loss. The next most important systems are the CCWS and the ESWS.

Table 19.1-58—U.S. EPR Risk-Significant Human Actions based on FV Importance - Level 2 Internal Flooding shows the risk-significant human actions based on FV importance.

Table 19.1-59-U.S. EPR Risk-Significant Human Actions based on RAW Importance Level 2 Internal Flooding shows the risk-significant human actions based on RAW importance.

Similarly to the fire LRF, Level 1 operator actions dominate the flood LRF. The importance results both based on FV and RAW did not identify important operator actions. This is driven by the dominance of the flood SIS initiator and the absence of Level 2 PRA actions credited in its mitigation path.

Table 19.1-60—U.S. EPR Risk-Significant Common Cause Events based on RAW - Level 2 Internal Flooding shows the risk-significant common cause events based on RAW importance.

This table shows a strong consistency with the results of the Level 1 analysis contained in Table 19.1-46. This is due to the importance of the electrical and HVAC support systems for the operation of the active components that are common to both analyses. The systems and I&C common cause values do show additional systems with large contributions to the risk. The I&C common cause importance measures are similar to those identified in the fire LRF results.

Table 19.1-61—U.S. EPR Risk-Significant I&C Events based on RAW Importance - Level 2 Internal Flooding shows the risk-significant common cause I&C events based on RAW importance.

There is a very strong correlation between the results of the Level 1 and Level 2 I&C common cause analysis in Table 19.1-47. This is consistent with the role that the I&C system plays in the initiation of protective signals and the control of active components throughout the plant.

#### 19.1.5.2.3.4 Key Assumptions

A key assumption to the Level 2 flooding events modeling is as follows: an unisolated flood in the annulus which results in the loss of instrumentation and signals to and from the containment results in the failure of all Level 2 operator actions except those related to outboard containment isolation valves.

The other important assumption is related to the scrubbing factor applied to accident sequences with SIS flood initiator. The IRWST water inventory discharged into the safeguard building from the SIS break would cover approximately 50 percent of the piping leading to scrubbing of the fission products if any are released.

#### 19.1.5.2.3.5 Sensitivity Analysis

As discussed for internal events (see Section 19.1.4.2.2.6), the focus of sensitivity studies in support of the Level 2 PRA was on the impact of the phenomenological events modeled in the PRA. In general, sensitivity can be assessed by considering what the impact on the results, in terms of LRF, would be if the phenomena were sure to occur or sure not to occur. The reasoning behind this approach and the criteria applied for identification of significant sensitivities are discussed in

Section 19.1.4.2.2.6.

Since the LRF results for floods are dominated by SIS flood initiator sequences discussed in Section 19.1.4.2.2.2 and Section 19.1.4.2.2.3, no individual phenomenological events make a large enough contribution to LRF for these to lead to a significant reduction in LRF when set equal to zero.

The following events can lead to a moderate increase in LRF if set equal to 1:

- The event L2PH STM EXP INV LP represents containment rupture due to in-vessel steam explosion in low pressure sequences. This event can increase the flood LRF by a factor of 5.6 if set to 1.
- L2PH VECF-FA(H) represents very early (before vessel failure) containment rupture due to flame acceleration in high pressure sequences. This event can increase the flood LRF by a factor of 5.5 if set equal to 1.
- L2PH VECF-H2DEF(HL) represents very early containment rupture due to hydrogen deflagrations after hot leg rupture or in a high pressure sequence. This event can increase the flood LRF by a factor of 2.3 if set equal to 1.

The observations made in the internal events case are also relevant in the case of flood events. The events representing hydrogen loads were evaluated as being of small likelihood, even with the use of some conservatism in the modeling. The U.S. EPR Level 2 analysis assessed in-vessel steam explosion causing containment failure as a very low probability event, but not of sufficiently low probability for it to be removed from the model.

In addition, sensitivity studies were performed to investigate the induced SGTR contribution and the key factors that reduce its importance to the LRF results.

These results show that for flood events, as for internal events, depressurization unavailability has a higher impact on RC702 frequency than feed water unavailability. As for fire events, all contributions to flood RC702 come from the Level 2 creep induced SGTR with no contribution from SGTR. Simultaneous unavailability of both depressurization and feedwater leads to 21 percent of the flood LRF. Although the increase factor from the sensitivity is applied to the total frequency of RC702, its low contribution to the flood LRF leads to a moderate increase of the LRF frequency.

#### 19.1.5.2.3.6 Uncertainty Analysis

The results of the uncertainty evaluation for the Level 2 Flooding Events LRF will be presented in Figure 19.1-14—U.S. EPR Level 2 Flood Events Uncertainty Analysis Results - Cumulative Distribution for Flood Events LRF.

The basis for the input uncertainty distributions for systems related basic events and operator actions is discussed in the sub-sections related to the Level 1 PRA. As

discussed in Section 19.1.4.2.2.7, for quantitative evaluation of the overall uncertainty on the LRF, uncertainty distributions are added for the Level 2 phenomenological basic events. These events are identified in the PRA database by use of the prefix "L2PH". The distribution form chosen for these basic events is discussed in Section 19.1.4.2.2.7.

### 19.1.5.2.3.7 PRA Insights

Unlike for internal events, the flood LRF is dominated by bypass sequences resulting from the SIS flood initiator in the Safeguard Building. This flood initiator disables SIS suction in all four trains by draining the IRWST into the Safeguard Building. The next highest contribution is from Level 2 creep induced SGTR (due to the high probability of induced tube ruptures) followed by a small contribution from containment isolation failure.

Unlike for internal events the flood LRF is less sensitive to the unavailability of depressurization and feed water as it only impacts RC702, which has a small contribution to LRF.

The dominance of ISLOCA sequences for LRF, leads to a higher fraction of flood CDF resulting in LRF (about 14 percent). Other phenomenological challenges were not identified as leading to significant probabilities of large release.

The most important systems are related to the RCP seals cooling followed by the cooling chain. The important systems come from the Level 1 core damage sequences. The Level 2 sequences do not credit any additional systems in the SIS flood case that contributes about 95 percent of the flood LRF.

Operator actions are dominated by Level 1 actions.

In terms of non-LRF containment failure release categories, RC602 and RC801 have the highest conditional failure probability. RC602, late basemat failure is dominated by flood in the reactor building annulus leading to failure of all signals to components inside the containment including the MOVs on the passive flooding lines of basemat flooding. RC802 has the exact same fraction as the ISLOCA containment bypass RC802 that contributes to the flood LRF. A split fraction of 0.5 is used for both success and failure to account for the water inventory from the SIS flood itself that would cover the pipe break and therefore scrub the radioactive releases. The detailed analysis supporting the 0.5 value is documented in the flooding analysis and is based on pipe segments counting.

### 19.1.5.3 Internal Fires Risk Evaluation

#### 19.1.5.3.1 Description of Internal Fire Risk Evaluation

##### 19.1.5.3.1.1 Methodology

Based on good spatial separation of the safety trains in the U.S. EPR, a conservative internal fire analysis has been performed in the PRA. The aim of this conservative analysis is to show that the CDF/LRF, as a result of a more detailed internal fire evaluation, will not change the conclusion that the overall CDF/LRF meets the U.S. EPR design objective. The conservative internal fire analysis method implies that the fires are analyzed for an entire fire area (FA) (i.e., a location separated by three-hour fire barriers), that the worst PRA scenario resulting from the failure of all SSC in the FA is modeled, and that the total area fire ignition frequency is applied to that scenario. Based on this approach, for each building containing SSC credited in the PRA, the following steps are performed for the internal fire evaluation.

- Estimate fire frequency based on the available industry experience. Use conservative fire frequency estimates for locations where no available industry data applies.
- Assume that each fire will grow to be a fully developed fire (i.e., do not consider the possibility that the fire will self-extinguish).
- Analyze possible fire scenarios for the location and, based on the PRA model, select the worst-case scenario.
- Credit automatic fire suppression, if the specific fire does not affect it. Manual fire suppression is only credited in the MCR.
- Credit human recovery actions only for control room fires. These actions are implemented from the RSS that is physically separated from, and electrically independent of, the control room.
- Apply the total building/FA frequency to the worst scenario, and calculate the corresponding CDF and LRF.

Since the analyzed fire locations are separated by three-hour fire barriers, as defined in the Fire Hazard Analysis (FHA), the propagation between areas is not considered. Fire-damage models and associated computer codes are not used, since all equipment inside an FA is assumed to fail.

##### 19.1.5.3.1.2 Internal Fire Frequencies

**Fire Areas Selected for Internal Fire Risk Evaluation**

The fire PRA utilizes the partition of the plant into FAs as defined in the FHA. In order to streamline quantification, the numerous FAs in the plant are grouped into a

limited number of PRA fire areas (PFAs) that contain SSC modeled in the PRA analysis, and where a loss of equipment due to a fire would have a similar impact on the plant response. For example, the SB 1 is divided into five PFAs:

- PFA-SB 1-MECH, which includes the pump room of SB 1.
- PFA-SB 1-ELEC, which includes the AC switchgear room and cable floor of SB 1, analyzed together with PFA-SB 1-DC, which includes the DC switchgear room and the I&C room of SB 1.
- PFA-BATT1, which includes the battery room of SB 1.
- PFA-VLVR1, which represents the MFW/MS valve room located on top of SB 1.

U.S. EPR FAs and corresponding FAs modeled in the PRA are defined in Table 19.1-62—U.S. EPR Fire Areas and Corresponding Fire Areas Modeled in the PRA (PFAs), and, for SB 4 and SB 2, illustrated in Figure 19.1-16—Cross-section of Safeguard Building 4 Illustrating the PRA Fire Areas and Figure 19.1-17—Cross-section of Safeguard Building 2 Illustrating the PRA Fire Areas, respectively.

The fire areas where fire would not lead to a fire induced initiator, or does not lead to a plant trip with a significant impact on the mitigating systems, are excluded from the fire evaluation. Based on this limited impact assessment, the four Emergency Power Generating Buildings and the Nuclear Auxiliary Building are excluded from further analysis.

The PFAs defined in Table 19.1-62 are further grouped as fire scenarios are defined (see Section 19.1.5.3.1.3), by selecting one PFA as representative of symmetrical PFAs. The fire scenario is defined and modeled as occurring in the chosen PFA; its frequency is defined as the sum of fire ignition frequencies for all the PFAs represented by the scenario.

### Fire Frequencies for the Selected Fire Areas

The method used to evaluate fire ignition frequencies is based on the U.S. operating experience documented in RES/OERAB/S02-01, "Fire Events – Update of U.S. Operating Experience 1986-1999" (Reference 42). Each evaluated PFA is matched with a corresponding generic location in that reference. Correction factors are also applied to account for the specificity of the U.S. EPR compared to standard U.S. plants (e.g., a larger number of components and locations).

For areas that do not directly correspond to generic locations defined in Reference 42, the method described in Reference 6 is used. This method defines plant-wide fire ignition frequencies for each type of component. An ignition frequency for a specific U.S. EPR PFA is derived by estimating the percentage of components in that area, for each component type. As defined above, the correction factors are also used to

account for the specificity of the U.S. EPR. This method is only used for three PFAs: transformer yard, MFW/MS valve room, and containment pressurizer area. Sources of information for identifying the fire sources within each fire area of the plant included the following:

- Electrical Load List.
- General Arrangement Drawings.
- Fire Hazard Analysis.

The transient fires are not specifically considered in the analysis. It is assumed that they are enveloped in the used generic fire frequencies. For the areas where component specific frequencies are used (transformer yard, MFW/MS valve room and containment), it was assumed that a transient contribution would be very limited.

The PRA fire area frequencies and their basis are defined in Table 19.1-63—Basis for PFA Fire Frequencies. Because these frequencies are based on limited information, CNI are used to model uncertainties in the estimated values. The CNI distribution applies because there is a large uncertainty in the value of the parameter, and the shape of the distribution is basically unknown. These distributions are shown associated with the fire scenario frequencies, which will be discussed in the next section (see Table 19.1-64—Fire Scenarios Description and Frequency Calculation).

#### 19.1.5.3.1.3 Fire Scenarios

As explained above in Section 19.1.5.3.1.2, the worst fire scenarios, one for each selected area, are defined in order to provide a conservative estimate of the internal fire risk. In all but one case, a fire in a PRA FA is assumed to disable all components located within that area.

As discussed in the previous section, close to 30 PFAs, which are defined in Table 19.1-62, are further grouped by selecting one PRA FA as representative of multiple symmetrical PRA FAs. For example, the fire scenario Fire-SAB14-AC represents a fire occurring in the AC switchgear room of SB 1 or SB 4. The scenario is modeled as failing all of Division 4. The frequency of the scenario is calculated as the sum of the fire ignition frequencies in the switchgear rooms of SB 1 and SB 4. Division 4 is chosen as representative and more conservative, since the single train of SAHRS is supplied from Division 4.

Spurious actuation of systems caused by simultaneous electrical hot shorts is considered when applicable. The applied probability of a hot short, given a fire, is 0.17 for an MOV and 0.33 for an SOV (refer to Reference 6).

Automatic fire suppression is credited when available and not affected by the fire. Two 100 percent capacity diesel engine-driven fire pumps ensure that suppression can

be credited even if a consequential LOOP occurs. Manual suppression is credited only in the MCR because it is constantly manned.

Fire scenarios are quantified using the same fault tree and event tree logic used in the Level 1 internal events evaluation. Mitigating systems that are assumed to be unavailable in a fire scenario are not credited. A different value was used for consequential LOOP for fire events leading to a controlled shutdown. The value is estimated based on the value for the consequential LOOP leading to auto scram, reduced by a factor of five. The reduction is based on an estimate that 20 percent of fire initiators leading to a controlled shutdown may result in an automatic plant trip. The thirteen fire scenarios selected in the internal fires PRA are defined in Table 19.1-64. This table gives the fire scenario identifier and description, summarizes the effects the scenario has on mitigating systems, defines the suppression credited, and gives the scenario frequency and basis for that frequency.

#### 19.1.5.3.2 Results from the Internal Fire Risk Evaluation

##### 19.1.5.3.2.1 Risk Metrics

The total CDF from internal fire events is 1.8E-07/yr, less than 1E-06/yr. This is well below the NRC goal of 1E-04/yr (SECY-90-016, Reference 30) and the U.S. EPR probabilistic design goal of 1E-05/yr. Mean value and associated uncertainty distribution can be found in Section 19.1.5.3.2.7.

##### 19.1.5.3.2.2 Significant Initiating Events

All fire scenarios/initiating events modeled and their contribution to the internal fire CDF are given in Table 19.1-65—U.S. EPR Initiating Event Contributions - Level 1 Internal Fires (Contributing more than 1% to Internal Fire CDF). Fire initiating events and their contributions are illustrated in Figure 19.1-15. As can be seen from Figure 19.1-15, 6 out of 13 fire initiating events contribute less than one percent of the internal fire CDF. The fire in the AC/DC switchgear room of SB 1 or SB 4 is the single largest contributor. This could be explained by the importance of electrical Divisions 1 and 4 for the supply of front-line and support systems, as explained in the discussion of system dependencies in Section 19.1.4.1.1.3.

The next three biggest contributors to fire risk are the fire in the MCR, the fire in the mechanical division (pump room) of an SB, and the fire in the MFW/MS valve room. The MCR contribution includes the failure of the operator action to transfer to the RSS following a fire in the MCR. Although this failure probability is low, it is assumed to directly result in core damage. The fire in the mechanical division (pump room) of an SB is modeled as affecting the running train of CCW. The system dependencies detailed in Section 19.1.4.1.1.3 explain this relatively important contribution. The MFW/MS valve room contribution results largely from a specific fire-induced sequence that combines spurious operation of an MSRT and the inability to close two

MSIVs (see Section 19.1.5.3.2.3).

The fifth biggest contributor to the internal fire risk is the fire in the switchgear building. The fire in the switchgear building has effects comparable to an LBOP initiating event with a loss of non-safety electrical power and SBO DGs. Its relatively high risk can be explained by the loss of some non-safety systems and subsystems that are credited in the PRA model.

The last two initiators from Table 19.1-65 contribute close to almost 1 percent to the overall fire risk, and are associated with fires in the pressurizer compartment, leading to a spurious opening of one PSRV, and fires in ESW pump building, disabling one ESW train.

#### 19.1.5.3.2.3 Significant Cutsets and Sequences

The top 100 cutsets from the RS output for quantification of the fire CDF are evaluated in detail. One cutset dominates the fire risk, with individual contributions of about 14 percent to the fire CDF. Due to the lack of detailed design and procedures, conservative assumptions were made for the fires in the MCR, and the importance of this cutset could be attributed to these assumptions. With this exception, cutset contribution to the internal fire CDF is evenly distributed: fewer than 10 cutsets contribute more than one percent to the fire CDF. The number of cutsets that contribute to 95 percent of the fire CDF is larger than 20,000.

The significant cutsets for the internal fires are shown in Table 19.1-66—U.S. EPR Important Cutset Groups - Level 1 Internal Fire Events (Top 100 Events). In this table the first 100 cutsets are grouped based on the associated initiating event and on their similar impact on mitigating systems. The corresponding sequence in the event tree is identified for each group. The table indicates for each group its number, the number of cutsets in the group, the total CDF of the group, its percentage contribution to the total fire CDF (i.e., contribution of the group itself and cumulative contribution), a representative cutset and the description of the sequence of events. As shown in Table 19.1-66, the top 100 cutsets are organized into 17 groups, representing over 45 percent of the fire CDF. These groups are discussed below:

Group 1 represents a single cutset: fire in the MCR and failure of the operators to transfer control to the RSS in adequate time.

Groups 2 through 10 represent the RCP seal LOCA sequences resulting from a fire in the AC/DC switchgear room of SB 1 or SB 4. A fire in the switchgear room of SB 1 or SB 4 results in a loss of the running CCW pumps and, if a switchover to the standby CCW pump is not successful, in a loss of CCW CH 2, and consequently in a loss of cooling to the RCP pump 3 and 4 motors or a loss of thermal barrier cooling to the seals of all four RCPs if they are supplied from this header. This switchover to the standby CCW pump could fail either because of the electrical support failure (Groups

2, 3 and 5), or due to unavailability of the standby CCW train (Groups 4, 6, 7, 8, 9 and 10). The RCP LOCA could occur either because of a loss of the RCP motor cooling and a failure to trip the pumps auto or manually (Groups 2, 3, 4, 6, 7 and 8), or because of a loss of seal cooling (Groups 5 and 10). Loss of seal cooling is initiated by a loss of thermal barrier cooling. When the CVCS suction switchover to the IRWST is required, the CVCS would fail because Division 4 power is required to perform the switchover. This results in a loss of CVCS seal injection, and total loss of the seal cooling to the affected RCPs. A failure to isolate seals for one of the RCPs, leads to a seal LOCA with an assumed probability of 0.2. In Table 19.1-66, which summarizes the top 100 cutsets, the seal LOCA sequences represent over 40 percent of the fire CDF. Overall, a consequential seal LOCA accounts for over 80 percent of the fire CDF. Such high percentage can be contributed to the dual fire impact, disabling the RCP pumps motor or seal cooling and impacting ability to trip the pumps.

Group 11 represent a single cutset also describing a fire in the AC/DC switchgear room of SB 1 or SB 4, followed by a failure of an entire PS. Failure of operator action to provide a long term control of EFW/MSRT fails all SG cooling. Feed and bleed is not available because Division 4 is lost.

Groups 12 and 13 in Table 19.1-66 represent sequences that result from a fire in the MFW/MS valve room. The fire results in a spurious opening of one MSRIV, followed by a fire related failure of two MSIVs to close on demand, resulting in the blowdown of two SGs. Failure to align the RHR or failure of the RHR system results in core damage.

Group 14 represents a fire in the Switchgear Building, causing loss of MFW/SSS, a common cause failure of EFW pumps which disables SG cooling, and feed and bleed fails because of failure to open pressurizer safety relief valves (primary depressurization valves are also disabled by the fire).

Group 15 represents a single cutset also describing a fire in the Switchgear Building followed by a consequential LOOP and an independent CCF of all EDGs to run. Since the SBO DGs are disabled by the fire, this sequence leads to a total SBO. The consequential LOOP sequences represent 5 percent of the overall fire risk.

Group 16 represents a single cutset resulting from a fire in the pressurizer compartment. Spurious operation of any pressurizer valve leads to a small LOCA. A CCF to open the MSRTs prevents success of secondary cooldown. Feed-and-bleed is disabled by the fire.

The important CDF sequences for internal fires are presented in Table 19.1-129—U.S. EPR Important Sequences – Level 1 Internal Fire Events (Contributing more than 1% to the Total CDF). The “important” CDF sequences are defined as those sequences with a sequence frequency greater than one percent of total at power CDF, as presented in Section 19.1.8.11. For each sequence, Table 19.1-129 gives corresponding

event tree, sequence number, event tree sequence identifier, the sequence frequency, and a brief description. It also connects the sequence to the corresponding cutset group in Table 19.1-66, which gives a more detailed description of the sequences.

#### 19.1.5.3.2.4 Significant, SSC, Operator Actions and Common Cause Events

Table 19.1-67 through Table 19.1-73 show the important contributors to the internal fire CDF. Importance is based on the FV importance measure (FV ≥0.005), or the RAW importance measure (RAW ≥2).

Table 19.1-67—U.S. EPR Risk-Significant Components based on FV Importance - Level 1 Internal Fire Events shows the top risk-significant SSC based on the FV importance measure. The ESWS trains, the EDG trains, and the Division 1 and 2 BRA 480V MCCs have the highest FV. The ESW trains are important for the successful CCW switchover and preserving cooling to the CCW common headers and RHR heat exchangers. The presence of EDG trains highlights the importance of consequential LOOP events following a fire. Division 1 and 2 BRA 480V MCCs are also important to support a successful CCW switchover and also to support a partial cooldown function through MSRTs that require a specific combination of two divisions to perform their function.

Table 19.1-68—U.S. EPR Risk-Significant Components based on RAW Importance - Level 1 Internal Fire Events shows the top risk-significant SSC based on the RAW importance measure. The most important components are Division 1 and 2 BRA 480V MCCs and the breakers related to their successful operation. Their importance is discussed in the paragraph above.

Table 19.1-69—U.S. EPR Risk-Significant Human Actions based on FV Importance - Level 1 Internal Fire Events shows the risk-significant human actions based on the FV importance measure. The most important operator actions are operator failure to trip RCP pumps on a loss of motor cooling and failure to transfer to the RSS following an MCR fire. The first action reflects the importance of RCP seal LOCAs in the plant fire risk. The second action is required in order to mitigate the most important fire sequences - a fire in the MCR.

