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 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 in which 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 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 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. However, some design change features have not been specifically included in the PRA model. Refer to Section 19.1.2.4 for information on design changes.

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 3, Reference 4, and Reference 5). The ASME PRA Standard presents high-level requirements and, for each of these, a set of more detailed supporting requirements. The supporting requirements are related to the three capability categories addressed 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 summary of the degree to which the U.S. EPR PRA relates to the capability categories for the nine technical elements addressed in the PRA Standard.

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 or before fuel load.

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.

The ASME PRA Standard does not address external events, low power shutdown or internal fire events. For these types of analyses where the ASME PRA Standard does not apply, AREVA NP has employed the latest NRC guidance available to perform assessments commensurate with the uses of the PRA. This additional guidance includes the following:

- Internal fire analysis. NRC has not yet endorsed a fire-PRA standard. The internal fire analysis for the U.S. EPR PRA employs 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 addressed below and in Section 19.1.5.2.

- Low power and shutdown (LPSD) analysis. The ASME PRA Standard 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.

- PRA-based seismic margins assessment. The U.S. EPR PRA employs a margins approach to evaluate potential vulnerabilities to seismic events. Neither the margins approach, nor the method for conducting a seismic PRA is addressed by standards endorsed by the NRC. The approach as implemented for the U.S. is consistent with guidance in SECY-93-087 (Reference 2) and follows the general approach delineated in Appendix B of ANSI/ANS-58.21-2003, standard for external events (Reference 7).

- 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 NUREG-1407 (Reference 8) and in Reference 7.

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 are 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. 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 the iterative nature of the interface between design and PRA, it is not always possible to incorporate all differences identified between the plant design change features and the PRA model in a timely manner. A summary of plant design changes planned for future revision to the PRA model is provided below. As discussed below, these design change features have been assessed qualitatively for impact on the PRA model. Based on the qualitative assessment, these design features do not have a significant impact on the PRA results and conclusions.

1. Modification of manual actuation of safety systems – This change will remove the direct safety information and control system (SICS) to priority and actuator control system (PACS) system-level manual actuations and will route the system level manual actuation signals through the Protection System (PS). Component-level actuations will be provided via process automation system/diverse actuation system (PAS/DAS). PRA impact - Requires modeling of PS dependence with the appropriate human actions. Since the design provides multiple means for performing key operator actions, the impact upon human reliability analysis (HRA) results is minor. In the unlikely event of PS failure, some of the operator actions may require a longer time to perform via the component level controls than is currently assumed in the PRA. However, these moderately affected human error probabilities (HEP) will be offset by the probability of a PS failure. Therefore, this design change feature is judged to have no significant impact on the PRA results and conclusions.

2. Protection system functional requirements – This change will duplicate high reactor coolant system (RCS) pressure and high steam generator (SG) pressure trips in both the A and B subsystems of the PS. PRA impact – Revise the common-cause failure (CCF) model in the PS fault trees to account for the functional dependence. This change neither helps nor hurts the PRA results, because the CCF model does not distinguish between four channels of the same parameter and eight channels of the same parameter. This is because software CCF is assumed to affect all identical channels, and the Risk Spectrum® implementation of the Multiple Greek Letter (MGL) method used for hardware CCF ignores any redundancy over four channels. This design change does not impact the functional diversity that is provided by other trip parameters. Therefore, this design feature is judged to have no significant impact on the PRA results and conclusions.

3. Steam generator tube rupture (SGTR) mitigation response – There are two aspects to this change. The first part of the change will remove automatic partial cooldown (PCD) initiation on high SG level (and subsequent automatic isolation of the chemical and volume control system (CVCS) on high SG level and PCD finished); therefore, for an SGTR, automatic PCD will occur with SIS actuation on low RCS pressure. The second part of the change is to the timing associated with isolation of the affected SG and main steam relief train (MSRT) reset (on high SG level or high SG activity), which will be changed to coincide with PCD initiation rather than waiting for PCD to finish.

The PRA credits operator action for SGTR mitigation (reactor trip, isolation of affected SG, and cooldown) because it may take a relatively long time to reach the automatic setpoints on either high SG level or low RCS pressure. The PRA credits the automatic SGTR response as a backup; that does not change because the analyses show that the low RCS pressure setpoint will be actuated eventually, even if CVCS is running. Furthermore, analyses of a double-ended break of a single tube indicate that the setpoint for initiation of PCD with SIS actuation (on low RCS pressure) is reached before the setpoint for high SG level; therefore, elimination of the PCD signal on high SG level does not have a significant effect on the PRA.