Table 19.1-70—U.S. EPR Risk-Significant Human Actions based on RAW Importance - Level 1 Internal Fire Events shows the risk-significant human actions based on the RAW importance measure. Only five operator actions are considered important based on their RAW value: transfer to the RSS following an MCR fire, operator failure to initiate RHR cooling in twelve hours, operator failure to manually align EFW tanks within six hours, operator failure to trip RCP pumps on a loss of motor cooling, and operator failure to initiate a feed and bleed for transient events. The very high RAW of the failure to transfer to the RSS can be explained by the fact that this event is assumed to lead directly to core damage.

Table 19.1-71—U.S. EPR Risk-Significant Common Cause Events based on RAW Importance - Level 1 Internal Fire Events shows the risk-significant common cause events based on the RAW importance measure. The most important common-cause events based on the RAW values are the CCFs of EFW pumps to start and run, the CCF of standby Cooling Tower Fans to start and run, the CCF of safety related batteries and the CCF of LHSI/MHSI common injection check valves to open. The importance of these common cause events reflects the general importance of the consequential LOOP and the seal LOCA sequences to the total fire risk.

Table 19.1-72—U.S. EPR Risk-Significant Common Cause I&C Events based on RAW Importance - Level 1 Internal Fire Events shows the significant common-cause I&C events based on the RAW importance measure. As illustrated in this table, I&C common-cause events (I/O module, software, sensors, computer processors, or SAS) have a high RAW. This is because a CCF of the signals could contribute to an actuation or control failure of safety systems such as EFWS or SIS. The most important common cause I&C failure is the CCF of all four trains of SG level sensors on all four SGs, which fails the EFWS actuation function in both the protection system and the DAS.

Table 19.1-73—U.S. EPR Risk-Significant PRA Parameters - Level 1 Internal Fire shows the significant modeling parameters used in the analysis, the significant preventive maintenance performed on the various trains, and the significant LOOP-related basic events. The significance is determined based on either the FV or RAW importance measure, as defined above. This table illustrates a high significance (a high FV) of the parameters used in the modeling of an RCP seal LOCA and the parameters used to predict the MS line isolation for the fires in the MFW/MS valve room. LOOP-related events (a LOOP during 24 hours, or a consequential LOOP) also show a high significance (a high RAW).

#### 19.1.5.3.2.5 Key Assumptions

Some of the key PRA assumptions related to the modeling of fire events are listed below:

- Because of incomplete information on equipment and cable locations, it is assumed that a fire in any fire area or building will fail all equipment at this location.
- Spurious operations due to simultaneous hot shorts are considered. The probability of a closed-circuit failure of a cable affected by a fire is set to 0.17 for an MOV circuit and to 0.33 for a solenoid-operated valve (SOV) circuit.
- A fire causing a spurious operation of an MSRT is assumed to affect the MSIV from the same division with a probability of 0.5, and the MSIV from the second division with a probability of 0.1. Based on the spatial separation and the possible combustible loads, these assumptions are likely to be conservative.

- Due to divisional separation measures in the CSR, a fire in the CSR is assumed to disable only one electrical safety division (Division 4 is assumed). This is a conservative assumption because the safety division with the worst impact on the plant mitigation is selected (containing SAHR Train). Non-safety division cables are also assumed to be separated from the safety divisions.

- The risk from fire in the annulus fire area is expected to be negligible. Although the annulus contains safety-related cables for all four safety trains, the frequency of spontaneous cable ignition is reduced because the cables are IEEE qualified. In addition, spatial separation between the safety divisions and limited heat load from the cables in case of fire reduce the likelihood that more than one train will be affected. This assumption will be reevaluated when design inputs on the cable routing in annulus become available.

- For a fire in the electrical area of Safeguards Building 4, the progression of the fire is important to the consequence. A fire that begins in room 34UJK10 027, that fails the two RCP trip breakers located in Room 27, and subsequently spreads to Room 26 without failing power to the RCP is a potential fire risk problem (since it requires an RCP trip while simultaneously disabling the normal method of executing the RCP trip function). This sequence is estimated to be of low probability. The probability of this scenario is represented in the model as basic event "RCP-TRIP-FIRE" which is assigned a basic event probability of 0.20 to account for the low likelihood for this specific combination of events. A loss of RCP motor cooling, with failure to trip the pump is conservatively assumed to result in a seal LOCA.

#### 19.1.5.3.2.6 Sensitivity Analysis

A sensitivity analysis was performed to evaluate the impact of a series of the PRA modeling assumptions on the fire CDF, including the above assumptions specific for the internal fires analysis.

The sensitivity results are shown in Table 19.1-74—U.S. EPR Level 1 Fire Events Sensitivity Studies. Several insights can be drawn from the sensitivity cases analyzed.

Most of the cases studied in Section 19.1.4.1.2.6 for internal events are also analyzed. It allows for a comparison of the impact of the same parameters on the internal events CDF and the fire CDF. The fire CDF is generally less sensitive to some LOOP related parameters that are important for the internal events CDF, such as common cause events grouping or assumptions on LOOP recoveries and DG mission time. A consequential LOOP only accounts for about 4 percent of the fire risk while LOOP events account for more than 50 percent of the internal events risk. Sensitivity to HEPs is equivalent for fire events and for internal events CDF. This confirms that operator actions are important to the fire risk.

The fire CDF shows comparable sensitivity to assumptions on the seal LOCA probability and a higher sensitivity to the volume control tank (VCT) unavailability. This is consistent with the high importance of components and assumptions related to

the mitigation of seal LOCAs, as noted previously in Section 19.1.5.3.2.5. In particular the VCT unavailability assumption is important, because the dominant fire scenario prevents a CVCS switchover to IRWST from succeeding thereby disabling the CVCS seal injection. However, assumptions on the Seal LOCA probability are slightly less important because in the fire risk profile the majority of the seal LOCA sequences are due to a fire-related failure to trip an affected RCP pump.

It is also interesting to notice that the fire CDF is more sensitive than the internal events CDF to the opening logic of the MSRTs. The dominant fire scenario includes the loss of one electrical division; therefore, a single failure in another division would prevent the MSRTs from opening.

The impact on the CDF of the assumptions specific for the fire events modeling is also analyzed. The fire CDF is found to be sensitive to an assumption of a fire affecting both an MSRT and an MSIV. Simultaneous consideration of hot shorts and the modeling assumption on a complete separation of the safety and non-safety divisions in the CSR are not found to have a significant impact on the fire CDF.

### 19.1.5.3.2.7 Uncertainty Analysis

The results of the uncertainty evaluation for the Level 1 Fire Events CDF are presented in Figure 19.1-18—U.S. EPR Level 1 Internal Fire Events Uncertainty Analysis Results - Cumulative Distribution for Fire Events CDF.

The uncertainty results are summarized below:

- CDF Internal Fire Events Mean Value: 2.1E-07/yr.
- CDF Internal Fire Events 5 percent Value: 1.2E-08/yr.
- CDF Internal Fire Events 95 percent Value: 7.4E-07/yr.

This ninety-fifth percentile CDF value is more than two orders of magnitude below the NRC goal of 1E-04/yr.

Uncertainty on the Level 1 Fire PRA results is quantified using a process similar to that described for internal events in Section 19.1.4.1.2.7. Parametric uncertainty was represented by selecting an uncertainty distribution for each parameter type including fire initiating events, as described in Section 19.1.4.1.2.7. Because the internal fire initiating event frequencies are based on limited information, CNI are used to model uncertainties in the estimated values. The CNI distribution applies because there is large uncertainty in the value of the parameter, and the shape of the distribution is basically unknown. These distributions are shown associated with the fire scenario frequencies in Table 19.1-64—Fire Scenarios Description and Frequency Calculation.

#### 19.1.5.3.2.8 PRA Insights

The two cutsets that are the largest contributors to the fire CDF are the result of conservative modeling assumptions made due to the lack of detailed design or detailed procedures.

The scenario that contributes the most to fire risk is the fire in the switchgear room of SB 1 or SB 4. It accounts for over 65 percent of the overall fire CDF. Such a high percentage can be attributed to the importance of a seal LOCA (discussed below) and the fire impact on the CCW common header supplying cooling to the RCP pump motors and thermal barrier. This impact on the CCW common header is the result of the modeling assumptions on the running train of CCW. This scenario dominance also highlights the reliance of some important safety functions (e.g., CCW switchover function, steam relief via MSRTs, or primary bleed) on a multiple number of electrical divisions.

Seal LOCA sequences are very important to the fire risk. They contribute to over 80 percent of the overall fire CDF. Such a high percentage can be explained by a dual fire impact, disabling the RCP pumps motor or seal cooling and impacting ability to trip the pumps.

The importance measures of systems and components for the internal fires risk show that a broad spectrum of SSC are risk-significant based on their FV, but none of them dominates. In other word the safety significance of components to the internal fires risk is equally distributed among systems and plant functions. This shows that there is no obvious vulnerability in the U.S. EPR design with respect to the mitigation of the credible fire scenarios. Even though several conservative assumptions were made in the analysis, the total risk from fire events is low with a CDF of less than 2E-07/yr. This illustrates the robustness of the U.S. EPR design and the good spatial separation of the safety trains in the U.S. EPR.

### 19.1.5.3.3 Level 2 Risk Metrics for Fire Events (LRF and CCFP)

Total LRF from internal fire events is 7.3E-09/yr. This is well below the NRC goal and U.S. EPR probabilistic design goal of 1E-06/yr. Mean value and associated uncertainty distribution can be found in Section 19.1.5.3.3.6. The number of cutsets contributing to 95 percent of the internal events LRF is 33,101.

The CCFP from all fire events (at power) large release sequences is 0.04.

#### 19.1.5.3.3.1 Fire Events Core Damage Release Category Results

The Release Categories and their contribution to the fire events LRF and the associated CCFP are shown in Table 19.1-75—Level 2 Fire Events Release Category Results - LRF.

LRF for fire events is approximately 50 percent of the internal events. Although the top initiator from internal events (SGTR) is not included in the Fire model, the fraction of CDF progressing to a LRF is close to that for internal events. The fire LRF is smaller than the internal LRF and is dominated by creep induced SGTR. Approximately 51 percent of the LRF for fire events comes from Release Category RC702, representing creep induced SGTR. The top cutset (larger than 1 percent) represents pressurizer fire with secondary depressurization and failure of all SIS leading to a Seal LOCA. Other important contributors to the internal events LRF are discussed below:

- The second largest contributor is release category RC205 (about 30 percent of the fire LRF) representing large containment isolation failure with failed vessel recovery without MCCI and failed SAHRS sprays. This release category is highly increased compared to internal events. The top cutsets represent fire in Safeguard Building 4 and a random failure of electrical Division 1 failing containment isolation.

- The third largest contributor is RC404 (about 14 percent of the fire LRF), is also highly increased compared to internal events. This category is dominated by phenomenological failures of the containment at the time of vessel failure (vessel rocketing, hydrogen combustion loads and direct containment heating).

Other containment failure release categories with a conditional probability greater than 1 percent are (1) long term containment failure (with a top cutset representing late steam explosion in the spreading area) without MCCI and failed containment sprays (RC504), (2) small containment isolation failure (RC206) with a loss of Division 4 to the fire initiator and random loss of electrical Division 1 and (3) long term overpressure due to basemat failure with MCCI (RC602).

#### 19.1.5.3.3.2 Significant Level 2 Fire Events Cutsets and Sequences

The significant cutsets for the fire events Level 2 PRA are described in Table 19.1-76—Level 2 Fire Events Significant Cutsets and Sequences. In this table, all of the cutsets contributing more than one percent to LRF are listed. If there were no cutsets in a release category that were greater than one percent of LRF, then only the top cutset in the release category is reported, regardless of its contribution. The columns in the table show: release category, cutset frequency, the basic events in the cutsets and their descriptions, and a sequence description that includes a description of both the Level 1 and Level 2 aspects of the cutset.

The fire event LRF is dominated by induced SGTR with a depressurized secondary side of the SG. Important cutsets that contribute one percent or more to large release for fire events are described below.

**Release Category RC203:**

This cutset group contributes less than 1 percent to the LRF. The sequence represents a fire in the switchgear rooms of Safeguard Building 4 disabling electrical Division 4. Loss of running CCW Division 4 requires switchover to the standby CCW pump which is disabled by a loss of 31BRA. These failures lead to a loss of CCW CH2 and a loss of cooling to the RCP 3 and 4 motor bearings requiring the pumps to trip. The trip is disabled by a fire in the area and failure to trip the RCP supply breaker in the SWGR building results in a RCP seal LOCA. Loss of 31BRA in addition to the loss of Division 4 disables both partial cooldown and feed and bleed. After core damage occurs, the sequence leads to large containment isolation failure because the leak off system lines are open and fail to close due to loss of electrical Divisions 1 and 4 followed by a containment annulus venting failure. There is no pit overpressure failure in cases where complete circumferential failure of the vessel does not occur. Loss of electrical Divisions 1 and 4 leads to failure of SAHRS sprays and significant MCCI occurs following failure of the MOVs on the passive flooding lines to open.

**Release Category RC205:**

This cutset group contributes approximately 29 percent to the LRF. The sequence represents a fire in the switchgear rooms of Safeguard Building 4 that disables electrical Division 4. Loss of the running CCW Division 4 requires switchover to the standby CCW pump which is disabled by a loss of 31BRA. These failures lead to a loss of CCW common header 2 and a loss of cooling to the RCP 3 and 4 motor bearings requiring the pumps to trip. The trip is disabled by a fire in the area and failure to trip RCP supply breaker in the SWGR building results in a RCP seal LOCA. Loss of 31BRA in addition to the loss of Division 4 disables both partial cooldown and feed & bleed. After core damage occurs the sequence enters the low pressure containment event tree after a successful depressurization. Large containment isolation failure occurs due to the leak off system lines being open and failure to close due to loss of electrical Divisions 1 and 4 followed by a containment annulus venting failure. There is no pit overpressure failure in cases where complete circumferential failure of the vessel does not occur. Loss of electrical Divisions 1 and 4 leads to failure of SAHRS sprays. No MCCI occurs with successful opening of the MOVs on the passive flooding lines.

**Release Category RC404 – Cutset 1:**

This cutset group contributes approximately 3.5 percent to the LRF. The sequence represents a fire in the MCR and the operator failure to evacuate and transfer control to the Remote Shutdown Station in time to prevent core damage. After core damage, the sequence remains at high pressure with failure of the depressurization due to the fire initiator. Early containment failure occurs at the time of vessel failure due to vessel rocketing. No pit overpressure failure occurs with complete circumferential failure of

the vessel. There is no significant MCCI with successful passive flooding valves opening and failure to start the SAHRS sprays.

**Release Category RC404 – Cutset 2:**

This cutset group contributes about 4 percent to the LRF. The sequence represents a fire in the switchgear rooms of Safeguard Building 4 disables electrical Division 4. Loss of running CCW Division 4 requires switchover to the standby CCW pump which is disabled by a loss of 32BRA. These failures lead to a loss of CCW common header 2 and a loss of cooling to the RCP pumps 3 and 4 motor bearings requiring the pumps to trip. The trip is disabled by a fire in the area and failure to trip the RCP pump supply breaker in the SWGR building results in a RCP pump seal LOCA. Loss of 32BRA in addition to the loss of Division 4 disables both partial cooldown and feed & bleed. After core damage the sequence remains at high pressure with depressurization failure. Early containment failure occurs at the time of vessel failure due to vessel rocketing. No pit overpressure failure occurs with complete circumferential failure of the vessel. There is no significant MCCI with successful passive flooding valves opening and failure to start the SAHRS sprays.

**Release Category RC 702 – Cutsets 1:**

This cutset group contributes about 1 percent to the LRF. The sequence represents a fire in the pressurizer compartment that induces a small LOCA. CCF of the common suction strainers results in the loss of all injection. After core damage this sequence results in creep induced steam generator tube rupture following a seal LOCA or 2 inch diameter small LOCA with a secondary depressurization.

**Release Category RC 702 - Cutsets 2:**

This cutset group contributes approximately 2.6 percent to the LRF. The sequence represents a Fire in switchgear rooms of Safeguard Building 4 which disables electrical Division 4. CCF of the standby UHS fans results in the loss of CCW common header 2 loss of cooling to the RCP 3 and 4 motor bearings requiring the breakers to the pumps to trip. The trip is disabled by a fire in the area and failure to trip RCP supply breaker in the SWGR building results in a RCP seal LOCA. The CCF of the standby UHS fans also results in the loss of injection and long term cooling of the IRWST. After core damage the sequence results in creep induced steam generator rupture following a 2 inch diameter seal LOCA with a secondary depressurization.

**Release Category RC 702 - Cutsets 3:**

This cutset group contributes approximately 1.4 percent to the LRF. The sequence represents a fire in switchgear rooms of Safeguard Building 4 that disables electrical Division 4. CCF of the standby UHS fans results in the loss of CCW common header 2 loss of cooling to the RCP 3 and 4 motor bearings requiring the pumps to the pumps to

trip. The trip is disabled by a fire in the area and failure to trip RCP supply breaker in the SWGR building results in a RCP seal LOCA. The CCF of the standby UHS fans also results in the loss of injection and long term cooling of the IRWST. After core damage the sequence results in creep induced steam generator rupture following a 0.6 inch diameter seal LOCA with a secondary depressurization

**Release Category RC 702 - Cutsets 4:**

This cutset group contributes approximately 3.3 percent to the LRF. The sequence represents a fire in switchgear rooms of Safeguard Building 4 which disables electrical Division 4. Loss of running CCW Division 4 requires switchover to the standby CCW pump which is in maintenance. These failures lead to a loss of CCW common header 2 and a loss of cooling to the RCP 3 and 4 motor bearings requiring the pumps to trip. The trip is disabled by a fire in the area and failure to trip the RCP supply breaker in the SWGR building results in a RCP seal LOCA. CCF of the common discharge injection valve results in the loss of all injection. After core damage the sequence results in creep induced steam generator rupture following a 0.6 inch diameter seal LOCA with a secondary depressurization

**Release Category RC 702 - Cutsets 5:**

This cutset group contributes about 1.8 percent to the LRF. The sequence represents a Fire in switchgear rooms of Safeguard Building 4 disables electrical Division 4. Loss of running CCW Division 4 requires switchover to the standby CCW pump which is in maintenance. These failures lead to a loss of CCW common header 2 and a loss of cooling to the RCP 3 and 4 motor bearings requiring the pumps to trip. The trip is disabled by a fire in the area and failure to trip the RCP supply breaker in the SWGR building results in a RCP seal LOCA. CCF of the common discharge injection valve results in the loss of all injection. After core damage the sequence results in creep induced steam generator rupture following a 0.6 inch diameter seal LOCA with a secondary depressurization

#### 19.1.5.3.3.3 Significant Fire Event CDES, Initiating Events, Phenomena and Basic Events

Table 19.1-77—U.S. EPR Core Damage End States Contributions - Level 2 Internal Fires shows the distribution of CDES that are analyzed by the containment event tree.

The list of fire CDES contributions to LRF shows a dominance of high pressure core damage sequences.

Approximately 90 percent of the sequences involve Seal LOCA CDES (SS and SSD). 38 percent of the sequences (TRD, SSD and SLD CDES) involve a depressurized secondary side of the SGs. As noted in the discussion of internal events, a depressurized secondary side, especially in the case of a seal LOCA, raises the probability of an

induced SGTR. Many fire initiators lead to the possibility of seal LOCAs; these events may have a depressurized secondary side due to operator actions performing a full secondary cooldown to achieve conditions for LHSI injection. Thus, RC702 is still the largest contributor although no SGTR initiator is modeled.

As in internal events, fire core damage sequences generally depressurize prior to vessel failure, either due to operator intervention or an induced hot leg rupture.

Table 19.1-78—U.S. EPR Initiating Events Contributions - Level 2 Internal Fires shows the contribution of the fire initiating events to LRF.

Of the listed initiators, only IE-FIRE-PZR involves a LOCA, but with only 1 PSV open, this is a small LOCA. Small LOCA sequences are modeled as proceeding to core damage at high pressure. The events IE FIRE-SAB14-ELEC, IE FIRE-SAB-MECH, IE FIRE-ESW, and IE FIRE-SWGR all correspond to fire initiators for which seal LOCAs are a possibility. The increased possibility of a thermally induced steam generator tube rupture with seal and small LOCA (with secondary depressurized) contributes to the importance of these initiating events in the LRF results. All the listed initiating events are modeled as having some susceptibility to flame acceleration hydrogen combustion events due to the high pressure core damage sequences that lead to hydrogen loads before and at vessel rupture.

The internal fire LRF is dominated (88 percent) by a single initiator representing a fire in the switchgear rooms of Safeguard Building 1 or 4 IE FIRE-SAB14-ELEC. This initiator represents a loss of both AC and DC power supplies. The next largest contributors are, fire in the main control room IE FIRE-MCR (5 percent), fire in the pressurizer compartment IE FIRE-PZR and fire in the mechanical pump room of any safeguard building IE FIRE-SAB-MECH (each contributing 2 percent), fire in the switchgear building IE FIRE-SWGR and fire in the Essential Service Water Pump Building IE FIRE-ESW (each contributing 1 percent).

Table 19.1-79 through Table 19.1-82 show the important contributors to the internal fire LRF. Importance is based on the FV importance measure (FV ≥0.005), or the RAW importance measure (RAW ≥2).

Table 19.1-79—U.S. EPR Risk-Significant Phenomena Based on FV Importance - Level 2 Internal Fires shows the risk-significant containment phenomena based on FV importance.

The basic events for phenomenological events contributing more than 10 percent to the LRF are discussed below:

- The event L2PH NO CCI represents sequences without ongoing MCCI with successful basemat flooding. This event contributes 46 percent to the fire LRF and

does not represent a direct containment failure but rather characterizes sequences leading to LRF.

- L2PH PF-VF NO-CBV=N represents sequences without pit failure at the time of vessel rupture for cases without circumferential break of the vessel. This event contributes 35 percent to the fire LRF and does not represent a direct containment failure but rather characterizes sequences leading to LRF.

- L2PH ISGTR-SS2D=Y and L2PH ISGTR-SS0.6D=Y contribute to approximately 49 percent of LRF. These events represent a direct containment failure via bypass following SGTR with secondary depressurized (contribution from Level 2 creep induced ruptures only).

- L2PH CBV HP contributes 11 percent to the fire LRF representing a complete circumferential rupture of the vessel in high pressure sequences leading to vessel rocketing. This event represents containment failure at vessel rupture and would lead to a release category in the group RC400.

- L2PH PF-VF CBV=N contributes 11 percent to the fire LRF and represents pit overpressure at high pressure vessel failure (from circumferential breach of the vessel) leading to melt plug failure. This event does not represent a direct containment failure but rather characterizes high pressure sequences leading to LRF.

- The next basic event representing direct containment failure is L2PH EARLYCF FA(HP) contributing 1 percent to the fire LRF. This event represents the likelihood of containment failure occurring due to loads from an accelerated flame originating in the lower or middle equipment rooms. These rooms are expected to experience short term transient accumulation of hydrogen during a high pressure core damage sequence, due to hydrogen release at vessel failure. This event was applied for all high pressure core damage sequences that remain at high pressure. The evaluation of this event includes consideration of the likelihood of continuous burning (rather than accumulation) of released hydrogen and also takes into account the short term nature of the localized hydrogen peak concentration, since this is reduced in the longer term by action of recombiners. Accelerated flames were considered as leading to severe loads on the containment structure even in the absence of deflagration-to-detonation transition. Only limited credit was taken for reduction of the assessed probabilities for mixtures that are close to the concentration limits for flame acceleration.

- Many events have RAW values greater than 2. These events represent containment rupture and leakage from hydrogen loads as well as in vessel steam explosion and vessel rocketing.

Table 19.1-80—U.S. EPR Risk-Significant Phenomena Based on RAW Importance-Level 2 Internal Fires shows the risk-significant containment phenomena based on RAW importance.

The insights from this table are discussed in the Sensitivity Analysis section below.

Table 19.1-81—U.S. EPR Risk-Significant Equipment based on FV Importance - Level 2 Internal Fires shows the top risk-significant SSC based on FV importance.

This table shows a strong consistency with the results of the Level 1 analysis contained in Table 19.1-67. This is due to the importance of the electrical and HVAC support systems for the operation of the active components that are common to both analyses. The largest contributing group is the ESW system followed by the electrical system followed by SIS. These groups contribute more than 40 percent each. Overall important systems are similar to those identified in the internal events LRF analysis.

Table 19.1-82—U.S. EPR Risk-Significant Equipment based on RAW Importance - Level 2 Internal Fires shows the top risk-significant SSC based on RAW importance.

As with the FV results, this table shows a strong consistency with the results of the Level 1 analysis contained in Table 19.1-68. This is due to the importance of the electrical and HVAC support systems for the operation of the active components that are common to both analyses.

Table 19.1-83—U.S. EPR Risk-Significant Human Actions based on FV Importance-Level 2 Internal Fires shows the risk-significant human actions based on FV importance.

Similar to the internal events LRF, the Level 1 operator actions dominate the internal LRF. The three largest contributors are actions related to RCP trip failure, transfer from the MCR to the RSS, and failure to recover room cooling. An examination of the operator actions based on RAW values did not show in additional Level 2 operator actions as significantly contributing to the LRF. As mentioned for internal events (Section 19.1.4.2.2.4), it can be observed that the main Level 2 actions considered in time frames that are relevant for LRF are (a) backup actions for containment isolation, (b) operator entry to the OSSA and manual depressurization of the RCS. As also discussed in Section 19.1.4.2.2.4, neither of these actions are single failures from the point of view of preventing large release.

Table 19.1-84—U.S. EPR Risk-Significant Human Actions based on RAW Importance-Level 2 Internal Fires shows the risk-significant human actions based on RAW importance.

It is noted that no Level 2 operator actions are important for LRF based on RAW. The reasons for this are the same as those discussed above for FV importance.

Table 19.1-85—U.S. EPR Risk-Significant Common Cause Events based on RAW Importance - Level 2 Internal Fires shows the risk-significant common cause events based on RAW importance.

This table shows a strong consistency with the results of the Level 1 analysis contained in Table 19.1-71. This is due to the importance of the electrical and HVAC support systems for the operation of the active components that are common to both analyses. Common cause events have been ranked based on RAW values for systems and I&C equipment. SG level sensors CCF has the largest RAW of the I&C systems. This is because the failure probability is low and these sensors are involved in the operation of the EFWS. Failure of EFWS leads to high pressure scenarios with the secondary depressurized which leads to unscrubbed SGTR (RC702) and is the largest contributor to the fire LRF.

Table 19.1-86—U.S. EPR Risk-Significant I&C Common Cause Events based on RAW Importance - Level 2 Internal Fires shows the risk-significant I&C common cause events based on RAW importance.

There is a very strong correlation between the results of the Level 1 and Level 2 I&C common cause analysis. This is consistent with the role the I&C system plays in the initiation of protective signals and the control of active components throughout the plant.

#### 19.1.5.3.3.4 Fire Events Level 2 Key Assumptions

A key assumption to the Level 2 fire events modeling is as follows: a fire in the main control room with operator failure to evacuate in a timely manner resulting in core damage fails all Level 2 operator actions that may be required in the early stages of the severe accident.

#### 19.1.5.3.3.5 Fire Events Level 2 Sensitivity Analysis

As discussed for internal events (Section 19.1.4.2.2.6), the focus of sensitivity studies in support of the Level 2 PRA was on the impact of the phenomenological events modeled in the PRA. In general sensitivity can be assessed by considering what the impact on the results, in terms of LRF, would be if the phenomena were sure to occur or sure not to occur. The reasoning behind this approach and the criteria applied for identification of significant sensitivities are discussed in Section 19.1.4.2.2.6.

Compared to the internal LRF results, the fire LRF shows a greater number of phenomenological events with RAW values larger than 2. The largest observed sensitivity to an individual phenomenological event is similar to the internal LRF. The following events can lead to a significant increase in the fire LRF if set equal to 1:

1. L2PH VECF-FA(H) and L2PH VECF-FA(H)L represent respectively very early (before vessel failure) containment rupture and leak due to flame acceleration in high pressure sequences. These events can increase the fire LRF by factors of 13.9 and 6.8 respectively if set equal to 1.

2. The events L2PH STM EXP INV HP and L2PH STM EXP INV LP represent containment rupture due to in-vessel steam explosion in high and low pressure sequences respectively. These events can increase the fire LRF by factors of 13.8 and 11.9 respectively if set to 1.

3. L2PH CBV HP represents containment rupture following vessel rocketing due to a complete circumferential rupture of the vessel leads to a fire LRF increase factor of 11.9 if set to 1.

4. L2PH EARLYCF FA(HP) and L2PH EARLYCF FA(HP)L represent respectively early (at vessel failure) containment rupture and leak due to flame acceleration in high pressure sequences. These events can increase the fire LRF by factors of 11.1 and 10.4 respectively if set equal to 1.

5. L2PH EARLYCF DEF(H)L and L2PH EARLYCF DEF(H) represent respectively early (at vessel failure) containment leak and rupture due to hydrogen deflagration in high pressure sequences. These events can increase the fire LRF by factors of 10.9 and 9.4 respectively if set equal to 1.

6. L2PH ERLYCF DCH(HP)L and L2PH ERLYCF DCH(HP) represent respectively early (at vessel failure) containment leak and rupture due to direct containment heating in high pressure sequences. These events can increase the fire LRF by factors of 10.5 and 9.1 respectively if set equal to 1.

7. L2PH VECF-H2DEF(H)L represents very early containment leak (before vessel rupture) following vessel rocketing due to a complete circumferential rupture of the vessel leads to a fire LRF increase factor of 9 if set to 1.

8. L2PH VECF-H2DEF(HL)L and L2PH VECF-H2DEF(HL) represent respectively very early (before vessel failure) containment leak and rupture due to hydrogen deflagration in high pressure sequences with hot leg rupture. These events can increase the fire LRF by factors of 8.8 and 3.5 respectively if set equal to 1.

The observations made for internal events regarding hydrogen deflagration causing containment failure are also relevant in the case of fires. The U.S. EPR Level 2 analysis assessed in-vessel steam explosion causing containment failure as a very low probability event, but not of sufficiently low probability for it to be removed from the model. Sensitivity to in-vessel steam explosions arises because, if not excluded from the model, these events are applicable to a large proportion of core damage sequences.

In addition to the above, sensitivity studies were performed to investigate the induced SGTR contribution and the key factors that reduce its importance to the LRF results. The two factors identified were FW availability to any SG and operator depressurization; success of either of these functions, included in the CET, avoids the possibility of induced SGTR. The sensitivity studies were performed with a new quantification of sequence 8 of CET1 HI PRESSURE, as described in the internal events section.

The results obtained show that for fire events the availability of depressurization has a similar impact to that of feedwater to any SG. Note that for fire events, all contributions to RC702 come from Level 2 induced SGTR as no SGTR initiator is modeled. However, compared to internal events the changes seen in this sensitivity study causes a factor of 2 increase in the fire LRF from a base case of 7.3E-9/yr to 1.4E-8/yr.

Although RC702 has a higher contribution to LRF in the internal events case, the impact of the sensitivity on the internal LRF was smaller compared to the impact on the fire LRF. This is because the increase factor from the sensitivity study was only applied to a fraction of RC702 frequency (to sequences other than from SGTR initiators). In the case of the fire sensitivity, the increase factor was applied to the total frequency of RC702 (as there is no contribution from SGTR initiators).

#### 19.1.5.3.3.6 Fire Events Level 2 Uncertainty Analysis

The results of the uncertainty evaluation for the Level 2 Fire Events LRF will be presented in Figure 19.1-19—U.S. EPR Level 2 Fire Events Uncertainty Analysis Results - Cumulative Distribution Function for Fire Events LRF.

The basis for the input uncertainty distributions for systems related basic events and operator actions is discussed in the sub-sections related to the Level 1 PRA. As discussed in Section 19.1.4.2.2.7, for quantitative evaluation of the overall uncertainty on the LRF, uncertainty distributions are added for the Level 2 phenomenological basic events. These events are identified in the PRA database by use of the prefix "L2PH." The distribution form chosen for these basic events will be discussed in Section 19.1.4.2.2.7.

#### 19.1.5.3.3.7 Fire Events Level 2 PRA Insights

In the absence of the specific challenges and bypasses of containment seen in the internal events analysis, the results for LRF for fire events are dominated by creep induced SGTR containment isolation failure and phenomenological challenges. Induced SGTR and containment isolation failure are due to a loss of electrical Division 4 from fire initiators and a concurrent loss of electrical Division 1. The loss of these two divisions disables the depressurization function (that prevents creep induced SGTR) and fails containment isolation. The specific issue for fires is the possibility of containment failure due to loads at the time of vessel failure (higher contribution than for internal events due to lower contributions from other sequences).

The phenomena of thermally-induced steam generator tube rupture, which was assessed as having a large probability for high pressure sequences (transient or small and seal LOCAs) in conjunction with a depressurized secondary side and an absence of feedwater to the steam generators also features in the results (49 percent contribution to LRF). This high contribution to LRF is principally due to the high probabilities of

induced SG tube ruptures. Sensitivity on the unavailability of depressurization and feed water to at least one SG showed an increase factor of 2.9 in the Fire LRF.

Despite the dominance of a single phenomenological issue for LRF, it is noted that LRF is about 4 percent of CDF for fire events close to the contribution from internal events. Other phenomenological challenges such as hydrogen combustions were not identified as leading to significant probabilities of large release.

The most important systems for the fire events LRF belong to the cooling chain (ESWS) followed by the electrical system and SIS overall similar to the internal events LRF results.

Operator actions are dominated by Level 1 actions with no Level 2 action contributing more than 1 percent.

In terms of non-LRF containment failure release categories RC206 (small containment isolation failure) and RC504 (long term containment failure without MCCI and with failed SAHRS) are important contributors.

#### 19.1.5.4 Other Externals Risk Evaluation

The design certification scope of external event screening includes an assessment of high winds, hurricanes, and tornadoes and external flooding as described below.

A COL applicant that references the U.S. EPR design certification will perform the site-specific screening analysis and the site-specific risk analysis for external events applicable to their site.

##### 19.1.5.4.1 High Winds, Hurricane, and Tornado Risk Evaluation

All U.S. EPR Seismic Category I structures are designed to meet the following standards for high winds, hurricanes, and tornadoes.

**High Winds**

The U.S. EPR Seismic Category I structures are designed to withstand high wind load characteristics as specified in NUREG-0800, Section 3.1.1. The EPR Seismic Category I structures are specifically designed for a basic wind speed of 230 mph.

**Tornado and Hurricane Wind Loads**

The U.S. EPR Seismic Category I structures are designed to meet the design-basis tornado wind characteristics of Tornado Intensity Region 1 and the hurricane wind characteristics as specified in NUREG-0800, Section 3.3.2. Tornado Intensity Region 1 is characterized by a maximum tornado wind speed of 230 mph (184 mph maximum

rotational speed, 46 mph maximum translational speed). Hurricane is characterized by a selected maximum hurricane wind speed of 230 mph.

#### Tornado and Hurricane Missiles

The U.S. EPR Seismic Category I structures are designed to the design-basis tornado missile characteristics of Region 1 (most limiting U.S. region) and design-basis hurricane missile characteristics as specified in NUREG-0800, Section 3.5.1.4. The design basis tornado and hurricane missiles include (1) a massive high-kinetic-energy missile that deforms on impact, (2) a rigid missile that tests penetration, and (3) a small rigid missile of a size sufficient to pass through any opening in protective barriers.

U.S. EPR Seismic Category I structures include:

- Reactor Building (RB) and Reactor Building annulus.
- Safeguard Buildings (SBs).
- Emergency Power Generation Buildings.
- Essential service water Pump Structures.
- ESW Cooling Water Structures.
- Fuel Building (FB).
- Vent Stack.

Based on the U.S. EPR design, a tornado, hurricane, or high wind event will not have a significant impact on safety-related equipment. The most limiting impact from a tornado, hurricane, or high wind would likely be a LOOP.

The U.S. EPR has a robust design to cope with a LOOP event. Four independent EDGs (protected within the EPGB) are available to provide power to the safety buses. Although not specifically protected from high winds and tornado, two SBO diesels, which are located separately from the EPGB, are likely to be available to backup the EDGs.

#### High Winds, Hurricane, and Tornado Evaluation Conclusion

The preceding high winds, hurricane, and tornado structural design features, in combination with the U.S. EPR onsite divisional and backup power supplies, provide a robust design against potential high wind, hurricane, and tornado hazards.

### 19.1.5.4.2 External Flooding Evaluation

Safety-related systems and components housed in the Seismic Category 1 buildings are protected from external floods and groundwater by the flood protection measures

summarized below. Refer to Section 2.4 and Section 3.4 for further information on external flood design protection features.

- Structures, including penetrations (e.g., piping and cable penetrations), are designed for the buoyancy loads and hydrostatic pressure loads resulting from groundwater pressure and external flooding.

- Portions of the buildings located below grade elevation are protected from external flooding by water stops and water proofing. All exterior wall or floor penetrations located below grade are provided with watertight seals. No access openings or tunnels penetrate the exterior walls of the Nuclear Island below grade.

- The roofs of the buildings are designed to prevent the undesirable buildup of standing water in conformance with RG 1.102. The roofs of the structures do not have parapets that could collect water. The maximum rainfall rate for roof design is 19.4 inches per hour. The design static roof load for rain, snow and ice is 100 pounds per square foot, which includes the weight of the 100-year return period snow pack and the weight of the 48-hour probable maximum winter precipitation.

- The structures hardened against airplane crash have exterior doors resistant to intrusion by aircraft fuel, and therefore these exterior doors would also provide additional protection against potential flood water.

#### External Flooding Evaluation Conclusion

The preceding external flooding design features, in combination with the U.S. EPR requirements for building location relative to the probable maximum flood (PMF) and maximum groundwater elevation, provide a robust design against potential external floods.

### 19.1.5.4.3 External Fire Evaluation

For the U.S. EPR, the structural design of safety-related structures, the physical arrangement of these structures and the cleared zones surrounding plant structures provide significant protection from external hazards including external fire.

The impact of external smoke on the habitability of the main control room is considered in the design of the control room envelope (CRE) and the control room air conditioning system (CRACS) (refer to Section 6.4 and Section 9.4). The CRE has isolation capability in the event of external fire/smoke and the CRACS is operated in full recirculation mode. The CRACS maintains the control room envelop at a positive pressure to prevent uncontrolled, unfiltered in-leakage during normal and accident conditions. The CRACS can support occupancy for eight people in the MCR and associated rooms for 70 hours without outside makeup air. Portable self-contained breathing apparatus (SCBA) are also available for use by the control room operators.

#### External Fire Evaluation Conclusion

The preceding external fire design features, in combination with the U.S. EPR requirements for structural design, structure location and design considerations of the CRE, provide a robust design against potential external fire and smoke events.

## 19.1.6 Safety Insights from the PRA for Other Modes of Operation

### 19.1.6.1 Description of the Low-Power and Shutdown Operations PRA

#### 19.1.6.1.1 Methodology

The LPSD analysis is an extension of the at-power PRA to include the plant operating states (POS) associated with taking the reactor from hot standby to cold shutdown, mid-loop operation, refueling, and startup. Although the overall LPSD PRA methodology is the same as the at-power PRA, unique initiating events, success criteria, and accident response are developed for each POS. An overview of the methodology focusing on the differences to the at-power methods is provided below.

#### POS

The POS analysis is specific for shutdown operation. The LPSD PRA includes several POS to represent plant and system configurations during shutdown evolutions. In the U.S. EPR analysis, two POS states are analyzed as power states: POS A (full power to hot standby) and POS B (hot standby to hot shutdown). The process of identifying a reasonable set of POS includes consideration of changes in the RCS conditions, impacts on initiating events, safety functions, unavailability of safety trains, success criteria, and evaluation of transition states versus steady-states. The POS selection is based on the following key characteristics:

- RCS level (pressurizer, mid-loop, cavity pool flooded).
- RPV integrity (head on, head off).
- Number of RHR trains operating/available (including their support systems).

Other characteristics (e.g., temperature, pressure, the number of available SGs, and the number of RCPs running) are evaluated and accounted for in the PRA modeling of each POS.

#### Initiating Events

Although the methodology is essentially the same as that described for the at-power PRA, a unique set of initiating events are identified for LPSD. The main initiating event of interest during shutdown is a loss of decay heat removal. The decay heat removal function is provided by the operating RHR system, except during fuel off load when spent fuel pool cooling (SFPC) provides this function. The identification of

unique causes for an RHR system failure (e.g., RHR components, support systems, human interface and LOCA) is included in the fault tree modeling of this initiator.

Special evaluations of potential level drop events during mid-loop, flow diversions in the RHR system (LOCA inside containment) and LOCA outside containment events are also included in the initiating event analysis.

#### Success Criteria

Many of the success criteria developed for the at-power model are applicable to shutdown operation. For example, one of four MHSI pumps is a success during at-power for SLOCA makeup, as it would be during shutdown. In some cases the success criteria requirement is relaxed. For example, the number of PSVs required for the primary feed-and-bleed function is reduced from three of three to two of three or one of three.

The evaluation of time available to prevent the RCS from boiling and subsequent core uncovery for different times after shutdown is important during LPSD. As decay heat declines with time after shutdown, the time available for operator actions increases, and the demand for inventory makeup decreases. For example, one day after shutdown, a single CVCS pump could provide adequate RCS makeup. The thermal-hydraulic calculations performed for shutdown states are straightforward, based on standard liquid heat-up and bulk boiling equations.

#### Accident Sequence Model, Operator Actions and Systems Analysis

Again, although the methodology is the same as for at-power, unique event tree models are required for unique POS, initiating events, and success criteria. There are a number of new specific operator actions evaluated in the LPSD PRA. However, the same methodology used for the at-power PRA model is used for LPSD. The system fault trees developed for the at-power PRA are modified to account for different configurations, success criteria, and maintenance alignments in shutdown. For example, several LHSI trains are operating in an "RHR mode" versus "SIS automatic standby" mode during at power. Also, standby RHR trains require manual actuation.

### 19.1.6.1.2 POS Definition

There are a number of changing conditions that can occur during LPSD evolutions (e.g., decay heat level, RCS physical status, availability of equipment). Thus, the objective is to define a representative set of initial conditions or plant operating states (POS) that reasonably capture the LPSD evolutions. The POS selection is based on the following key characteristics: RCS level (e.g., pressurizer, mid-loop, cavity pool flooded), RPV integrity (head on, head off), number of RHR trains operating/available (including their support systems).

A summary of the POS developed for the U.S. EPR can be seen in Table 19.1-87—Plant Operating States (POS). The following summarizes the selected POS:

- POS A and B include power operation Mode 1, startup Mode 2, and hot standby Mode 3. These POS are characterized by SG heat removal (T > 248°F).
- POS CA includes hot shutdown Mode 4 and a part of cold shutdown Mode 5, characterized by RHR heat removal with level in the pressurizer (T ≈248°F to 131°F).
- POS CB applies to the part of cold shutdown Mode 5, characterized by RHR heat removal with level at mid-loop with RPV head on (T ≈131°F).
- POS D applies to refueling Mode 6, characterized by RHR heat removal at mid-loop with RPV head off (T ≈131°F).
- POS E applies to refueling Mode 6, with reactor cavity flooded (T ≈131°F).
- POS F applies to the case where the core is off loaded to the spent fuel pool.

POS A and B are analyzed in the at-power PRA model because of their similar configurations; decay heat is being removed with SGs. Power operation is the most conservative mode of those included in POS A and B. The remaining POS are analyzed in the LPSD PRA model. POS and related parameters are defined in Table 19.1-87.

#### 19.1.6.1.3 Initiating Events

Table 19.1-88—LPSD Initiating Event List provides the list of initiating events specific for the LPSD PRA. The following summarizes:

- Loss of RHR – Loss of decay heat removal during various LPSD states occurs because of a loss of RHR/LHSI trains or their supporting systems (e.g., loss of offsite power or loss of CCW/ESW cooling). Multiple RHR trains have to fail to cause this initiating event. The RHR system and its support systems, including offsite power, are included in the analysis.
- Diversions and leaks in operating RHR – Flow diversions and leaks (SLOCA and LLOCA) to the IRWST (LOCA inside containment) could result in loss of RHR suction to all operating RHR pumps and, therefore, present potentially important initiating events.
- Loss of inventory due to RHR ISLOCA – This event is a postulated leak/break in the operating RHR system outside containment and subsequent failure to isolate the break. Reliable detection features included in the U.S. EPR design improve mitigation of this event.
- Loss of inventory due to Level Drop – Draining the RCS too low and causing cavitation of the RHR pumps is considered an important event during mid-loop

operation and is included as an initiating event. Automatic isolation features reduce the likelihood and improve mitigation of this event.

Human errors that contribute to each of the above initiators (e.g., failures to isolate flow diversions or to stop drain down in mid-loop) are explicitly modeled in the initiating event fault trees.

Human-induced initiators during shutdown maintenance activities will be evaluated when the plant-specific shutdown procedures are available.

Overfill events in the pressurizer solid state that could lead to a low temperature overpressure event have not been considered likely and have not been identified as initiating events that could significantly contribute to risk. Inadvertent start of a reactor coolant pump, or a MHSI pump, could cause an overpressure event when the pressurizer is solid. However, the PSVs and RHR relief valves would protect the system from overpressure and the exposure time is considered to be very small.