Early isolation of the affected SG and RCS cooldown helps reduce reactor coolant loss by reducing the pressure differential between the impacted SG and the RCS. Early isolation also minimizes secondary side contamination, and reduces offsite releases during cooldown. Because the U.S. EPR has abundant SG cooling capacity with the three unaffected SGs, isolation of the impacted SG should not have any significant impact on RCS depressurization. Based on the above, this design change feature is judged to have no significant impact on the PRA results and conclusions.

4. Emergency feedwater (EFW) flow control via safety automation system (SAS) – EFW is initiated via the PS, but EFW flow control will be performed by SAS. PRA impact – Assess EFW dependence on SAS. The EFW design includes a flow control valve in each train (separate from the level control valve); this valve is normally partially closed to protect against overfeed in the case of a steam line break. In order to achieve the full credited EFW flow, the flow control valve must open, which is not currently included in the model. Not accounting for this feature in the model has a minor impact on the PRA because the probability of independent failure (or CCF) of the flow control valves or their signals, is small relative to the probability of independent failure (or CCF) of the EFW pumps– about an order of magnitude less. Therefore, this design feature is judged to have no significant impact on the PRA results and conclusions.

5. Station blackout (SBO) Division 2/3 electrical power –The alternate feed power supply connection from Division 1 to Division 2 and from Division 4 to Division 3 was changed. The currently modeled alternate feed connection from Division 1 to Division 2 is from bus 31BDC to bus 32BDB. The currently modeled alternate feed connection from Division 4 to Division 3 is from bus 34BDC to bus 33BDB. The new arrangement will have the alternate feed connection from bus 31BDA to bus 32BDB and from 34BDA to 33BDB.

   This change establishes a direct connection from the SBO BBH buses to Divisions 2 and 3. Therefore the alternate feed is not required to come from an SBO-backed bus because the alternate alignment will only be used during emergency diesel generator (EDG) or bus maintenance in the emergency power supply system (EPSS) divisions and not used during SBO operations.

   The PRA model credits the alternate feed from Division 1 to Division 2 and from Division 4 to Division 3 in SBO conditions and in non-SBO conditions. This

change does not modify the availability of those functions or the context in which they will be performed, but modifies the way that they will be executed.

The failure probability of those functions, as modeled in the PRA, is dominated by human errors. Those human errors were assigned HEP values judged to be conservative for this alternate feed configuration. Therefore, this design change is judged not to have a significant impact on the current conclusions of the PRA.

6. Component cooling water (CCW) common header cooling to reactor coolant pump (RCP) thermal barriers – This design change consists of having one CCW common header cooling all four RCP thermal barriers, instead of each common header cooling two RCP thermal barriers. In case of a loss of cooling from one header, a manual switchover to the second header can be performed. This change has been quantitatively evaluated and results in a small decrease in seal LOCA contribution to internal event CDF. A larger decrease in internal fire and flood event CDF can be attributed to the conservative treatment of these events, which is likely to change as a result of more realistic fire and flood PRA updates. Overall, this design change is judged not to have a significant impact on the current conclusions of the PRA.

7. EFWS supply header isolation valves – This design change consists of maintaining the EFWS supply header isolation valves closed. If one or more EFW train is unavailable, a manual action is required to interconnect the four tanks so that the entire EFW inventory is available. In case of a pipe break or a tank leakage in the EFWS (internal flooding), the operators no longer have to isolate the leaking train to avoid losing all EFW inventory. One tank inventory still may be lost; therefore, it is necessary to refill one of the intact tanks in order to achieve the 24-hour mission time.

   This change results in a measurable increase in internal event and internal flooding CDF, driven by operator failure to perform the interconnection. PRA insights and assumptions regarding manual isolation of an EFWS pressure boundary failure are also affected, as this isolation is no longer needed. This effect is recognized in Table 19.1-108, Item 10, and Table 19.1-109, Item 66.