As stated in Section 19.1.2.2, the COL applicant will review plant-specific shutdown procedures and strategies to confirm that the assumptions used in the LPSD PRA remain valid.

#### 19.1.6.1.4 Success Criteria

Decay heat levels are very important inputs in the analysis of timing and success criteria during LPSD. Since decay heat is a function of the time after a trip, success criteria are different for each POS and they are a function of the POS durations. POS duration is conservatively estimated based on the European experience with the same type of reactor. It is based on a basic shutdown duration (i.e., no extra work performed) of 21 days. Thirteen of these days are assumed to be spent in refueling (POS E and F), and the other eight days are distributed between shutting down and starting up after the refueling.

In specifying system and function success criteria, core damage in shutdown is defined as uncovering of the core: the coolant level reaching the top of active fuel (TAF). Like at-power operation, to constitute a success end state for the LPSD PRA model, each accident sequence is expected to result in a safe, stable state for 24 hours - mission time.

Figure 19.1-20—Time to TAF - Level 1 Shutdown plots the approximate amount of time, given the loss of heat-removal capability and subsequent loss-of-coolant inventory, until the coolant level reaches TAF. Standard liquid heat-up and bulk boiling equations are used. Parameters used in these equations such as coolant temperature and volume, and heat load from decay heat and RCP pumps vary over time and various POSs.

The following summarizes differences in success criteria versus at-power modeling:

- RCP Trip – During POS CA, it is assumed that two pumps are running. Thus, only two pumps have to trip on loss of pump cooling (seal cooling is not required during shutdown, as pressure and temperatures are lower).

- Partial cool down (PCD) – PCD is not required for LOCAs since RCS pressure is already low and secondary cooling MSRV setpoints are low enough to ensure that RCS pressure does not exceed MHSI shutoff head.

- Primary Bleed – One or two PSV may be required for primary bleed versus three of three PSVs in the at-power model (conservatively, three of three are still required in the model).

- IRWST cooling – Not required when the RPV head is off.

#### 19.1.6.1.5 Accident Sequences

The following event tree models were developed to model accident response to the LPSD initiating events (event tree top events are summarized in Appendix 19B):

Event Tree "SD RHR C" models plant responses to loss of RHR while in POS CA or CB. The loss of RHR initiating event model includes operator actions to recover RHR (e.g., start a standby pump train). Event tree top event "TR LOCASD" models the probability of a transient-induced LOCA. LOCA response requires feed-and-bleed cooling success because it is conservatively assumed that the LOCA may not be large enough to provide sufficient bleed. Three ways to fail the TR LOCASD top event have been considered:

- PSV fails to reclose after RCS heats up.

- RCP seal LOCA.

- RPV or PZR vent fails to close. This condition was considered and screened because the time to uncover the core is more than a day, allowing significant time for operators to isolate the path.

Event Tree "SD RHR D" models plant responses to loss of RHR while in POS D. Since the RPV head is off, the model is much simpler than for State C. The initiating event model includes recovery of RHR standby trains.

Event Tree "SD ULD CB" models plant response to an uncontrolled level drop in POS CB. Since RCS inventory is assumed to be diverted via CVCS storage outside containment, the long-term failure to isolate is assumed to result in a loss of the IRWST outside containment and containment bypass.

Event Tree "SD ULD D" models plant response to an uncontrolled level drop in POS D. Since the RPV head is off, the model is much simpler than for State C. The RCS

inventory is assumed to be diverted via CVCS storage outside containment, and the long-term failure to isolate is assumed to result in a loss of the IRWST outside containment and containment bypass.

Event Tree "SD LOCA C S" models plant response to a small LOCA inside containment while in POS CA or CB. The LOCA S initiating event model includes pipe break, as well as small RHR flow diversions.

Event Tree "SD LOCA C L" models plant response to a large LOCA inside containment while in POS CA or CB. The LOCA L initiating event model includes large RHR flow diversions. Since the LOCA is large, no credit is taken for RHR or secondary heat removal.

Event Trees "SD LOCA D S" and "SD LOCA E S" model plant response to a small LOCA inside containment while in POS D or E. The LOCA initiating event model includes pipe break, as well as small flow diversions from the RHR system.

Event Trees "SD LOCA D L" and "SD LOCA E L" model plant response to a large LOCA inside containment while in POS D or E. The LOCA L initiating event model includes large flow diversions from the RHR system.

There are several Event Trees "SD RHR ISLOCA" that model RHR pipe break LOCA events outside containment. The probability of failure to isolate this type of event is already included in the initiating event frequency. Thus, these initiating events result in a loss of the IRWST outside containment, core damage, and containment bypass. The shutdown event trees are shown in Appendix 19B.

#### 19.1.6.1.6 Operator Actions in Shutdown

The corresponding human error probabilities were estimated by using the same method as at-power operation - SPAR-H. The use of SPAR-H is appropriate for the current stage of the U.S. EPR design when operating guidelines and procedures are not available. As discussed in Section 19.1.4.1.1.5, the SPAR-H method bases its probability estimates primarily on time available for the diagnosis and action, coupled with high-level PSFs.

The timing of operator actions in shutdown depends on the initiating event and the specific POS. Timings are based on the time to TAF, calculated for the specific initiators. In this phase, all PSFs are assumed to be optimal (equal to one).

Operator actions in shutdown are summarized below in the following three groups:

1. Operator actions included in the initiating events.

2. Operator actions in response to loss of RHR.

3. Operator actions in response to loss of inventory.

Alarms and indications available for diagnosis are also summarized below.

The action connected with support system operation (electrical and HVAC) are considered to be the same as in the at-power PRA model.

### Operator Actions Included in the Initiating Events

Operator actions are included in the initiating event analysis as summarized below:

- Recover loss of operating RHR trains by starting a standby RHR train.
- Isolate RHR flow diversions before level drops to the RHR protective trip on low loop level.
- Stop uncontrolled level drop (ULD) when going to mid-loop (human error is also analyzed as a contributor to the initiating event).

### Operator Actions in Response to Loss of RHR

The following key operator actions are identified in the accident sequence analysis:

- Start the standby RHR train or LHSI train.
- Establish primary feed and bleed cooling (applies when RPV head on).
- Establish reactor coolant makeup (applies when RPV head off).
- Establish IRWST cooling.

Alarms and indications available for diagnosis for operator actions, may differ from action to action, but generally include the following:

- Initiating event specific cues (e.g., system trouble, no flow).
- RCS/RHR temperature and pressure.
- RPV level.
- IRWST temperature.
- Containment pressure and temperature.

### Operator Actions in Response to Loss of Inventory

The following key operator actions are identified in the accident sequence analysis.

- Establish reactor coolant makeup.

- Start the standby RHR train.
- Establish primary bleed (given a loss of secondary cooling).
- Isolate flow diversion or letdown.
- Establish IRWST cooling.

Alarms and indications available for diagnosis for operator actions, may differ from action to action, but generally include the following:

- RHR failure cues (e.g., system trouble, no flow).
- RCS/RHR temperature and pressure.
- VCT level and coolant storage level.
- IRWST level and temperature.
- Containment pressure and temperature.

#### 19.1.6.1.7 System Analysis

The following summarizes differences in system models versus at-power modeling:

- RHR – The system is modeled as normally operating with suction from hot legs rather than in standby with suction from IRWST. SIAS actuation is removed from the model, since this is disabled by the P14 permissive during shutdown. Therefore, a start of RHR standby pump requires operator action.
- SIAS – The safety injection signal is changed in the MHSI model to low delta $P_{sat}$ in POS CA and to low loop level in POS CB, POS D, and POS E.
- CVCS – Charging system is not credited in shutdown.
- EFW – Auto reset of the P13 permissive is required for automatic EFW operation during POS C. Also, only the normal pressure control mode of MSRTs is required (MSSVs are not credited). A PCD function is disabled by P14 permissive, the MSRT pressure is set to 145 psia and is not automatically reset.
- RCP – Only two pumps are running during POS CAD and would be required to trip upon loss of motor cooling. Seal cooling is not required during shutdown.

The following summarizes LPSD systems with auto actuation signals modeled:

- RHR protective trip – Low loop level will trip the operating RHR pumps to protect the pumps and allow them to be restarted post trip either in RHR or the LHSI mode of operation. Failure of this trip function is included as a failure mode of the RHR pumps. Success allows the pump to be manually recovered later.

- RHR isolation – High sump level in the SB automatically isolates the respective RHR train and trips the pump. This is modeled in the RHR ISLOCA initiating event fault tree.

- Low pressure reducing station isolation – During an uncontrolled drain down event (ULD), low loop level automatic isolation of the low pressure reducing station is modeled. Failure is assumed to result in diversion of IRWST water outside containment requiring operator response.

The probability of plugging the IRWST suction strainers is modeled the same as at-power operation (i.e., CCF). Maintenance work during shutdown could result in a higher probability of plugging. However, the IRWST design is somewhat unique in comparison to the PWR plants operating in the USA. The structure is very large with separation between suction lines to the four SB; three levels of filters are also provided: trash racks, retaining baskets, and six strainers with a back flush capability. This probability of plugging is also dependent on maintenance procedures that will be in place to control foreign material, but are not available in this phase. As a result, the present modeling of the IRWST suction strainers was not changed.

Preventive maintenance modeling was revised for LPSD because of obvious differences in risk management strategies from power operation. Assumptions on maintenance strategies are as follows:

- Maintenance on the SG systems is assumed to be performed on two SGs that are not available in states CA and CB.

- Maintenance on the other trains is assumed to occur in state E. One division is assumed to be out for maintenance during that state.

Available mitigating systems in different POSs are defined in Table 19.1-89—System Availability During Shutdown.

### 19.1.6.1.8 Fire & Flooding Events in Shutdown

Limited evaluation of fire and flooding initiators is performed in the LPSD PRA. Fire and flooding events are evaluated with bounding analyses similar to the analysis performed at-power. Since there is physical separation between RHR trains, and at least two are operating during shutdown, fires and floods can only impact one operating train. Because of the physical separation between operating and standby trains, the impact of the possible degradation in the fire and flood barriers during shutdown is assumed to be not significant. Transient combustibles and maintenance activities may result in a higher fire/flood frequency during shutdown in certain parts of the plant, but are judged to be not significant for the protected RHR trains providing decay heat removal. The risk from a fire in the main control room at-power also envelops the risk in shutdown. The assumption made at-power of core damage if the

operators fail to evacuate is conservative for shutdown, where loss of the MCR would not directly result in an initiating event.

Additionally, the following fire and flooding events that could cause scenarios specific to shutdown are identified:

- Flooding in the annulus that propagates to two Safeguard Buildings (SB), disabling both running residual heat removal (RHR) trains.
- Fire-induced hot short that causes an uncontrolled level drop.
- Fire-induced hot short that causes a flow diversion due to spurious operation of a motor-operated valve.

The frequency of each of these three scenarios is evaluated. In each case, it is found to be at least two orders of magnitude less than the frequency of the equivalent initiating event in the internal event LPSD PRA (i.e., loss of RHR, uncontrolled level drop and flow diversion LOCA).

The effect of each of these three scenarios on mitigating systems is also evaluated, and sensitivity studies are performed to evaluate the increase in shutdown risk posed by these initiators. The relative change in CDF is found to be negligible for loss of RHR and uncontrolled level drop, and very small for the RHR flow diversion. This is due to the low frequency of these events and their limited impact on mitigating systems.

Based on the bounding nature of the at-power fire and flood evaluations and on the low risk impact of shutdown-specific internal hazards, the risk from fire and flood events during at-power operation is assumed to envelop the risk during shutdown.

### 19.1.6.2 Results from the Low-Power and Shutdown Operations PRA.

#### 19.1.6.2.1 Risk Metrics

The total CDF from shutdown events is 6.0E-08/yr, well below the NRC safety goal of 1E-04/yr (SECY-90-016) and the U.S. EPR probabilistic design goal of 1E-05/yr. Mean value and associated uncertainty distribution can be found in Section 19.1.6.2.7.

#### 19.1.6.2.2 Significant Initiating Events

The significant shutdown initiating events and their contribution to shutdown core damage frequency are given in Table 19.1-90—U.S. EPR Significant Initiating Events Contributions - Level 1 Shutdown (Contributing more than 1% to SD CDF). Only those initiating events that contribute more than one percent to the total internal events CDF are listed in the table. All initiating events and their contributions are illustrated in Figure 19.1-21—U.S. EPR Initiating Event Contributions - Level 1 Shutdown. As can be seen from Table 19.1-90 and Figure 19.1-21, nine shutdown

initiating events dominate shutdown core damage frequency, loss of RHR in state CB, CA and DU, Small LOCA events in states CAD and CBD, and uncontrolled level drop in states CBD and DU. Note that the LOOP event is included in the loss of RHR initiating event. Based on the FV importance measures from the shutdown model, the LOOP events during shutdown contribute approximately 44 percent of the total risk.

The total contribution of each POS is illustrated in Table 19.1-91—U.S. EPR Shutdown State (POS) Contributions - Level 1 Shutdown. This table shows the estimated POS duration, the CDF and CDF/day for each POS. The highest contribution is from POS CBD, CAD, and DU which is to be expected because these are states where RCS is being drained to mid-loop and an uncontrolled level drop could occur (CBD and DU) or the state with the highest decay heat (CAD). The POS contribution is also illustrated in Figure 19.1-22—U.S. EPR Shutdown State Contribution - Level 1 Shutdown.

#### 19.1.6.2.3 Significant Cutsets and Sequences

The cutset contribution to the shutdown event CDF is equally distributed. Only 20 of the top cutsets contribute more than one percent to the total CDF. The number of cutsets that contribute to 95 percent of the CDF is above 11,000. This shows that there are no outliers in the U.S. EPR shutdown event CDF.

The significant cutsets for the shutdown events are illustrated in Table 19.1-92—U.S. EPR Important Cutset Groups - Level 1 Shutdown (Top 100 Events). In this table, cutsets are grouped based on their similar/symmetric impact on mitigating systems. Such groups of the cutsets usually correspond to specific sequences in event trees. These sequences are also identified in the table. Columns in the table show: group number, numbers of cutsets included in the group, frequency range of the cutsets included in the group, group percentage contributions to total CDF, cumulative percentage contributions to total CDF, a selected representative cutset with corresponding basic events and their descriptions, and the sequence description.

As shown in Table 19.1-92, the top 100 cutsets are grouped into 20 groups, representing over 60 percent of the CDF. Seven of these groups are LOOP related (i.e., started with a LOOP/Loss of RHR initiating event). Five of these groups are related to an SLOCA initiating event, and six are related to uncontrolled level drop events in POS DU and CBD. Only one group represents a RHR ISLOCA cutset.

In Table 19.1-92, Groups 1, 2, 3, and 5 represent a small LOCA in POS CA, CB, D and E due to an inadvertent opening of LHSI overpressure protection safety valve and an operator failure to isolate. Core damage occurred because of a CCF of the IRWST sump strainers or cold leg injection check valves, common to all injection systems.

Group 4 represents a Large LOCA due to an inadvertent opening of an IRWST suction valve and an operator failure to isolate, followed by a CCF of the IRWST sump strainers, leading to core damage.

Groups 6, 8, 9, and 13 all represent a loss of RHR cooling due to a LOOP event during POS CA, CB and D, followed by a CCF of all EDGs including signal related failures. Since CCW trains are not supplied from SBO DGs, the only way to cool the plant is by the EFW pump in Division 1 (in POS CA and CB only SGs 1 and 2 are assumed to be available, in POS D no SGs are available) or the SAHR dedicated ESW/CCW. In the summarized cutsets, various combinations disable these two systems, for example a loss of SBO DG in Division 1 would disable both of these systems. Groups 7 and 12 similarly represent a loss of RHR cooling due to a LOOP event during POS D, followed by a failure of feed and bleed due to a loss of injection.

Group10 represents a loss of RHR cooling due to a LOOP event during POS CAD, CBD, CBU, and DU, followed by a CCF of all safety-related batteries on demand. This results in a total loss of instrumentation, and, because no instrumentation is available to operators, these sequences are conservatively assumed to lead to core damage, without crediting a LOOP recovery or non safety batteries.

Group 11 represents a loss of RHR system in POS CBD, due to a total loss of the HVAC system which occurred after the SAC air supply fans failed to run and no compensatory operator action was implemented. The result is a loss of all safety divisions.

Groups 14, 15, and 17 represent uncontrolled level drop events in POS DU and CBD, which started with failures of CVCS low pressure reducing station MOVs to close on demand (combinations of hardware, signal and operator action), followed by a long term operator failure to isolate leak and prevent a slow RCS drain outside containment. Similarly, Groups 16 and 18 also represent uncontrolled level drop events in POS DU and CBD, which started with failures of CVCS low pressure reducing station MOVs to close on demand, in this case followed by a CCF of the IRWST sump strainers failing all injection trains.

Similarly to Group 11, Group 19 represents uncontrolled level drop events in POS DU and CBD, due to a total loss of the HVAC system which occurred after the SAC air supply fans failed to run and no compensatory operator action was implemented. The result is a loss of all safety divisions.

Group 20 represents a LOCA outside containment in POS E, caused by a pipe break in an operating RHR train, followed by a failure of both manual and auto isolation.

”Important” CDF sequences, with a sequence frequency greater than one percent of total core damage frequency (as presented in Section 19.1.8.1), are shown in

Table 19.1-130—U.S. EPR Important Sequence(s) – Level 1 Shutdown (Contributing more than 1% to the Total CDF). Only one sequence has a frequency greater than one percent of the total core damage frequency. For that sequence, Table 19.1-130 gives event tree, sequence number, corresponding initiating event, event tree sequence identifier, the sequence frequency, and a brief description. It also connects the sequence to the corresponding cutset group in Table 19.1-92, which gives a more detailed description of the sequence.

#### 19.1.6.2.4 Significant SSC, Operator Actions, and Common Cause Events

Table 19.1-93 through Table 19.1-99 show the important contributors to shutdown CDF. Importance is based on FV importance measure (FV ≥0.005), or RAW importance measure (RAW ≥2). Note that the SSC and CCFs that could directly cause an IE were not ranked based on RAW importance measure.

Table 19.1-93—U.S. EPR Risk-Significant Components based on FV Importance - Level 1 Shutdown shows the top risk-significant SSC based on FV importance. The components with the highest FV are the EDG and SBODG trains, the first SIS isolation check valves, and IRWST sump strainers. The importance of these SSC can be explained by a high LOOP and LOCA contribution to the LPSD CDF.

Table 19.1-94—U.S. EPR Risk-Significant Equipment based on RAW Importance - Level 1 Shutdown shows the top risk-significant SSC based on RAW importance. Most of the top SSC are from the HVAC and electrical system, including chillers crosstie MOVs, load centers, switchgears, MCCs, DC buses and safety batteries.

Table 19.1-95—U.S. EPR Risk-Significant Human Actions at Shutdown based on FV Importance - Level 1 Shutdown shows the top risk-significant human actions based on FV importance. The most important operator actions based on the FV are operator failure to isolate RHR flow diversion in states CA and CB, operator failure to isolate the CVCS low pressure reducing station, and operator failure to stop draindown at mid-loop. These actions are important because they are needed to prevent the occurrence of the important LPSD initiators.

Table 19.1-96—U.S. EPR Risk-Significant Human Actions based on RAW Importance - Level 1 Shutdown shows the risk-significant human actions based on RAW importance. The most important operator action based on RAW is the operator failure to isolate CVCS low pressure reducing station. This action is important because it is needed to prevent the occurrence of the important LPSD initiators: uncontrolled level drops.

Table 19.1-97—U.S. EPR Risk-Significant Common Cause Events based on RAW Importance - Level 1 Shutdown shows the risk-significant common-cause events based on RAW importance. The most important CCFs based on RAW importance are CCFs to open LHSI/MHSI common injection valves and CCF plugging of IRWST sump

strainers. These events are important because both of these CCFs would disable all safety injection.

Table 19.1-98—U.S. EPR Risk-Significant Common Cause I&C Events based on RAW Importance - Level 1 Shutdown shows the significant common-cause I&C events based on RAW importance. As illustrated in this table, I&C common-cause events (e.g., I/O modules, software, sensors, or computer processors or SAS) have a high RAW. This is because a CCF of the signals could lead to an actuation failure of MHSI or EDGs (Protection system) or failure of CVCS isolation on ULD (SAS).

Table 19.1-99—U.S. EPR Risk-Significant PRA Parameters - Level 1 Shutdown shows the significant modeling parameters used in the analysis and the significant LOOP related basic events. The significance is determined based on either the FV or RAW importance measure, as defined above. This table illustrates the high significance (a high FV) of the parameters used to support cooling in the SBO conditions and in the modeling of shutdown initiating events (e.g., LOOP, induced LOCAs or ISLOCAs).

#### 19.1.6.2.5 Key Assumptions

General modeling assumptions are similar to the assumptions used in the at-power PRA. Additional shutdown assumptions are listed below.

- Shutdown states CAD1, CAD2, and CAD3, as defined in Table 19.1-87 are analyzed as one state, CAD.
- The heat load impacting the coolant at any single point on the curve is considered constant for the duration of the TAF calculation. The decrease in decay heat over time is conservatively not incorporated. Thus the plotted time to boil off coolant until TAF is lower than actual.
- One train of RHR and cooling to its heat exchanger adequately removes decay heat in all cases, except when both:

  1. The plant is in POS Dd, and
  2. The CCW train cooling the RHR heat exchanger is also cooling the CCW common header.

  For this exception, one train of RHR is sufficient if QNA loads are removed from the CCW common header and in any case, two trains of RHR are sufficient.

- Maintenance on the SG systems is assumed to be performed on two SGs, which are assumed not available in states CA and CB. Maintenance on all other trains is assumed to occur in state E. One division is assumed out for maintenance during that state.

- Two EFW trains are assumed to be available during POS CA and POS CB, with the remaining two trains unavailable due to maintenance. Considering the lower decay heat during shutdown, two EFW tanks are assumed to be sufficient during times when two EFW trains are out for maintenance during shutdown. The EFW inventory fault tree is not modified from the at-power model. Therefore, the need for refilling and cross-connecting EFW tanks is modeled for failures of EFW trains that are assumed to be out of service for maintenance. This modeling is conservative and does not have a significant impact on the results.

- Because of maintenance unavailability assumptions, the charging system is not credited, even though it is likely to be available in states CAD and CBD.

- IRWST cooling is not required when the RPV head is off: Makeup to the RPV for boil-off is required when heat removal is lost. It takes more than three days to boil-off the IRWST if it is assumed that the steam is not condensed in the containment and returned to the IRWST. This is conservative and provides the basis for not modeling IRWST cooling when the RPV head is removed.

- Possible transient LOCA events through RPV and PZR vent are not considered. The PRZ vent is normally open during shutdown. The RPV vent is open during mid-loop and during plant startup after refuel. Given RCS temperatures and pressures, a loss of inventory in the form of steam was evaluated after a loss of RHR cooling. The pressurizer vent contains a flow restrictor, which significantly limits the flow well below the makeup capacity of the CVCS system. The RPV vent is a one-inch line, and it would take a large amount of time to uncover the core by venting steam through this line. The risk from this event is not considered significant because the operators have more than enough time to isolate the vent or to provide makeup to the RCS. Based on the above discussion, these events were not identified as transient LOCAs that need to be included in the analysis.

- Three of three PSVs are assumed to be required as in the power operation model for feed-and-bleed, which is conservative for shutdown (two of three is expected to be adequate and one of three is adequate post refueling).

- It is assumed that a transient-induced LOCA response requires feed-and-bleed cooling success, because LOCA size may not be large enough to provide sufficient bleed.

- The probability that the IRWST suction strainers are plugged was not increased relative to the power operation PRA model. The IRWST design (e.g., large, separation between suction lines, debris retaining capability) and plant procedures (e.g., foreign material control) are expected to ensure that this probability is low.

- Risk from the pressurizer solid state was not considered. Inadvertent start of a reactor coolant pump or a MHSI pump could cause an overpressure event when the pressurizer is solid. The PSVs and RHR relief valves would protect the system from overpressure and the exposure time is small. Thus, overfill events that could lead to a low temperature overpressure event have been considered not likely and have not been identified as initiating events that could significantly contribute to risk.

- The EPR PRA does not specifically model nozzle dam installation since it is considered an infrequent evolution. The EPR PRA assumes that the core will be offloaded every fuel cycle. When nozzle dams are used, measures will be taken to reduce the CDF impact. To ensure that the risk of a sudden loss of RCS inventory during nozzle dam installation/removal and cold leg work does not have a large impact on the results of the EPR LPSD PRA, nozzle dams installation should be consistent with GL 88-17 and IN 88-36.

#### 19.1.6.2.6 Sensitivity Analysis

A sensitivity analysis was performed to evaluate the impact of general modeling assumptions, most of them are also analyzed in Level 1 at power.

The sensitivity results are shown in Table 19.1-100—U.S. EPR LEVEL 1 Internal Events Sensitivity Studies - Level 1 Shutdown. Several insights can be drawn from the sensitivity cases analyzed.

The LPSD CDF is found to be more sensitive to assumption on preventive maintenance than the at-power CDF, as it will be discussed below. Diversity of EDGs and SBOs is also found to have a strong impact. The sensitivity on HEPs is also strong. The LPSD CDF is also sensitive to the assumption on the unavailability of the UHS in SBO conditions, which did not have a significant impact on the at-power CDF. These high impacts could be explained by a high LOOP contribution to the LPSD CDF. Also, human actions are essential in shutdown. A sensitivity run was performed to evaluate a benefit from assuming that in the shutdown the UHS fans may not be required. The sensitivity run shows that the UHS fans were not important contributors to the LPSD risk.

A separate sensitivity case was run to check the preventive maintenance assumptions in the LPSD PRA. Preventive maintenance was extended from POS E to POS DU and POS CBU on one train of safety systems, including RHR. This resulted in an increase in the LPSD CDF for a factor larger than 22. Such a large increase can be attributed to the importance of any RHR train and supporting systems in shutdown.

#### 19.1.6.2.7 Uncertainty Analysis

The results of the uncertainty evaluation for the LPSD operation CDF are presented in Figure 19.1-23—U.S. EPR Level 1 Shutdown Events Uncertainty Analysis Results - Cumulative Distribution for Low Power and Shutdown CDF.

The uncertainty results are summarized below:

- CDF LPSD Operation Mean Value: 6.7E-08/yr.
- CDF LPSD Operation 5 percent Value: 3.9E-09/yr.
- CDF LPSD Operation 95 percent Value: 2.0E-07/yr.

This ninety-fifth percentile CDF value is more than two orders of magnitude below the NRC goal of 1E-04/yr.

Uncertainty on the Level 1 Shutdown PRA results is quantified using a process similar to that described for internal events in Section 19.1.4.1.2.7. Parametric uncertainty was represented by selecting an uncertainty distribution for each parameter type, as described in Section 19.1.4.1.2.7. Modeling uncertainty was not included in the shutdown uncertainty model.

#### 19.1.6.2.8 PRA Insights

The LPSD PRA results have shown that events leading to losses of RHR in shutdown are unlikely, but together contribute over 50 percent of the shutdown risk. The dominant contributor to these initiating events is a LOOP during shutdown states. LOCAs in shutdown contribute approximately 30 percent and the uncontrolled level drops in shutdown contribute 15 percent to the LPSD CDF.

If the assumptions on the POS durations are to be neglected, the highest risk states are CAD, CBD and DU. Decay heat is the highest in POS CAD, while CBD and DU are the states where active draining to mid-loop occurs. The possibility to over drain and to have an uncontrolled level drop makes these states relatively important even though overall risk is low.

### 19.1.6.3 Description of Level 2 PRA for Low-Power and Shutdown Operations

#### 19.1.6.3.1 Low Power and Shutdown Operating States Level 2 Methodology

The LPSD Level 2 analysis extends beyond the at-power PRA to include the Plant Operating States (POS) characterized by zero operating power. Over the course of these LPSD POSs, the reactor is taken from hot standby to cold shutdown through mid-loop operation followed by refueling and startup. Although the overall LPSD PRA Level 2 approach is the same as the at-power analysis, the assumptions on initiating events, systems status, and operators actions require a unique treatment for each of the LPSD POSs. A detailed analysis of the shutdown Level 2 PRA is performed when differences in assumptions are significant; otherwise, the at-power results are used when bounding.

##### 19.1.6.3.1.1 POS Definition

The Plant Operating States used in the Level 1 PRA for Low-Power and Shutdown represent the plant and system configurations during all shutdown phases. The similar POSs from Level 1 analysis, representing shutting down and starting up phases are combined to streamline Level 2 analysis. Since the decay heat levels are different in these two phases, the more conservative decay heat from the shutting down phase is used. These POSs are summarized in Table 19.1-110—Level 2 Low Power Shutdown

Plant Operating States Definition along with the key parameters to be considered in each POS. Decay heat levels are defined for both Level 1 POSs.

Additional characteristics (e.g., RCS pressures and temperatures, number of available SGs, number of RCPs running, number of mitigating systems available) are evaluated for the detailed Level 1 PRA modeling of each POS. A summary of the POS developed for the U.S. EPR can be found in Table 19.1-87—Plant Operating States (POS).

#### 19.1.6.3.1.2 CDES Definition

The core damage end states (CDES) developed in the Level 2 PRA for at-power operations and described in Section 19.1.4.2.1.1 are modified to be integrated in the LPSD Level 2 PRA analysis. The major modifications are to apply each CDES for different LPSD POSs. These newly developed CDES, used to support the quantification of the LPSD Level 2 PRA analysis, are summarized in Table 19.1-111—Level 2 Low Power Shutdown Core Damage End States Definition.

The primary system is considered pressurized in states CA and CB and depressurized in POSs D and E. Therefore, for states D and E, all the CDES are directed to low pressure CETs. For states CA and CB, the CDES are at high pressure and are directed to high pressure CET, except if a manual depressurization has occurred

In selection of CDES, a distinction between CA and CB is considered when estimated hatch closure timings are different as in all LOCA sequences.

In state CA, all transient-induced LOCAs are treated as seal LOCAs. This difference of treatment only affects the induced RCS rupture evaluation. It is conservative to assume that all transient-induced LOCAs are seal LOCAs since this is the initiating event that creates the conditions most likely to induce SGTR.

#### 19.1.6.3.1.3 Containment Isolation

All containment isolation valves are considered to have equal or higher probabilities of being open compared to the full power. No containment isolation line is assumed to be closed during the entire shutdown duration period. Assumptions were made on the fraction of time certain containment isolation valves were open, when no precise information was available.

The differences between shutdown and at-power containment isolation models are summarized in Table 19.1-112—Level 2 Low Power Shutdown Containment Isolation.

#### 19.1.6.3.1.4 Equipment Hatch Closure

Per technical specifications, the equipment hatch can be open anytime that the RCS temperature is below 200°F. The equipment hatch is considered open in shutdown POS CA, CB, and E and is considered closed in D. When the hatch is initially open, it

is assumed the hatch must be closed prior to boiling in the core to prevent releases to the environment. Failure to close the hatch is treated in the containment event trees as a large CI failure. The ability to close containment hatches and penetrations during Modes 5 and 6 prior to steaming to containment is important. It is assumed that procedures and training will be developed to achieve containment hatch and penetrations closure.

Except in POS E, where it is assumed outage equipment cannot be moved, the ability to close the hatch is credited. The initial actions are performed inside the containment; therefore, the boiling time is considered to be the most limiting criterion in determining the time available to close the hatch. It is estimated to be 1 hour for LOCA sequences and two hours for transient sequences. The closing action is assumed to take 20 minutes if power is available, or 90 minutes requiring 6 operators if the power is not available.

#### 19.1.6.3.1.5 Assumptions on Systems and Operator Actions in the Shutdown Level 2 PRA

Similarly to the at-power analysis, and in addition to the needed support systems, several frontline systems are credited in the shutdown Level 2 CET that are also credited in the shutdown Level 1 PRA model. These systems are credited as follows:

- SAHRS train is credited in Level 1 for long term heat removal by cooling the IRWST. In Level 2, SAHRS is credited for core spreading area flooding, active core melt cooling and the containment spray functions.

- Safety injection system is used for RCS inventory control in the Level 1 and the Level 2. In the Level 2, LHSI can prevent RPV failure. LHSI injection through the RHR heat exchanger is also credited for active core melt cooling as a backup to SAHRS.

The description of the major U.S. EPR frontline and support systems that are modeled in the shutdown Level 1 PRA is provided in Section 19.1.6.1.7.

The same human actions credited in the at-power Level 2 PRA are considered in the shutdown Level 2 PRA. The differences (e.g., additional actions, timing differences, Level 1 and Level 2 dependencies) are discussed in Section 19.1.6.3.3.5.

The LOOP is modified in the shutdown Level 2 PRA; it is not considered as a direct initiating event. It is modeled through a loss of RHR initiating event, and random LOOP in 24 hours is no longer an issue. LOOP recovery during the three time frames defined in the Level 2 at power PRA is credited in a similar way to the at-power LOOP recovery model.

### 19.1.6.3.2 Phenomenological Analysis

Shutdown temperatures, pressures, and decay heat levels are lower than at full power, resulting in most phenomenological evaluations at full power being bounding for the shutdown sequences. A review of the accident sequences occurring at full power resulted in identifying the phenomena, described in Sections 19.1.6.3.2.1 through 19.1.6.3.2.3, as requiring further investigations under shutdown conditions.

### 19.1.6.3.2.1 Induced RCS Rupture – Preclusion of Hot Leg Rupture, Modification of ISGTR Probability

RCS rupture modes are because of creep rupture, a temperature and pressure dependent phenomenon. RCS ruptures are possible in pressurized POS CA and CB where the cooling system is closed and can re-pressurize up to the RHR safety valves set point of 800 psia.

#### Induced Hot Leg Rupture:

Shutdown conditions (i.e., lower power, pressure, temperature, flow) make hot leg rupture unlikely. Therefore, it is not credited in the containment event trees for states CA and CB. This assumption is considered conservative based on the following:

- Induced hot leg rupture (IHLR) is a beneficial failure regarding the RCS system depressurization, but it contributes to a higher probability of containment failure following hydrogen combustion loads because the discharge in a given location may increase the hydrogen inventory.

- The hot leg rupture contribution to higher probabilities of containment failure through hydrogen combustion is outweighed by the more important decrease in probabilities of containment failure as a result of high pressure following direct containment heating, or vessel rocketing. Since IHLR is a beneficial failure mode with respect to containment failure, it is conservative not to credit its occurrence. Therefore, a probability of zero for IHLR occurrence was used in the shutdown model.

#### Induced Steam Generator Tube Rupture:

For LOCA sequences, reduced probabilities of induced SGTR were calculated in both POSs CA and CB compared to at-power. These probabilities were based on the probability of loop seal clearance determined in the at-power analysis. This approach is judged to be conservative, as loop seal clearance was found to be a major driver of induced SGTR in the at-power analysis. The values of 5.0E-02 for Seal LOCAs and 1.25E 02 for small LOCAs from the uncertainty study are used.

For transient sequences in POS CA and CB, MAAP runs did not predict tube ruptures even with thinned tubes. The probability of induced SG tube rupture is assessed based on insights from the at-power analysis; the probability of induced tube ruptures

following transient initiator was found to be of the same order of magnitude as the probabilities associated with small and seal LOCAs but smaller. Therefore a probability of 1.0E-02 for induced SGTR following transient initiators during shutdown states CA and CB is used.

#### 19.1.6.3.2.2 Hydrogen Phenomena Description and Probabilistic Evaluation

The hydrogen combustion modes considered in the shutdown states are as described in the at-power analysis in Section 19.1.4.2.1.2. The phenomenological assessments performed for containment loads derived from hydrogen combustion addressed containment failure because of overpressure from hydrogen deflagration or dynamic loads from flame acceleration. As identified in Section 19.1.4.2.1.2, there is a third hydrogen combustion mode known as deflagration-to-detonation transition. This destructive combustion mode is not explicitly modeled since the resulting loads are expected to be similar to flame acceleration loads and the flame acceleration is a pre-condition for detonation.

**Assessing hydrogen deflagration loads:**

A hydrogen deflagrations loads assessment was performed on a global basis based on the global AICC pressure.

Consistent with the full power study, hydrogen burning was not credited for hydrogen inventory reduction and the in-vessel hydrogen production was assessed as being in the range 30.5 percent to 65.5 percent equivalent Zircaloy oxidation.

Although induced hot leg rupture is not credited in shutdown conditions (see Section 19.1.6.3.2.1), conservatively the additional discharge of 300 kg of hydrogen due to this phenomenon was taken into account for all cases.

The baseline pressures used in assessing the probabilities of containment failure following hydrogen deflagrations were conservatively kept the same as at power.

**Assessing hydrogen flame acceleration loads:**

Similar to the at-power study, the analysis of local concentrations susceptibility to flame acceleration was carried out assuming the most conservative gas mixture properties including steam.

A limiting mixture concentration for flame acceleration susceptibility (as a function of oxygen and steam concentrations) was dynamically evaluated. A comparison of the combustible gas (i.e., hydrogen and carbon monoxide) concentration against this limiting mixture concentration was conducted for the 27 node MAAP model. According to the MAAP results, flame acceleration potential existed in the IRWST (containment node 2), the reactor pit (containment node 8) and the equipment rooms

(containment nodes 4, 6, and 10). To avoid an overestimation of the steam concentration in the IRWST volume and to approach more realistic conditions during shut-down, appropriate changes were made compared to the power operation model to increase the steam condensation in the IRWST volume. Additionally, a reduced number of recombiners may be available during certain periods of shutdown operation depending on the maintenance schedule. Therefore, the fraction of available PARs is varied in the MAAP runs for shutdown operation.

The results of the assessment of the containment failure probabilities following Hydrogen loads from both deflagration and flame acceleration are presented below. These probabilities are given for different time frames and represent either local (leak) or global (rupture) damage to the containment.

**Time frame before vessel failure:**

- Hydrogen deflagrations loads: high pressure core damage transient resulting in a probability of containment failure of 1.1E-03 for leak and 3.0E-05 for rupture.
- Hydrogen flame acceleration loads: high pressure core damage transient resulting in a probability of containment failure of 3.1E-03 for leak and 8.9E-07 for rupture.
- Recombiners damaged by accelerated flame: 3.1E-03.

**Time at vessel failure:**

- Hydrogen deflagrations loads: As the peak pressure following an AICC is higher before vessel failure than at vessel failure and the action of the recombiners until vessel failure reduces the amount of hydrogen participating in AICC, an evaluation of the hydrogen loads based on the global AICC pressure resulted in a negligible probability of containment failure.
- Hydrogen flame acceleration loads: high pressure core damage transient resulting in a probability of containment failure of 3.8E-03 (2.9E-03 for leak and 9.3E-04 for rupture).
- Recombiners damaged by accelerated flame: 4.1E-02.

**Time frame after vessel failure:**

- No significant hydrogen amounts higher than the peak masses were identified for short and long term periods after vessel failure. In addition the steam concentration exceeds the 55 percent threshold in the short and long term after vessel failure, inerting the containment for hydrogen deflagrations. The analysis of this time frame is considered bounding and the containment failure from hydrogen deflagration in this time period is discounted. Oxygen leakage back into containment (resulting in de-inerting the containment atmosphere) is not expected.
- Hydrogen flame acceleration loads:

- Containment rupture probability with intact recombiners: 9.0E-05
- Containment rupture probability with 50 percent recombiner availability: 1.0E-04
- Containment rupture probability with 25 percent recombiner availability: 5.0E-04

In all three scenarios, the contribution of containment leak is negligible. The failure probabilities apply both in high pressure and low pressure CDES.

#### 19.1.6.3.2.3 Other Phenomena

**Containment Fragility Curve**

The containment fragility curve developed for the full power states as a function of pressure loads can conservatively be used in the shutdown conditions. The composite fragility curve is weakly sensitive to temperature. Therefore, the curve used with a temperature of 309°F at power is adequately bounding for shutdown.

**Fuel Coolant Interactions**

*In-Vessel Steam Explosions:*

The assessment of the probability of in-vessel steam explosions failing containment at-full power is considered to be bounding for the shutdown conditions. The parameters, involved in the probabilistic evaluation, are unchanged in the probability of in-vessel steam explosions assessment.

The total mass of core, the total energy stored in the core material per unit mass at the time of relocation, and the fraction of core material in lower head participating in pre-mixing are expected to be unaffected by the power level. Also, the conversion ratio from thermal to mechanical energy, the fraction of mechanical energy transmitted to the slug, and the probability of steam explosion when a melt pour occurs are considered unchanged or lower given the lower operating pressure.

*Ex-Vessel Steam Explosions:*

The phenomenological evaluation in this case used the most conservative case from the full power study. This case was essentially a pour of the molten corium into an ex-vessel pool at vessel failure for a sequence where:

- The RCS was depressurized due to an induced hot leg rupture (at the RV nozzle), leading to water spillage in the reactor pit.
- The flow of corium into the pool is at the same rate as at vessel failure.

- A water pool for premixing of approximately 4 ft and 7 ft depth developing in the reactor pit for central and lateral RPV breach respectively.

However, since the induced hot leg rupture was discounted from the shutdown analysis, the precondition for ex-vessel steam explosion is not met.

### In-Vessel Recovery

The in-vessel recovery phenomenological evaluations at full power were applied to the shutdown without further modifications because the decay heat levels during the starting period of the shutdown sequences are similar or lower than at full power.

### Loads at Vessel Failure

The results of the at-power study are considered to be applicable in the shutdown conditions according to the following considerations:

- The vessel failure mode is independent from the reactor operated temperature, pressure or level of decay heat.

- Overpressurization of the reactor pit, rocketing of the vessel and direct containment heating are considered to be bounding in the at-power analysis since the operation pressure is lower in shutdown.

### Long Term Challenges

*Debris Quench Overpressure:*

The overpressure arising from debris quench at power is conservatively applied to shutdown. The fraction of debris quenched, the pressure increase in containment per fraction of debris quenched and the base initial containment pressure at the time of debris flooding are not expected to be higher than at power.

*Significant MCCI:*

The lower decay heat levels during shutdown are likely to lead to similar and even lower probabilities of MCCI occurrence.

*Containment Overpressure Failure due to non-condensable gases, Basemat Penetration or No Failure:*

In the event of an accident sequence with MCCI ongoing and sprays, active cooling or safety injection system preventing long term overpressure by steaming, the full power assessment considers whether a basemat melt-through or overpressure due to non-condensable gases would happen first. If steaming is not controlled, an overpressure would be the first failure mode. It is expected that the lower decay heat levels at shutdown would cause the basemat melt-through and the overpressure due to non-

condensable gases to be delayed, but there is no reason to expect a significant shift in the relative timing of the two failure modes.

Therefore, the probabilities at power are used without further modifications. Note that the probability of neither failure mode occurring may increase during shutdown due to the lengthening of the basemat erosion and overpressure transients. However, no credit was taken for this effect because the CET sequences involving either basemat erosion or overpressure due to the generation of non-condensable gases would be significant in the overall results.

*Containment Overpressure Failure due to Incomplete Melt Transfer:*

Because of the limited information on this phenomenon, high probabilities were assigned in the full power study and there is no reason to consider changing the values for the shutdown case. The full power study also assigned high probabilities in the case of a hot leg rupture, leading to a flooded reactor pit. However, as previously stated, no evidence of hot leg rupture was derived from the MAAP simulations at shutdown. Therefore, the modification of this probability is irrelevant.

**Equipment Survivability**

This evaluation is not affected by the power status of the reactor.

### 19.1.6.3.3 Containment Event Trees Analysis

#### 19.1.6.3.3.1 Containment Event Trees

The shutdown Level 2 PRA uses a total of four containment event trees. Most of the CETs used in the shutdown model are identical to the ones used at full power. Three types of CETs are carried out in the Level 2 shutdown model:

1. ISLOCA CETs.
2. Low pressure CETs.
3. High pressure CETs.

These full power CETs are modified in the shutdown Level 2 model to support the following conditions:

- Distinction between the different POS; C, D, and E achieved by assigning the appropriate CDES/POS combination in the link trees. The at power CETs are used without modification in the shutdown model, except for POS E where a specific low pressure CET is used.
- The low pressure CET (See Figure 19C-9) for POS E is modified to not account for the success of the containment isolation. This is because the equipment hatch closure is impossible in state E preventing successful containment isolation. The

only branches left are the ones resulting from a failure of isolation of an opening larger than 3 inches. Therefore, the function events representing the containment isolation (#T1 CI), containment failure before vessel breach (#T1 CF), late containment failure due to hydrogen deflagration, flame acceleration or quench spiking (#T3 CFH20), containment steam pressurization control (# T3 STMCNTL), and long term containment failure (#T3 LTCF=NO/OP/BMT) are removed with all the resulting branches.

- In the high pressure event tree (See Figure 19C-7) for POS C, the IHLR probability is conservatively taken to be zero by setting the probability of the function event (i.e., IHLR) to zero.

#### 19.1.6.3.3.2 Accident Class Release Categories

Fission product release categories have been defined to group the accident sequences end points of the Shutdown Level 2 CETs that have similar release characteristics (i.e., source terms).

These release categories are based on the same attributes as the at-power analysis that are discussed in Section 19.1.4.2.1.3 in Section, "Accident Class Release Categories." The release categories for the shutdown analysis are the same as for the at-power analysis and are provided in Table 19.1-19—Release Category Definitions.

#### 19.1.6.3.3.3 Source Term Evaluation

The source term associated with potential severe accident sequences identified by the Level 1 PRA occurring from an initially at-power condition is analyzed as part of the Level 2 PRA study. Tools, models, and codes available for such analysis are relatively mature; although, large uncertainties still exist with regard to certain phenomena and processes. The EPR Level 2 PRA used the MAAP 4.0.7 code to quantify the source terms associated with the at-power severe accident sequence release categories.

The codes and models available to simulate an accident occurring during shutdown have a number of limitations because they were not originally designed to simulate these conditions. Examples of such limitations are:

- Difficulties in modeling "open" RCS states (i.e., those where the RPV head is removed, and where the refueling cavity may or may not be filled).

- Modeling the effects of air ingress during the event.

The approach adopted in this U.S. EPR PSA2 shutdown study is a simplified approach for estimating shutdown source terms that addresses the specific aspects of shutdown conditions judged as most important.

This approach uses the results from a set of MAAP runs that were performed specifically for the shutdown state. Source terms for the intact containment and for a

1-meter square containment failure at time zero were evaluated for POS CA and CB using MAAP. The results of these MAAP runs were combined with the results from the at-power analysis and modifications were made based on insights from sensitivity studies performed during the analysis of at-power source terms. These modifications include decontamination factors due to containment sprays for MAAP each fission product group, and a multiplication factor for the source term that is calculated assuming no fission product retention in the primary system.

The results of the shutdown source term analysis for each of the Plant Operating States are contained in Table 19.1-113, Table 19.1-114, and Table 19.1-115.

#### 19.1.6.3.3.4 Air Ingression

During accident scenario progression, the introduction of air into the damaged reactor core (air ingression) can further facilitate the oxidation of fuel. Some fission product releases, such as ruthenium (Ru), can be enhanced by the air ingression-induced fuel oxidation forming volatile Ru oxides ($RuO_x$) of radiological importance.

Air ingression scenarios with potential applicability to the EPR include:

1. Vessel Failure – Accidents where the RPV fails and air is drawn up into the vessel passing over the overheated fuel matrix.

2. Line Rupture – Breaks in the RCS line that allows air to be drawn down into the RPV and across the overheated fuel matrix.

3. Refueling Operations – Loss of coolant accident during refueling operations when the fuel handling when the RPV head is removed and the water level drops allowing the fuel to become exposed to air in the atmosphere.

During an EPR vessel rupture or breach, air ingression can occur when a failure in the lower vessel opens an air pathway upwards into the lower region of the core. Air can contact the overheated, damaged fuel in the reactor core. Similarly, a break or rupture in a portion of the RCS piping can open an air ingression pathway drawing air down through the RPV and allowing contact with fuel matrix in the reactor core. Both of these scenarios have the potential to generate high convective air flows through the core material and produce an environment of increased oxidation potential adjacent to the fuel matrix. These air ingression scenarios are analyzed in the EPR Level 2 with the impact evaluated in the EPR Level 3.

During shutdown refueling operations, the potential to establish an air ingression pathway exists when head had been removed and fuel is either in place or being moved. A rupture or breach of the vessel or other failure that results in the loss of coolant can cause the fuel to become uncovered. Without adequate cooling, the fuel can become overheated and fail. In this scenario, the fuel is oxidized when exposed to

air in the atmosphere. This air ingression scenario is addressed in the EPR Shutdown Level 2.

Due to the increased oxidation associated with the air ingression scenarios, the formation of $RuO_x$ compounds becomes a related effect. The contribution of the increased $RuO_x$ in the releases from air ingression accident scenarios is determined by MAAP analysis and is represented in the EPR Level 2 source term results. Ruthenium is present in the fuel as elemental Ru and is transformed to its form as $RuO_2$ in the fission product releases. Once the primary system or reactor pressure vessel has been breached, the Ru transport and release is phenomenologically characterized as $RuO_2$. Modeling of air ingression release scenarios is performed using the MAAP chemical transformation, equilibrium, reaction kinetics, aerosol and deposition rates, transport processes and other process variable applications from the existing subroutines and parameters to simulate air flow and oxidation rates. Further oxidation of $RuO_2$ into the highly volatile $RuO_4$ species is not modeled by MAAP; however, the total mass of Ru released from the fuel is not affected by this modeling decision.

Results of sensitivity analyses has shown that enhanced $RuO_x$ formation does increase the risk of early fatalities, but does not change the conclusions of the SAMDA analysis contained in the U.S. EPR Environmental Report (Reference 59).

#### 19.1.6.3.3.5 Large Release Definition

The definition of large release described in the at-power analysis is applied to the shutdown Level 2 analysis. Using the same criteria, the same set of Release Categories is found to lead to large release—RC201 through RC205, RC301 through RC304, RC702, and RC802.

It should be noted that the release fractions for RC206 in Plant Operating State D exceeds the guidelines for Large Release for I, Cs, and Te. However, because of the conservative nature of the process used for the estimation of release fractions with the primary system open, they are judged not to result in large releases.

It is further noted that release categories RC502, RC504, and RC602 are not judged to result in large releases in Plant States Ca and Cb even though the release fraction of tellurium (Te) in Tables 19.1-113 and 19.1-114 exceeds the value for large release fraction. This is because the release fractions for iodine, cesium, as well as tellurium dioxide and molecular tellurium (TeO2 and Te2) contributors to the Te group in these tables are all more than an order of magnitude below the guidance for large release. With such low values for the iodine, cesium, and tellurium species, it is unlikely that off-site consequences would be greater than one mean fatality at one mile.

#### 19.1.6.3.3.6 Human Reliability Analysis

The human reliability analysis for the Shutdown Level 2 PRA analysis is based on the analysis performed for the at-power Level 2. In particular, the severe accident management guidance upon which the Level 2 actions are based and the HRA methodology used are assumed to be similar in shutdown. Several elements are modified for the shutdown study:

- Four new actions are modeled in the hatch closure sequences. These actions cover the hatch closure with and without power for transient and LOCA sequences as described in Section 19.1.6.3.1.
- The event timelines are different; therefore, operator action timings were re-evaluated.
- The Level 1 actions modeled are different (shutdown actions instead of at-power); therefore, dependencies of Level 2 actions on Level 1 actions were analyzed.

All other elements of the at-power analysis were incorporated without modification.

### 19.1.6.4 Results of the Low Power and Shutdown Level 2 Evaluation

#### 19.1.6.4.1 Low Power and Shutdown Operating States Level 2 Risk Metrics (LRF, CCFP)

The total LRF from shutdown events is 7.9E-9/yr. This is well below the NRC goal and the U.S. EPR probabilistic design goal of 1E-6/yr.

The CCFP from shutdown events alone for large release sequences is 0.13.

Both the LRF from shutdown and CCFP values and goals, are considered in the combination with power operation, as discussed in Section 19.1.8.

#### 19.1.6.4.2 Low-Power and Shutdown Plant Operating States Core Damage Release Category Results

The release categories and their contribution to the shutdown events LRF and the associated CCFP are shown in Table 19.1-116—U.S. EPR Large Release Category Results - Level 2 Shutdown.

More than 85 percent of the total shutdown events LRF comes from three release categories: RC203 (51.2 percent), RC802 (23.8 percent) and RC204 (10.8 percent). Release category RC203 represents containment failure due to isolation failure with melt released from the vessel, ongoing MCCI, and failed containment sprays. RC204 is also a containment isolation failure with melt released from the vessel but no MCCI and successful SAHRS sprays. Containment isolation failure in shutdown also includes failures due to an open containment hatch.

Release category RC802 represents containment bypass due to ISLOCAs events in shutdown (RHR line ruptures outside containment). The three next largest contributors to the LRF (>one percent) come from RC201 (9.9 percent) and RC205 (3.2 percent). These release categories are discussed in two groups below. Release category RC201 represents containment failure due to isolation failure with melt retained in-vessel. Release category RC205 represents containment isolation failure with melt released from the vessel and flooded without containment sprays.

Overall, containment isolation failures RC201 to RC205 contribute about 75.1 percent to the total shutdown LRF. Although the containment hatch is closed in POS D, containment isolation RC203 is the dominant contributor to LRF in this POS because large containment isolation lines are open. The high contribution of containment isolation failures is expected for the shutdown events where there is less restriction on containment isolation and containment is open for outage activities.

Release categories RC300 and RC400 contribute about one percent of the total shutdown LRF and represent containment rupture before vessel breach and at vessel rupture respectively. In the shutdown sequences, containment rupture before vessel breach occurs due to hydrogen combustion loads.

The contribution to LRF from the different POSs is presented in Table 19.1-117—U.S. EPR Large Release Frequency for each POS - Level 2 Shutdown. The highest LRF contribution is associated with POS CB which is dominated by a loss of RHR cooling initiator followed by POSs CA, D, and E. The contributions of the different POSs to the total shutdown LRF are consistent with the contributions to the shutdown CDF with the exception of POS E. This POS represents a guaranteed large failure of containment isolation as the hatch is assumed to be open and cannot be closed as the vessel heads off and the boiling time is too short to credit operator actions. Therefore, the LRF frequency is the same as the CDF and the CCFP is equal to 1.

The conditional containment failure probabilities in POS CA and CB are the same and slightly higher than in POS D (0.11 versus 0.10). Although, containment isolation modeling is similar in POS CA and CB the hatch closure modeling is different. It is assumed that POS CB has a higher operator failure probability to close the hatch because the water inventory is lower (mid-loop), leading to a shorter boiling time and therefore less time to perform the operator action. This results in POS CB contributing more to the shutdown LRF than POS CA. The sequences in POSs CA and CB are driven by a common cause failure of HVAC in all four divisions disabling the electrical supply to containment isolation MOVs, basemat flooding, and SAHRs sprays.

The contribution to LRF from shutdown initiating events is shown in Table 19.1-118—U.S. EPR Large Release Frequency for each Initiating Event - Level 2 Shutdown. Three events contribute over 10 percent each to the total LRF: Loss of RHR during Shutdown State CBD (12.6 percent), RHR ISLOCA During Shutdown

State E (11.6 percent), and loss of RHR During Shutdown State CAD (11.1 percent). The initiator loss of RHR from shutdown POS C and D contributes about 50 percent of the shutdown LRF and RHR ISLOCA in POS C, D, and E contributes about 24 percent of the shutdown LRF. The high contribution of this initiator to the LRF is due to the loss of electrical divisions from common cause failure of the HVAC systems which lead to the initiator loss of RHR and fails the containment isolation power supply (hatch closure in POS C and large containment isolation lines in POS C and D).

Uncontrolled level drop initiators in POS C and D contribute to about 14 percent of the shutdown LRF, followed by small LOCA and large LOCA (contributing 11 percent and 1 percent respectively) in POS C, D, and E.

A matrix of different release category frequencies for different POS states is shown in Table 19.1-119—U.S. EPR Release Category Frequencies for each POS - Level 2 Shutdown. The release categories that contribute to the total Large Release Frequency are bolded.

Figure 19.1-32, Figure 19.1-33, Figure 19.1-34, and Figure 19.1-35 illustrate release category contributions to the LRF in different POSs. POS C is dominated by RC203 (about 60 percent) representing containment isolation failure with failed in-vessel recovery, ongoing MCCI, and failed SAHRS sprays. The next contributors contribute the same fraction (about 16 percent) to POS C shutdown LRF. These are release category RC201 representing containment isolation with successful vessel recovery and RC802 representing ISLOCA events. All other release categories contribute less than 3 percent.

POS D is also dominated by RC203 (about 73 percent) representing containment isolation failure with failed in-vessel recovery, no MCCI, and successful SAHRS sprays. The next release category is RC802 with a similar contribution to that of POS C (about 16 percent). The remaining release categories represent containment isolation failures and contribute less than 10 percent.

POS E is dominated by RC 802 (about 50 percent) followed by RC204 and RC203. Although the containment hatch is open in this state, the release category representing ISLOCA sequences dominates the LRF in this POS. This is because the core damage sequences from ISLOCA initiators represent 50 percent of the shutdown CDF. Each POS contribution to the shutdown LRF is illustrated in Figure 19.1-36—POS Contributions to Shutdown LRF. As opposed to POS contribution to the shutdown CDF, POS D is the smallest contributor because the containment is assumed to be closed in that state. Shutdown initiating event contributions to the shutdown LRF are illustrated in Figure 19.1-37—Initiating Events Contributions to Shutdown LRF. Loss of RHR and RHR ISLOCA in POS C, D, and E contribute more than 74 percent to the total shutdown LRF.

### 19.1.6.4.3 Significant Cutsets and Sequences

Cutset contribution to the shutdown events LRF is equally distributed. The number of cutsets that contribute to 95 percent of LRF is over 14,000.

The significant cutsets for shutdown events are illustrated in Table 19.1-120—U.S. EPR Important Cutset Groups - Level 2 Shutdown. In this table, the top cutsets for each release category are grouped together based on their similar/symmetric impact on the Level 1 and Level 2 mitigating systems. Columns in the table show: corresponding release category, group number, the cutsets numbers included in the group, frequency range of the cutsets included in the group, group percentage contributions to the total shutdown LRF, and a selected representative cutset, with corresponding basic events and their descriptions.

As shown in Table 19.1-120, the top cutsets in all large release categories are grouped into 29 groups representing over 60 percent of the shutdown LRF. The top cutsets for each release category contributing more than one percent to the LRF are described below.

#### Release Category 201:

This cutset group contributes about 1.5 percent to the shutdown LRF. The sequence represents an RHR initiator caused by a LOOP event during shutdown and common cause failure of all 1E 2hr batteries results in failure of all EDGs. Failure of all EDGs and inability to connect SBODGs due to the loss of the batteries result in total loss of divisional power. After core damage, the depressurized sequence leads to large containment isolation failure due to the primary drain lines being open and failure to close following loss of electrical Divisions 1 and 4. In-vessel recovery is successful after power recovery within 7 hours.

Due to a conservative modeling choice in the in-vessel recovery, the phenomenological failure probabilities corresponding to LOOP and transient conditions are both applied to sequences starting as transient with a random LOOP within 24 hours.

#### Release Category 203:

This cutset group contributes about 12 percent to the shutdown LRF. The sequence represents RHR initiator caused by common cause failure of Safeguard Buildings 1 and 4 supply fans, which cause the loss of the running CCWS pumps plus operator failure to switch to standby CCWS pumps resulting in total loss of HVAC. Depressurization is failed due to the loss of electrical Divisions 1 and 4. After core damage, the depressurized sequence leads to large containment isolation failure due to the primary drain lines being open and failure to close following loss of electrical Divisions 1 and 4. There is significant MCCI with failure of debris flooding due to failure to open the

MOVs on the passive flooding lines. This sequence has no creep induced SGTR and no pit overpressure failure in cases without circumferential break of the vessel. SAHRS sprays are failed due to common cause of the IRWST strainers.

**Release Category 204:**

This cutset group contributes about 7 percent to the shutdown LRF. The sequence represents small LOCA in cold leg injection line 1, and common cause failure of common cold leg injection valves results in loss of all injection. After core damage, the sequence leads to large containment isolation failure due to the primary drain lines being open and failure to close following loss of electrical Divisions 1 and 4. There is significant MCCI with failure of debris flooding due to failure to open the MOVs on the passive flooding lines. SAHRS sprays fail due to common cause of the IRWST strainers.

**Release Category 205:**

This cutset group contributes less than one percent to the shutdown LRF. The sequence represents small LOCA in cold leg injection line 1, and common cause failure of common cold leg injection valves results in loss of all injection. After core damage, the sequence leads to large containment isolation failure because the hatch is open in POS E and cannot be closed. There is no MCCI with debris flooded following successful opening of the MOVs on the passive flooding lines. SAHRS sprays fail due to preventive maintenance.

**Release Category 802:**

This cutset group contributes about 19 percent to the shutdown LRF. The sequence represents ISLOCA caused by RHR Pipe break and failure to isolate. After core damage, the sequence leads to containment bypass following ISLOCA initiator with unscrubbed releases.

### 19.1.6.4.4 Significant CDES, Phenomena, Basic Events

Table 19.1-121—U.S. EPR CDES Contribution to the LRF - Level 2 Shutdown shows that the largest contributing CDES represents SGTR core damage sequences followed by Seal LOCA with a secondary side depressurized with a high likelihood of creep induced SGTR. Other important contributors (greater than one percent) are high pressure transients and small LOCA core damage sequences.

Table 19.1-122—U.S. EPR Risk-Significant Phenomena based on FV Importance - Level 2 Shutdown and Table 19.1-123—U.S. EPR Risk-Significant Phenomena based on RAW Importance - Level 2 Shutdown show important phenomenological events. Events contributing more than 10 percent to the shutdown LRF are discussed below:

- The event L2PH CCI-DRY contributes about 52 percent to the shutdown LRF. This event represents cases with dry spreading area (debris not flooded with significant MCCI) and appears in all RC203 cutsets (which itself contributes about 51 percent to the shutdown LRF). The remaining contribution comes from release categories with ongoing MCCI. This event does not represent a direct containment failure but rather a phenomenological occurrence during the sequences that have indirect impact on containment performance.

- L2PH PF-VF NO-CBV=N contributes about 41 percent to the shutdown LRF. This event represents cases without pit overpressure failure in cases without complete circumferential failure of the vessel. This event does not represent a direct containment failure but rather a phenomenological occurrence during the sequences that have indirect impact on containment performance.

- The event L2PH ISGTR-TR=N and L2PH ISGTR-SS,SL=N represent high pressure core damage sequences and seal or small LOCAs respectively, without SGTR and a pressurized secondary. These events contribute to about 28 percent and 11 percent of the shutdown LRF respectively and do not represent a direct containment failure but rather characterize the top contributing sequences to the LRF.

- L2PH STMEXP EXV=N contributes about 24 percent to the shutdown LRF. This event represents cases with ex-vessel steam explosion avoided in dry pit sequences. This event does not represent a direct containment failure but rather a phenomenological occurrence during the sequences that have indirect impact on containment performance. It should be noted that the shutdown analysis assumes that induced hot leg rupture does not occur and therefore the conditions for ex-vessel steam explosion are not met.

- L2PH NO CCI contributes about 13 percent to the shutdown LRF. This event represents the probability of avoiding molten core concrete interaction with a successful basemat flooding. This event does not represent a direct containment failure but rather a phenomenological occurrence during sequences that indirect impact on containment performance and is more relevant to characterize the source term.

- The next basic event representing direct containment failure due to a rupture is L2P VECF-FA(H) representing very early containment failure due to hydrogen flame acceleration (in high pressure sequences). This event contributes less than one percent to the shutdown LRF, however the early hydrogen failure event has the largest RAW value (close to 3.3) of the phenomenological events listed in Table 19C-2.

- Three events have RAW values greater than 2, these are:

  – L2PH STM EXP INV LP containment rupture at vessel rupture due to in-vessel steam explosion in low pressure sequences (RAW 6.8).

  – L2PS VECF-H2DEF H containment leak before vessel rupture due to hydrogen deflagration in high pressure sequences (RAW 3.3).

– L2PS VECF-FA(H) containment rupture before vessel rupture due to hydrogen flame acceleration in high pressure sequences (RAW 3.3).

Table 19.1-124—U.S. EPR Risk Significant Level 2 Human Actions based on either FV or RAW Importance - Level 2 Shutdown shows the risk-significant Level 2 human actions based on FV and RAW importance measures. Level 1 operator actions dominate the internal LRF with the three largest contributors being actions related to recovery of room cooling, CCW supply to common header, and isolation of RHR pipe break. The most important operator actions are actions to close equipment hatch in two different time frames, with or without power available. One of these actions is not credited in the model (probability of failure is set to one), that is the action to close hatch in one hour without power.

Most operator actions are relevant for long term mitigation of the containment overpressure, flooding of the basemat, and scrubbing of radioactive releases. These actions are not captured in the release categories defining the LRF and would be seen in sequences related to RC500 and RC600.

Table 19.1-125—U.S. EPR Risk Significant Components based on FV Importance Measure Related to Level 2 Specific Importance - Level 2 Shutdown and Table 19.1-126—U.S. EPR Risk Significant Components based on RAW Importance Measure Related to Level 2 Specific Importance - Level 2 Shutdown show the risk-significant components from the shutdown LRF calculation. Insights from these tables show that important components are similar to those identified in the at-power LRF. Considering contributions from the components listed, the following systems are the largest contributors; HVAC, electrical system, and SIS. Systems contribution based on RAW values did not identify additional systems as important. Note that the risk is dominated by support systems rather than frontline mitigation systems.

Passive SSCs are not represented in the LRF as they perform long term action where phenomena are slowly progressing. For instance, the PARs and spreading area structure would be represented in release categories RC500 and RC600 which are not part of the LRF group.

### 19.1.6.4.5 PRA Key Assumptions and Insights

#### 19.1.6.4.5.1 PRA Key Assumptions

Many assumptions are made in the process of evaluating and quantifying Level 2 phenomena in the LPSD state. The major assumptions are:

- The containment hatch would be closed in POS D, and that this would be regulated by implementation of NUMARC 91-06 guidance.

- In the case of an accident, the ability to close containment hatches and penetrations during Modes 5 and 6 prior to steaming to containment is important. It is assumed that procedures and training will be developed to ensure success of these actions.

- The equipment hatch is considered open in shutdown POS Ca, Cb, E, and closed in D. Except in POS E, the ability to close hatch is credited. The initial actions are performed inside the containment; therefore, the habitability of the containment (i.e., local temperature) is considered to be the limiting criterion in determining the time available to close the hatch. The closing action is assumed to take 20 minutes if power is available, or 90 minutes requiring 6 operators if the power is not available.

- All containment isolation valves are considered to have equal or higher probabilities of being open compared to the full power. No containment isolation line is assumed to be closed during entire shutdown duration.

- Although there could be a large difference in decay heat levels, the similar POSs from shutting down and starting up (i.e., CAd and CAu) are analyzed as 1 group. Decay heat from the shutdown states was used, which is conservative when estimating times available to close the hatch.

- Induced RCS ruptures (ISGTR) are only considered possible in pressurized POSs CA and CB. IHLR is assumed to not occur; this is a conservative assumption since the IHLR is beneficial in the RCS depressurization. ISGTR is not considered in transient sequences and retained with lower probabilities than at-power.

- In source term evaluation, the release fractions are calculated assuming all of the fission products are released into the containment atmosphere with no retention within the primary systems.

- Due to the limitations of the MAAP code, the phenomenon of air ingression into the corium in the vessel was not analyzed quantitatively; the release fractions do not reflect the impacts of the effects of Ru evolution.

- Scrubbing effects were not considered for ISLOCAs—RHR pipe breaks outside containment.

- In state CA, all transient-induced LOCAs are treated as seal LOCAs.

#### 19.1.6.4.5.2 PRA Insights

Some of the insights from the LPSD Level 2 PRA are:

- There are no outliers in the U.S. EPR shutdown events LRF.

- A significance of the contribution from different shutdown POSs to the LRF can be connected to either a high CDF, as in POS CA and CB, or to the containment status, as in POS E when containment is open and not re-closable.

- The containment hatch status and operator actions to close the hatch are important contributors to the shutdown events LRF.

- The event, "Very Early Containment Failure due to Hydrogen Flame Acceleration", is identified as an important contributor to the shutdown events LRF, with both importance measures, FV and RAW, above screening criteria.

### 19.1.7 PRA-Related Input to Other Programs and Processes

#### 19.1.7.1 PRA Input to Design Programs and Processes

Section 19.1.1.1 and Section 19.1.3.4 provide a description of how the PRA is used in the certified design process.

As stated in Section 19.1.1.1, the COL applicant will describe the uses of PRA in support of site-specific licensee design programs and processes.

#### 19.1.7.2 PRA Input to the Maintenance Rule Implementation

The PRA is not used to support Maintenance Rule implementation at the design certification stage.

As stated in Section 19.1.1.4, the COL applicant will describe the uses of PRA in support of licensee programs such as Maintenance Rule implementation during the operational phase.

#### 19.1.7.3 PRA Input to the Reactor Oversight Process

At the design certification stage, the PRA is not used to support the Reactor Oversight Process.

As stated in Section 19.1.1.4, the COL applicant will describe the uses of PRA in support of licensee programs such as the Reactor Oversight Process during the operational phase.

#### 19.1.7.4 PRA Input to the Reliability Assurance Program

The PRA is used to provide input to the RAP. Specifically, the PRA is used to identify SSC that are potentially risk-significant, and therefore should be considered by the RAP expert panel as candidate SSC under the RAP program. The probabilistic approach to determining SSC risk significance is based on assessment of PRA importance measures. The PRA importance measures do not provide the only insight to SSC risk significance determination. In addition to the PRA importance measures, the expert panel also considers deterministic, safety analysis insights and appropriate operating experience when making the final determination of the RAP scope. Refer to Section 17.4 for a description of the Reliability Assurance Program.

As stated in Section 19.1.1.4, the COL applicant will describe the uses of PRA in support of licensee programs such as RAP implementation during the operational phase.

### 19.1.7.5 PRA Input to the Regulatory Treatment of Non-Safety-Related Systems Program

The U.S. EPR plant design is an evolutionary design primarily based on existing LWR technology and incorporates safety-grade active systems with no passive backup systems. As a result, the RTNSS process is not applicable to the U.S. EPR design. The U.S. EPR design is capable of meeting NRC requirements without the need for the RTNSS process.

## 19.1.8 Conclusions and Findings

A summary of PRA assumptions and insights, and how they relate to the different U.S. EPR design features are presented in the following tables:

- Table 19.1-102—U.S. EPR Design Features Contributing to Low Risk.
- Table 19.1-108—U.S. EPR PRA Based Insights.
- Table 19.1-109—U.S. EPR PRA General Assumptions.
- Table 19.1-131—Key Sources of Uncertainties

The numerical results are discussed below.

### 19.1.8.1 Risk Metrics:

The total CDF from internal events, internal flooding events, and internal fire events at power is 4.8E-07/yr. This is well below the NRC goal of 1E-04/yr (SECY-90-016), and the U.S. EPR probabilistic design goal of 1E-05/yr.

The total CDF from all events in shutdown is 6.0E-07/yr, also well below the NRC goal of 1E-04/yr (SECY-90-016), and the U.S. EPR probabilistic design goal of 1E-05/yr.

The total CDF from all events at power and shutdown is 5.4E-07/yr, also well below the NRC goal of 1E-04/yr (SECY-90-016), and the U.S. EPR probabilistic design goal of 1E-05/yr.

Total LRF from internal events, internal flooding events, and internal fire events at power is 3.0E-08/yr. This is well below the NRC goal and the U.S. EPR probabilistic design goal of 1E-06/yr.

The CCFP from internal events, internal flooding events, and internal fire events at power, for large release sequences is 0.06.

Mean values and associated uncertainty distributions can be found in Section 19.1.8.4.

The total LRF from shutdown events is 7.9E-9/yr which is also well below the NRC and U.S.EPR probabilistic design goals. The resulting CCFP for shutdown events is 0.13.

The total LRF for both at power and shutdown events is 3.8E-08/yr. The resulting overall CCFP remains at 0.7. This demonstrates, on an overall basis, both NRC probabilistic goals and U.S. EPR probabilistic design goals for these parameters are met.

### 19.1.8.2 Risk Distribution:

The distribution of the at-power CDF from internal events, floods, and fires is illustrated in Figure 19.1-24—U.S. EPR Level 1 Initiating Event Contributions to Total CDF at Power. Internal events contribute 50 percent to the total risk, fires 38 percent and floods 12 percent.

The distribution between the different POS for Total CDF (at-power plus shutdown) is illustrated in Figure 19.1-25—U.S. EPR POS Contributions to Total CDF. The at-power contribution remains dominant overall while State CB dominates shutdown CDF.

The distribution between the different plant operating states is illustrated in Figure 19.1-38-POS Contributions to Total LRF. At-power risk contributes 79 percent to the total risk. State CB dominates shutdown LRF.

All at-power initiating events that contribute more than one percent to the total CDF at-power, are shown in Table 19.1-103—U.S. EPR Level 1 Top Initiating Event Contributions to the Total CDF at Power (Contributing more than 1% to Total CDF) Rank. Fire in the SB 1 or SB 4 switchgear rooms dominates the total risk. The LOOP SBO initiating event is the second largest contributor, followed by the general LOOP initiating event (which is not SBO or RCP LOCA related), SLOCA, and a Loss of Component Cooling.

The distribution of the at-power LRF from internal events, flood and fire initiating events is illustrated in Figure 19.1-26—U.S. EPR Level 2 Initiating Event Contribution to Total At-Power LRF. Internal events contribute 47 percent to the total risk, fires 25 percent and floods 28 percent. The largest contributors are SGTR (20 percent) and LOCCW (11 percent).

The distribution of the release categories for the total at-power LRF is illustrated in Figure 19.1-27—U.S. EPR Level 2 Release Category Contribution to Total At-Power LRF. Containment bypass from steam generator tube rupture in the Release Category 702 contributes approximately 48 percent to total LRF. Interfacing system LOCA from

SIS pipe breaks in Release Category 802 contributes approximately 27 percent to the total LRF. Large containment isolation failures in Release Categories 201 through 205 represent approximately 19% of the total LRF. Early containment failures at the time of vessel failure contribute approximately 4 percent, and very early containment failures before vessel rupture contribute approximately 2 percent to the total at-power LRF.

### 19.1.8.3 Importance Ranking:

Significant SSC, operator actions and common cause events are defined in the corresponding sections for internal, flood, fire and shutdown events.

### 19.1.8.4 Sensitivity and Uncertainty:

A sensitivity analysis was performed to evaluate the impact of a series of assumptions on the CDF from internal, fire and flooding events. The sensitivity results are shown in Table 19.1-104—U.S. EPR Level 1 Total Events Sensitivity Studies. The insights that can be drawn from these results are similar to those that were presented for internal events, flooding events, and fire events in the corresponding sections. The impacts from all initiating events are reflected in the total CDF.

As it can be seen from the table, the total CDF is sensitive (delta CDF >100 percent) to the assumptions on HVAC room recovery, HEP values, EDGs and SBO DGs common cause group, and taking all safety train out for a year. It is also sensitive (delta CDF ≈100 percent) to the assumptions on the RCP seal LOCAs and offsite power recovery. A very conservative sensitivity case was evaluated to estimate combined effects of different assumptions. Overall result is an approximate 14 times increase in the CDF, to 7.5E-06/yr, still well below the NRC goal of 1E-04/yr. This again confirms robustness of the U.S. EPR design.

The results of the Level 1 uncertainty analysis for all internal, fire, and flood initiators are shown in Figure 19.1-29—U.S. EPR Level 1 Internal Events Total Uncertainty Analysis Results - Cumulative Distribution for All Internal, Fire and Flood Events CDF. Treatment of parametric uncertainty is described in Section 19.1.4.1.2.7.

The uncertainty results are:

- CDF Internal, Fire & Flood Events Mean Value: 6.9E-07/yr.
- CDF Internal, Fire & Flood Events 5 percent Value: 1.0E-07/yr.
- CDF Internal, Fire & Flood Events 95 percent Value: 1.7E-06/yr.

This ninety-fifth percentile CDF value is more than one order of magnitude below the NRC goal of 1E-04/yr.

The results of the uncertainty analysis for at-power LRF from all internal, fire, and flooding initiators will be shown in Figure 19.1-30—U.S. EPR Level 2 Internal Events Total Uncertainty Analysis Results - Cumulative Distribution for All Internal, Fire and Flood Events LRF.

## 19.1.9 References


1. NUREG-0800, Section 19, "Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors," SRP. U.S. Nuclear Regulatory Commission, June 2007.

2. SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs," U.S. Nuclear Regulatory Commission, April 2, 1993.

3. ASME RA-S-2002, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," The American Society of Mechanical Engineers, April 5, 2002.

4. ASME RA-Sa-2003, Addendum A to RA-S-2002, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," The American Society of Mechanical Engineers, December 5, 2003.

5. ASME RA-Sb-2005, Addendum B to RA-S-2002, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," The American Society of Mechanical Engineers, December 30, 2005.

6. NUREG/CR-6850, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities," TR 1011989, Electric Power Research Institute and U.S. Nuclear Regulatory Commission Report, September 2005.

7. ANSI/ANS-58.21-2003, "External Events PRA Methodology," American National Standards Institute/American Nuclear Society, 2003.

8. NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events," U.S. Nuclear Regulatory Commission Report, May 1991.

9. NUREG/CR-4772, A. Swain, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," U.S. Nuclear Regulatory Commission Report, February 1987.

10. NUREG/CR-6883, D. Gertmen, H. Blackman, J. Marble, J. Byers and C. Smith, "The SPAR-H Human Reliability Analysis Method," INL/EXT O5-00509, Idaho National Laboratory/U.S. Nuclear Regulatory Commission, August 2005.

11. NUREG-1560, "Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance," U.S. Nuclear Regulatory Commission Report, Parts 2 – 5, Final Report (Vol. 2), December 1997.

12. NUREG-1742, "Perspectives Gained from the Individual Plant Examination of External Events (IPEEE) Program," U.S. Nuclear Regulatory Commission Report, Final Report (Vol. 1), April 2002.

13. NUREG/CR-5750, J.P. Poloski, et al., "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995," U.S. Nuclear Regulatory Commission, February 1999.

14. EPRI ALWR-URD, "EPRI Advanced Light Water Reactor Utility Requirements Document," December 1995.

15. NUREG/CR-5744, "Assessment of ISLOCA Risk-Methodology and Application to a Westinghouse Four-Loop Ice Condenser Plant," U.S. Nuclear Regulatory Commission, March 1992.

16. EPRI NSAC-154, "ISLOCA Evaluation Guidelines," Electric Power Research Institute, Final Report, September 1991.

17. NUREG/CR-6365, "Steam Generator Tube Failures," U.S. Nuclear Regulatory Commission, April 1996.

18. NUREG/CR-5500, "Reliability Studies," 2004 Updates, U.S. Nuclear Regulatory Commission, October-November 2005.

19. NUREG/CR-6928, Eide, S.A., et al. "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Commission Report, February 2007.

20. NUREG-1829, Tregoning, R., et al. "Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process," U.S. Nuclear Regulatory Commission Report (Draft Report for Comment), June 2005.

21. NUREG/CR-6890, S. A Eide, C. D. Gentillon, T. E Wierman and D. M. Rasmuson, "Reevaluation of Station Blackout Risk at Nuclear Power Plants," U.S. Nuclear Regulatory Commission Report, December 2005.

22. EGG-SSRE-8875, S. A. Eide, S. V. Chmilewski and T. D. Swantz, "Generic Component Failure Database for Light Water and Liquid Sodium Reactor PRAs," EG&G Idaho, 1990.

23. VGB-TW-803e, "Reliability Data for Nuclear Power Plant Components: Analysis for 2002," for the Centralized Reliability and Events Database (ZEDB), VGB Power Tech Service Gmbh, 2002.

24. EIReDA, EIReDA95, "European Industry Reliability Data Bank," Volume 2, 1977/ 1993.

25. NUREG-1715, "Component Performance Studies," U.S. Nuclear Regulatory Commission, 1999.

26. NUREG/CR-5485, "Common-Cause Failures in Probabilistic Risk Assessment," U.S. Nuclear regulatory Commission, November 1998.

27. CCF Parameter Estimations, 2003 Update," U.S. Nuclear Regulatory Commission, http://nrcoe.inl.gov/results/CCF/ParamEst2003/ccfparamest.htm, May 2006.

28. NUREG/CR-4772, Swain A., "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," SAND86-1996, U.S. Nuclear Regulatory Commission, February 1987.

29. ANP-10268P, Revision 0, "U.S. EPR Severe Accident Evaluation," AREVA NP Inc., October 2006.

30. SECY-90-016, "Evolutionary LWR Certification Issues and Their Relationships to Current Regulatory Requirements," U.S. Nuclear Regulatory Commission, January 1990.

31. B.R. Seghal et al. "Assessment of reactor vessel integrity (ARVI)." Report on EC contract FIKS-CT1999-00011, KTH, Royal Institute of Technology, Division of Nuclear Power Safety, Stockholm, Sweden.

32. NUREG/CR-6338, USNRC Contractor Report, "Resolution of the Direct Containment Heating Issue for all Westinghouse Plants With Large Dry Containments or Subatmospheric Containments," SAND 95-2381, U.S. Nuclear Regulatory Commission, January 1996.

33. NUREG/CR-6119, "MELCOR Version 1.8.5 manual. (Hydrogen burn model description)." Revision 2, Volume 2, U.S. Nuclear Regulatory Commission, May 2000.

34. NEA/CSNI/R(2000)7, Breitung, W., Chan, C.K., Dorofeev, S.B., Eder, A., Gelfand, B.E., Heitsch, M., Klein, R., Malliakos, A., Shepherd, J.E., Studer, E., Thibault, P. "Flame Acceleration and Deflagration to Detonation Transition in Nuclear Safety," (State-of-the-Art Report by a Group of Experts), OECD Nuclear Energy Agency, August 2000.

35. Deleted.

36. EPRI Product ID #1012045, "Assessment of a Performance Based Approach for Determining the SSE Ground Motion for New Plant Sites, V.2, Seismic Hazards Results at 28 Sites," Final Report, Electric Power Research Institute, May 2005.

37. EPRI Product Code #1012044, "Assessment of a Performance Based Approach for Determining the SSE Ground Motion for New Plant Sites, V.1, Performance Based Seismic Design Spectra," Final Report, Electric Power Research Institute, June 2006.

38. EPRI TR-103959, "Methodology for Developing Seismic Fragilities," Research Project RP2722-23, Final Report, Prepared for: Electric Power Research Institute, June 1994.

39. NUREG/CR-0098, N. M Newmark and W. J. Hall, "Development of Criteria for Seismic Review of Selected Nuclear Power Plants," U.S. Nuclear Regulatory Commission, May 1978.

40. EPRI TR-102266, "Pipe Failure Study Update," Electric Power Research Institute, 1993.

41. NUREG/CR-2300, "A Guide to Performing Probabilistic Risk Assessment of Nuclear Power Plants," U.S. Nuclear Regulatory Commission, 1983.

42. RES/OERAB/SO2-01, "Fire Events–Update of U.S. Operating Experience, 1986-1999," commissioned by the Office of Nuclear Regulatory Research, January 2002.

43. NUREG/CR-6928, Eide, S.A., et al. "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Commission Report, February 2007.

44. NUREG-1829, Tregoning, R., et al., "Estimating Loss-of-Coolant Accident (LOCA) Frequencies Through the Elicitation Process," U.S. Nuclear Regulatory Commission Report–Draft Report for Comment, June 2005.

45. NUREG/CR-6365, MacDonald, P.E., et al. "Steam Generator Tube Rupture Failures," U.S. Nuclear Regulatory Commission Report, April 1996.

46. NUREG/CR-6595, Appendix A, Rev 1, "An Approach for Estimating the Frequencies of Various Containment Failure Modes and Bypass Events," U.S. Nuclear Regulatory Commission, 2004.

47. NUREG-1524, "A Reassessment of the Potential for an Alpha-Mode Containment Failure and a Review of the Current Understanding of Broader Fuel Coolant Interaction Issues: Second Steam Explosion Review Work Group Workshop," U.S. Nuclear Regulatory Commission, 1996.

48. Deleted.

49. Deleted.

50. Deleted.

51. Deleted.

52. Deleted.

53. Deleted.

54. EMF-2110(NP)(A), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," Siemens Power Corporation, July 2000.

55. IEC-62340, "Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Requirements to Cope with Common Cause failure (CCF)," Edition 1.0, International Electrotechnical Commission, 12-7-2007.

56. IEC-60880, "Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions," Edition 2.0, International Electrotechnical Commission, 5-9-2006.

57. IEC-61508, "Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems," International Electrotechnical Commission.

58. ANP-10304, Revision 6, "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report," AREVA NP Inc., May 2013.

59. ANP-10290, Revision 1, "Environmental Report Standard Design Certification," AREVA NP Inc., September 2009.

60. DC-COL-ISG-020, "Interim Staff Guidance on Implementation of a Probabilistic Risk Assessment-Based Seismic Margin Analysis for New Reactors."

61. ASME/ANS RA-Sa-2009, "Addenda to ASME/ANS RA-S-2008: Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications."

62. Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of PRA Results for Risk-Informed Activities," Rev 2, March 2009.

63. EPRI, "Seismic Fragility Application Guide," EPRI Report 1002988, Palo Alto.

64. NUREG/CR-6906, "Containment Integrity Research at Sandia National Laboratories," Sandia National Laboratory/U.S. Nuclear Regulatory Commission, March 2006.

**Table 19.1-1—Characterization of U.S. EPR PRA Relative to Supporting Requirements in ASME PRA Standard**
**Sheet 1 of 2**

| Technical Area | U.S. EPR PRA Characteristics |
|---|---|
| Initiating Events Analysis (IE) | Comprehensive, systematic search made for initiating events. Most aspects of the IE analysis meet the supporting requirements of the standards. Elements of the PRA that cannot generally meet the requirements until later stages of design, construction and operation include the following:<br>● Plant-specific operating experience is not available for review, although experience of current plants was considered (IE-A3, IE-A7).<br>● Operators are not yet available to be interviewed (IE-A6).<br>● Initiating event frequencies reflect generic data (IE-C1).<br>● The ability to capture plant-specific information in the assessment of recovery actions is limited (IE-C1b, IE-C9).<br>● Plant-specific operating philosophy and procedures are not available (IE-C12). |
| Accident Sequence Analysis (AS) | Response to the initiating events was first delineated via the use of event sequence diagrams (ESD), and these were used to define core-damage sequences via the construction of event trees. Most aspects of the accident sequence analysis meet the supporting requirements of the standards. Elements of the PRA that cannot generally meet the requirements until later stages of design, construction and operation include the following:<br>● The functions and structure of the accident-sequence models reflect expectations of plant-specific operating practices, based on those of current plants (AS-A5, IE-B5a). |
| Success Criteria (SC) | Success criteria reflect design-specific calculations performed using the MAAP4 and SRELAP5 computer codes. These calculations meet the supporting requirements of the standard. An exception is as follows:<br>● Plant-specific operating philosophy and procedures are not available to confirm the bases for success criteria (SC-A6). |
| Systems Analysis (SY) | The systems analyses were accomplished via the construction of detailed fault trees. These fault trees reflect the design details available. Aspects that do not meet the requirements because of the state of the design include the following:<br>● Since the plant has not yet been constructed, it is not possible to collect information on the as-built, as-operated systems (SY-A2).<br>● Although it is reasonable to infer testing and maintenance practices and system operating procedures from operating plants, these elements do not yet exist (SY-A3, SY-A18, SY-A18a).<br>● Operation staff is not yet available to be interviewed and plant walkdowns cannot be conducted until the plant is constructed (SY-A4).<br>● There is not enough detailed design information to model all systems and equipment (i.e. normal heat sink, I&C PAS and SAS) (SY-A7). |

**Table 19.1-1—Characterization of U.S. EPR PRA Relative to Supporting Requirements in ASME PRA Standard**
**Sheet 2 of 2**

| Technical Area | U.S. EPR PRA Characteristics |
|---|---|
| HRA | HRA necessarily relies on significant plant-specific information that is not yet available. The nature of the human reliability analysis and the areas in which compensatory steps are addressed is summarized in Section 19.1.2.<br>● The lack of plant-specific operating and test and maintenance procedures would require a final confirmation of human actions evaluation (HR-A1, HR-A2, HR-A3, HR-C3, HR-E1, HR-E2, HR-E3, HR-F2, HR-H2). |
| Data Analysis (DA) | Parameter estimates necessarily reflect generic data. These data were obtained from the most relevant sources available. Specific requirements for which the data analysis does not meet the requirements include the following:<br>● The lack of plant-specific operating experience precludes the development and use of a plant-specific database or of specialization of generic data based on plant experience via Bayesian analysis (DA-B2, DA-C2 through DA-C13). |
| Internal Flooding (IF) | Some aspects of the internal flooding analysis are limited by the lack of plant-specific details. Specific areas in which the internal flooding analysis does not meet the requirements include the following:<br>● Plant information reflecting as-built, as-operated conditions does not yet exist (IF-A3).<br>● Walkdowns cannot be conducted until the plant is constructed (IF-A4, IF-B3a, IE-C9, IE-E8). |
| Quantification (QU) | The quantification was performed by solving the overall core-damage model using the linked fault-tree approach. The quantification satisfies the supporting requirements of the standard. |
| LERF (LE) | A detailed assessment of containment response and release frequency has been conducted. The assessment satisfies the supporting requirements of the standard, except for such aspects as system failure analysis and human reliability analysis, as addressed for technical areas SY, HF and DA above (LE-D5, LE-E1). |
| PRA Configuration Control (MU) | The PRA configuration control satisfies the supporting requirements of the standards, except for such aspects as monitoring of changes in operation and maintenance (MU-A1). |

**Table 19.1-2—Features for U.S. EPR that Address Challenges for Current PWRs**
**Sheet 1 of 6**

| Risk-Important Challenges for Current-Generation PWRs | U.S. EPR Features |
|---|---|
| **Features Relating to Potential for Core Damage** | |
| SBO<br>● Frequency of losses of offsite power<br>● Reliability of onsite emergency power<br>● Limited life for station batteries<br>● Potential for leakage from RCP seals | Reduction in potential for LOOP:<br>● Normal alignment of auxiliary power to switchyard (no need for fast transfer after reactor trip).<br>● Multiple auxiliary transformers for both safety-related and non-safety-related switchgear.<br>● Capability of turbine-generator runback to house loads on full-load rejection.<br>Redundancy and diversity of onsite emergency power sources.<br>● Four emergency diesel-generators.<br>● Two SBO diesel-generators, diverse from emergency diesel-generators.<br>● Careful design of cross-ties: cross-ties available for selected loads important to PRA. |
| Response to LOCAs<br>● Manual action to switch to sump recirculation<br>● Reliability of SISs<br>● Need for low-pressure pumps to supply suction to high-pressure pumps during sump recirculation following SLOCA<br>● Ability to depressurize RCS via aggressive cooldown to allow use of low pressure injection, given failure of high pressure injection | Enhanced reliability of safety injection in response to LOCAs:<br>● IRWST eliminates need for switchover for sump recirculation.<br>● Low-pressure pumps not required to support MHSI suction in long term.<br>● Four trains of each SIS (MHSI, LHSI, and accumulators).<br>Availability of alternative means for cooling:<br>● Four trains of emergency feedwater (EFW), each feeding a SG, with four-train redundancy for forced cooldown.<br>● Automatic partial cooldown (PCD) through the SG MSRTs used for depressurization of RCS and enabling MHSI for events involving high RCS pressure. Manual capability to perform fast cooldown (FCD) using MSRTs to enable LHSI should MHSI fail or become unavailable.<br>● Three PSVs or two dedicated depressurization valve trains available for depressurization of RCS if needed. |

**Table 19.1-2—Features for U.S. EPR that Address Challenges for Current PWRs**
**Sheet 2 of 6**

| Risk-Important Challenges for Current-Generation PWRs | U.S. EPR Features |
|---|---|
| Potential for RCP seal failure<br>● Reliance on CCW and service water for seal cooling and seal injection<br>● Operator action to trip RCPs to reduce potential for seal failure<br>● Materials used in seal construction | Enhanced capabilities to maintain RCP seal integrity:<br>● Four-train redundancy for cooling water systems, reducing likelihood of loss of thermal barrier cooling.<br>● Stand still seal system that serves as backup mechanical seal, reducing potential for seal LOCA-type events<br>● Automatic tripping of RCPs given total loss of seal cooling (thermal barrier cooling and seal injection) |
| Transients with total loss of heat removal<br>● Reliability of auxiliary feedwater systems<br>● Availability of means to depressurize reactor for feed-and-bleed cooling<br>● Reliability of operator action to initiate feed-and-bleed cooling | Improved systems for secondary heat removal<br>● Four-train redundancy for Emergency Feedwater<br>● Separate (non-safety-related) startup and shutdown feedwater system<br>Enhanced ability to achieve feed-and-bleed cooling<br>● Two different means for establishing bleed paths: three PSVs or two dedicated depressurization valve trains<br>● Four-train redundancy for injection via MHSI<br>● Larger pressurizer and greater inventory in SGs provides increased time for operator response<br>● IRWST eliminates need for switch to sump recirculation |

**Table 19.1-2—Features for U.S. EPR that Address Challenges for Current PWRs**
**Sheet 3 of 6**

| Risk-Important Challenges for Current-Generation PWRs | U.S. EPR Features |
|---|---|
| SGTR<br>● Potential for loss of RCS inventory and development of pathway to atmosphere due to stuck-open main steam safety/relief valve<br>● Availability of means to cool down RCS to limit loss through broken tube<br>● Ability to make up to refueling water storage tank for long term inventory control | Enhanced ability to avoid challenging main steam safety valves (MSSVs)<br>● Four-train redundancy for emergency feedwater<br>● Automatic isolation of all feedwater to faulted generator<br>● Enhanced ability to perform partial cooldown of RCS via MSRTs<br>Improved reliability and choices for achieving safety injection<br>● Four-train redundancy for MHSI and LHSI<br>● Enhanced ability to depressurize RCS via PSVs or dedicated depressurization valve trains<br>● MHSI pumps shutoff head is below the setpoints for the MSSVs (reduces the potential for causing a stuck open secondary relief on the ruptured SG). |
| Potential for internal flooding<br>● Risk-Significant equipment susceptible to flooding from turbine building<br>● Limited separation and physical barriers between divisions of safety systems | Substantially improved protection against internal floods<br>● All safety trains located in separate buildings, without communication between buildings<br>● Four-train redundancy, so that even if all equipment in one division were lost, reliable response would remain available. Systems and system dependencies are discussed in Section 19.1.4.1.1.3 |

**Table 19.1-2—Features for U.S. EPR that Address Challenges for Current PWRs**
**Sheet 4 of 6**

| Risk-Important Challenges for Current-Generation PWRs | U.S. EPR Features |
|---|---|
| Potential for internal fire<br>• Limited separation and fire barriers between divisions<br>• Limited options for response to fire in MCR<br>• Common location of essential cables and controls (e.g., in cable-spreading room)<br>• Potential for spurious operations induced by fires affecting control cables<br>• Large combustible loading associated with the lube oil RCP fires in the containment | Substantially improved protection against internal fires<br>• All safety trains located in separate buildings, without communication between buildings<br>• Four-train redundancy, so that even if all equipment in one division were lost, reliable response would remain available. Systems and system dependencies are discussed in Section 19.1.4.1.1.3<br>• Enhanced capability for action via remote shutdown panel in the event of MCR evacuation<br>• Separation and fire barriers between divisions of control and power cables<br>• Use of fiber optic cables eliminates potential for effects of "hot shorts" in these cables<br>• Minimized possibility of a fire induced LOCA: a spurious opening of PSVs or dedicated depressurization valve trains would require "hot shorts" in multiple separated divisions<br>• State-of-the art oil collection system, one for each RCP pump, minimizes possibilities for the large RCP lube oil fire |
| Impact of seismic events<br>• Inadequate anchorage, especially for electrical cabinets, batteries, and other equipment<br>• Effects of relay chatter<br>• Unreinforced masonry block walls<br>• Flooding due to failures of non-safety systems (e.g., condenser circulating water)<br>• Building interactions | Substantially improved protection against earthquakes<br>• Location of all safety systems within qualified structures<br>• Elimination of unreinforced masonry block walls as fire barriers<br>• Use of digital systems for instrument and control functions, this eliminates or reduces the electro-mechanical relays<br>• Elimination of potential for flooding of safety equipment due to failures in non-safety systems<br>• Careful attention to potential interactions between buildings |

**Table 19.1-2—Features for U.S. EPR that Address Challenges for Current PWRs**
**Sheet 5 of 6**

| Risk-Important Challenges for Current-Generation PWRs | U.S. EPR Features |
|---|---|
| **Features Relating to Containment Response and Release Potential** | |
| Phenomena associated with high-pressure melt ejection<br>● Accidents proceeding to core damage at high RCS pressure<br>● Geometries of reactor cavities conducive to transport of core debris to containment atmosphere<br>● Potential for direct impingement of core debris on side wall of containment | Reduced potential for high-pressure melt ejection<br>● Enhanced capability for partial depressurization to prevent core damage<br>● Depressurization via dedicated depressurization valve trains available after onset of core damage to achieve low RCS pressure<br>Limited potential for impact by high-pressure melt ejection<br>● Cavity design to direct core debris to core melt spreading area<br>● Limited pathways for dispersion to upper areas of containment<br>● Large, robust containment capable of accommodating significant loadings |
| Possibility of early failure due to hydrogen burns and rapid steam generation<br>● Accumulation of hydrogen in containment atmosphere before and immediately after vessel breach<br>● Blowdown prior to vessel failure<br>● Rapid steam generation due to interaction of core debris with water in reactor cavity | Enhanced ability to withstand early containment loadings<br>● Large, robust containment capable of accommodating significant loadings<br>● Availability of catalytic recombiners to prevent accumulation of hydrogen<br>● Cavity design that limits potential for energetic interaction of core melt and water |
| Potential for accidents that bypass containment<br>● Interfacing-systems LOCAs due to exposure of low-pressure piping to RCS pressure<br>● Significant contribution from SGTRs | Reduced potential for core damage due to bypass events<br>● LHSI system designed to maintain integrity even when exposed to full RCS pressure<br>● Reduced potential for core damage due to SGTRs, as described above |

**Table 19.1-2—Features for U.S. EPR that Address Challenges for Current PWRs**
**Sheet 6 of 6**

| Risk-Important Challenges for Current-Generation PWRs | U.S. EPR Features |
|---|---|
| Potential for late failure of containment<br>● Long term overpressurization due to lack of containment heat removal<br>● Potential for generation of combustible and non-condensable gases due to interactions of core-debris with containment basemat<br>● Potential for de-inerting containment upon recovery of containment sprays, creating environment for large hydrogen burn | Enhanced protection against long term challenges to containment integrity<br>● Containment heat removal via four-train LHSI system, with SAHRS as long term, non-safety backup<br>● Provisions for active cooling of core debris to prevent molten core concrete interactions<br>● Availability of catalytic hydrogen recombiners<br>● Limited reliance on containment spray, for removal of fission products only |

**Table 19.1-3—Example Review of Initiating Events for Applicability to U.S. EPR**
**Sheet 1 of 2**

| Initiating Events from NUREG/CR-5750 | Treatment in PRA for U.S. EPR |
|---|---|
| **Loss-of-Coolant Accidents** | |
| Large pipe break LOCA | Included explicitly (LLOCA) |
| Medium pipe break LOCA | Included explicitly (MLOCA) |
| Small pipe break LOCA | Included explicitly (SLOCA) |
| Very small LOCA/leak | Not modeled; assumed that normal charging will maintain RCS inventory |
| Stuck-open pressurizer power-operated relief valve | Not relevant for U.S. EPR |
| Stuck-open pressurizer safety/relief valve (one valve) | Design makes challenges to safety/relief valves very unlikely; premature opening included as contributor to SLOCA |
| Stuck-open pressurizer safety/relief valves (two valves) | Not modeled; low challenge rate due to design coupled with small probability of two valves failing open |
| RCP seal LOCA | Seal LOCAs due to spontaneous failures are implicitly included with SLOCA; seal failures as a consequence of loss of seal cooling are modeled explicitly |
| SGTR | Included explicitly (SGTR) |
| **Transients** | |
| Loss of offsite power | Included explicitly (LOOP) |
| Total loss of condenser heat sink | Included in loss of main condenser (LOC) |
| Inadvertent closure of all MSIVs | Included in loss of main condenser (LOC) |
| Loss of condenser vacuum | Included in loss of main condenser (LOC) |
| Turbine bypass unavailable | Included in loss of main condenser (LOC) |
| Total loss of feedwater | Included explicitly (LOMFW) |
| Other transients | Included explicitly under general reactor trip (GT) |
| **High-Energy Line Breaks or Leaks (Combined)** | |
| Steam-line break or leak outside containment | Included explicitly (SLBO) |
| Steam-line break or leak inside containment | Included explicitly (SLBI) |
| Feedwater line break or leak | Included implicitly in SLBI |
| Stuck open MSSVs | Included explicitly (MSSV) |
| Support-System Initiators | |
| Loss of vital medium-voltage AC bus | Included explicitly (31BDA) |

**Table 19.1-3—Example Review of Initiating Events for Applicability to U.S. EPR**
**Sheet 2 of 2**

| Initiating Events from NUREG/CR-5750 | Treatment in PRA for U.S. EPR |
|---|---|
| **Support System Initiators** | |
| Loss of vital low-voltage AC bus | Included implicitly in 31BDA |
| Loss of vital DC bus | Not modeled; loss of one DC division would not result in an initiator |
| Total loss of service water or component cooling | Included explicitly via a specific event representing a loss of service water or CCW |
| Partial loss of service water or component cooling | Included explicitly via a specific events representing a loss of service water or CCW |
| Loss of UHS | UHS system failures that result in inadequate cooling to the UHS are assumed to fail the associated ESW train, and these failure modes are included in the loss of ESW/CCW initiating event |
| Loss of instrument air | Not modeled; there are no significant air-operated valves or other components in U.S. EPR design |

**Table 19.1-4—Summary of Initiating Events for the U.S. EPR PRA**
**Sheet 1 of 3**

| Event | Mean Frequency (/yr) | Distribution Type (Parameters) | Source for Frequency |
|---|---|---|---|
| **Plant Transients** | | | |
| GT—general transient, including turbine or reactor trip that does not involve failure of systems that could be needed for core heat removal. | 7.5E-01 | Gamma (17.8) | NUREG/CR-6928 (Reference 19) |
| LOC—loss of main condenser, including MSIV closure, loss of condenser circulating water, etc. | 8.1E-02 | Gamma (20) | NUREG/CR-6928 |
| LOMFW—total loss of main feedwater | 9.6E-02 | Gamma (1.33) | NUREG/CR-6928 |
| **Loss-of-Coolant Accidents (LOCA)** | | | |
| SLOCA—small LOCA (0.6 to 3-in equivalent diameter) | 1.4E-03 | Gamma (1.4) | NUREG/CR-6928 and NUREG-1829,with addition of frequency for failure of the PSVs to reseat (2E-04/yr) |
| MLOCA—medium LOCA (3 to 6-in equivalent diameter) | 1.4E-05 | Gamma (0.5) | NUREG-1829 (Reference 44) |
| LLOCA—large LOCA (>6-in equivalent diameter) | 1.3E-06 | Gamma (0.42) | NUREG/CR-6928 |
| **SGTR** | | | |
| SGTR | 3.5E-03 | Gamma (0.5) | NUREG/CR-6928 |
| IND SGTR—SGTR induced by a steam line break | 1.2E-06 | Gamma (0.5) | Calculated based on methodology from NUREG/CR-6365 (Reference 45) |
| **Interfacing Systems LOCAs** | | | |
| ISL-CCW RCPTB—ISLOCA, with leakage to CCW due to failure of the thermal barrier cooling coils for RCP seal cooling | 3.8E-10 | Integrated (SOKC parameters included in the post-processing) | Fault-tree analysis |

**Table 19.1-4—Summary of Initiating Events for the U.S. EPR PRA**
**Sheet 2 of 3**

| Event | Mean Frequency (/yr) | Distribution Type (Parameters) | Source for Frequency |
|---|---|---|---|
| ISL-CVCS HPTR—ISLOCA due to rupture of tube in high pressure letdown cooler | 8.0E-9 | Integrated (SOKC parameters included in the post-processing) | Fault-tree analysis |
| ISL-CVCS REDS—ISLOCA due to spurious opening of reducing station | 4.3E-10 | Integrated (SOKC parameters included in the post-processing) | Fault-tree analysis |
| ISL-CVCS INJ—ISLOCA due to break in charging line | 5.7E-12 | Integrated (SOKC parameters included in the post-processing) | Fault-tree analysis |
| ISL-SIS LHSI—ISLOCA in injection line from LHSI | 8.4E-12 | Integrated (SOKC parameters included in the post-processing) | Fault-tree analysis |
| ISL-SIS MHSI—ISLOCA in injection line from MHSI | 9.8E-11 | Integrated (SOKC parameters included in the post-processing) | Fault-tree analysis |
| ISL-SIS RHR—ISLOCA in RHR suction line | 9.7E-11 | Integrated (SOKC parameters included in the post-processing) | Fault-tree analysis |
| **Secondary Side Breaks** | | | |
| SLBO—steam-line break outside containment (downstream from MSIV) | 2.1E-03 | Gamma (1.5) | NUREG/CR 5750 (excluding leaks) (Reference 13) |

**Table 19.1-4—Summary of Initiating Events for the U.S. EPR PRA**
**Sheet 3 of 3**

| Event | Mean Frequency (/yr) | Distribution Type (Parameters) | Source for Frequency |
|---|---|---|---|
| SLBI—steam-line break inside containment | 1.0E-03 | Gamma (0.5) | NUREG/CR 5750 |
| MSSV—spurious opening of main steam safety valve | 1.0E-03 | Gamma (0.5) | Frequency for SLBI applied |
| **Support System Failures** | | | |
| LOOP—loss of offsite power | 1.9E-02 | Gamma (0.84) | NUREG/CR-6890 (Reference 21) |
| LOCCW-Loss of Component Cooling water Common Headers | 2.5E-1 | Integrated | Fault-tree analysis |
| LBOP—loss of closed cooling water or auxiliary cooling water, resulting in a loss of balance-of-plant | 5.0E-02 | Integrated | Fault-tree analysis |
| 31BDA—loss of one division of emergency AC power (6.9 kV switchgear 31BDA) | 3.5E-02 | Integrated | Fault-tree analysis |

**Table 19.1-5—Systems Analyzed in U.S. EPR PRA**
**Sheet 1 of 4**

| System | Comment |
|---|---|
| **Systems Providing Control of RCS Inventory** | |
| Medium-head safety injection (MHSI) | • Four independent trains, physically separated in different SB<br>• Inventory control for LOCAs, SGTR, and feed-and-bleed cooling |
| Low-head safety injection (LHSI) | • Four independent trains, physically separated in different SB<br>• Inventory control for LLOCA; backup to MHSI for small and MLOCAs, given fast-cooldown of RCS<br>• Cooling of IRWST inventory via RHR heat exchangers<br>• Cross-connections enhance availability during maintenance without sacrificing independence |
| Accumulators | • Four separate accumulators (one for each RCS cold leg)<br>• Reflooding of core following LLOCA; additional inventory control for small and medium LOCAs |
| IRWST | • Single tank, integral to the containment structure<br>• Suction source for CVCS, MHSI,LHSI and SAHR<br>• Collects discharge from RCS (e.g., during LOCA), preventing need for change in mode for SISs<br>• Three levels of filters are provided in order to retain debris that could originate from a LOCA and clog the SIS suctions |
| EBS | • Two-train system capable of injecting highly borated water into RCS<br>• Manual backup to reactor shutdown systems |
| Chemical and volume control system (CVCS) | • Two-train, non-safety system<br>• Inventory control for RCS leaks, avoiding challenges to safety systems |
| Stand still seal system for RCPs | • Pneumatic seal, backup to normal multi-stage seals<br>• Deployed when RCPs trip on a loss of seal cooling |
| **Systems Providing Heat Removal** | |
| Main feedwater system (MFWS) | • Four trains with motor-driven pumps; three normally in service during power operation<br>• Continued secondary heat removal following reactor trip |
| Startup and shutdown system | • Single motor-driven pump<br>• Backup secondary heat removal |

**Table 19.1-5—Systems Analyzed in U.S. EPR PRA**
**Sheet 2 of 4**

| System | Comment |
|---|---|
| Emergency feedwater system (EFWS) | • Four independent trains, each with a motor-driven pump and dedicated tank to provide suction, located in physically separate SB<br>• Cross-connections for pumps permit any train to draw suction from any tank, and discharge to any SG<br>• Safety-related means for secondary heat removal when MFWS and SSS are unavailable |
| Main steam system (MSS) | • One MSRT and two MSSVs on each main steam line<br>• Path from any SG to any relief valve provides heat removal if MSIVs are open<br>• PCD and FCD accomplished via MSRTs.<br>• Isolation following SGTR or secondary line break via closing of MSIV |
| Pressurizer relief system | • Three PSVs with both spring-actuated and electrically operated pilot valves, and two SADVs which are MOVs<br>• Overpressure protection for RCS, and relief path for feed-and-bleed cooling |
| SAHRS | • Single-train system, with heat sink via dedicated trains of CCW and ESW<br>• SAHR takes suction from IRWST<br>• The SAHR discharge depends on the primary operating modes, which could be one of the following:<br>• backup to LHSI for cooling of IRSWT<br>• passive cooling of molten core debris.<br>• active spray for environmental control of the containment atmosphere.<br>• active recirculation cooling of the molten core debris.<br>• active recirculation cooling of the containment atmosphere.<br>• active back-flush of IRWST strainers. |

**Table 19.1-5—Systems Analyzed in U.S. EPR PRA**
**Sheet 3 of 4**

| System | Comment |
|---|---|
| **Support Systems** | |
| AC electric power systems | • Four independent safety divisions of electrical distribution, each housed within separate SB, supplied normally with offsite power from two auxiliary transformers<br>• Four non-safety trains of electrical distribution, supplied normally with offsite power from two auxiliary transformers<br>• Four emergency diesel-generators in two separate diesel buildings<br>• Two SBO diesel generators separated from and of diverse design with respect to the emergency diesel-generators<br>• Continued supply of offsite power to plant auxiliaries following reactor trip, without need for fast transfer<br>• Capability for runback and supply to house loads from main generator in the event of a load rejection |
| DC electric power systems | • Four independent safety divisions, each housed within separate SB, and each with its own battery (two-hour design capacity)<br>• Two trains for support of severe-accident functions, with batteries rated for 12-hr discharge |
| CCWS | • Four independent divisions, each housed within separate SB<br>• Provide thermal barrier cooling and motor cooling for the RCPs, cooling for the charging pumps, and Safety Chill Water units in Trains 2 and 3.<br>• Dedicated train loads include the MHSI pumps, the RHR/LHSI heat exchangers in all four trains, and the LHSI pumps in trains 2 and 3. |
| ESWS and UHS | • Four independent divisions, each housed within separate SB<br>• Cooling for CCWS and the EDGs, with UHS cooling provided by mechanical draft cooling towers (site-specific design for UHS may differ) |
| Safeguard buildings ventilation system | • Four independent divisions, one for each SB<br>• Two non-safety divisions, serve as backups to the safety divisions for maintenance purposes |

**Table 19.1-5—Systems Analyzed in U.S. EPR PRA**
**Sheet 4 of 4**

| System | Comment |
|---|---|
| Safety chilled water system | • Four divisions, each housed within separate SB<br>• Provides cooling to the SB HVAC, that includes cooling to ac and dc switchgear rooms and EFW pump rooms.<br>• Trains 1 and 4 of Safety Chilled Water are air-cooled whereas trains 2 and 3 are cooled by the CCW common headers.<br>• One Chiller has a capacity to cool two safeguard buildings: Train 1 or 2 safety chiller cools SB1 and SB2, Train 3 or 4 safety chiller cools SB3 and SB4.<br>• Trains 1 and 4 provide direct cooling to the LHSI pumps, such that these pumps are supported during a loss of CCW or ESW |
| Instrumentation & control systems | • Digital I&C systems for different functions (RPS, ESFAS, actuation and control of other safety and non-safety systems) |

Next File