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 as-designed, as-to-be-built, and as-to-be-operated conditions. When reviewing pending design changes and proposed model improvements, the impact on the CDF and LRF are estimated. Based on the estimated impact, one of the following update approaches will be taken:

- If the effect of the change(s) since the last PRA model update are such that the PRA no longer reasonably reflects as-designed, as-to-be-built, and as-to-be-operated conditions, then a PRA model update is implemented without waiting for the routine update cycle. The reasonableness determination is summarized as follows:

  – If the cumulative risk impact of the change(s) is more than 10 percent (either positive or negative) of the total CDF or LRF, then the PRA insights are assessed to see if they remain valid.

  – If the PRA insights are no longer valid, then the PRA is updated without waiting for the next routine update cycle.

- If cumulative risk impact of the change(s) is judged not to invalidate the PRA insights, then the PRA model will be revised at the next scheduled update.

- A PRA model update may also be implemented without waiting for the next routine update cycle based on consideration of several change attributes, including the level of complexity of the change and the ability to manage/control potential cumulative modeling impacts.

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 frequency of core damage and low frequency of large release 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 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 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 three 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 fully computerized control room also 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 so as 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 maintains the integrity of the containment by providing the ability to passively stabilize/cool molten core debris. A passive device 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 means 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) were permanently aligned to the safety chilled water system (SCWS). The original configuration entailed cooling of all four pumps by the component cooling water system (CCWS), with chilled water available as backup cooling to pumps 1 and 4. This change added diversity in the motor cooling and eliminated the need for manual alignment of backup cooling. Since Divisions 1 and 4 of the chilled water system are air cooled, the diversity extends to the heat sink used for cooling. The change in configuration also eliminates the potential that common cause failure (CCF) of the three-way valves supplying cooling water could affect two of the LHSI pumps.

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 emergency service water (ESW).

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.

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 are 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 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 check valve are unisolable (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 check 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. Partial losses of the CCW system are

also considered as initiators, resulting in several loss of CCW\ESW initiating events. Loss of an Ultimate Heat Sink (UHS) is also included in these events.

- 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 auxiliary cooling water system. Complete loss of the CCW 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, it also 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 (rough estimates of the recovery times are used).

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. 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 (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 MAAP 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 by opening the PSVs. The following systems can provide inventory make-up to the reactor vessel: MHSI, LHSI, Accumulators, CVCS and EBS. 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, operators 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 CVCS or 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 design 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 2005 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 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 three 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 open motor-operated valves (MOV) and the EFW pump discharge lines are interconnected via normally closed MOVs so that any EFW train can be connected to any SG or suction tank. Therefore, a suction tank leakage is considered in the PRA model as a common EFW failure. In many accidents, inventory of all four EFW tanks may be needed to cool the plant during a mission time of 24 hours. EFW discharge to the SGs is independent of the MFW and 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 severe accident depressurization lines. The severe accident depressurization lines consist of two parallel trains, each line having two SADV 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 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. U.S. EPR 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 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 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 reactor trip function of 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, will provide additional reliability and diversity for ESF functions that is not included in the current PRA model 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 10 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 39 units at 24 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 92 million operating hours of accumulated experience through calendar year 2008. During this time, there were some random failures of the computer processor modules, and no OS failures. A Chi-squared distribution with 95% confidence level was used to provide an upper bound OS failure rate (which at the time of analysis was based on experience through 2006). 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 qualified to a rigorous SIL, which is SIL-4. 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 conservative 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.

However, the PRA does not include credit for diverse automatic or manual actuations that may be required for D3, other than diverse reactor trip (for the ATWS rule). The D3 functions are backup automatic and manual actuations that are intended to mitigate SWCCF. In order to conservatively compensate for the effect of the D3 functions that have not been incorporated into the PRA, a recovery probability of 0.5 was applied to the application software CCF probability. When fully incorporated, the D3 functions will 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 EPR 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.

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 will be tempered somewhat by additional functions, which are incorporated into the DAS for D3, and are not credited in the design certification PRA.

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:

- 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 2.
- Cooling for charging pump Train 1.
- 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:

- Pump motor cooling and thermal barrier cooling for seals 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.
- Cooling for charging pump Train 4.
- 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. 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 complete 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 after about two hours (if compensatory manual actions are not implemented).
- Failure of the running CCW pump and failure of switchover for the associated CCW CH, if the loss of HVAC is in a division with an initially running CCW train (the base PRA model assumes that CCW Pumps 1 and 4 are initially running). As it is modeled, the CCW CH switchover dependent on HVAC for the Division 1 SAS instrumentation and logic.

Based on the above, a complete loss of HVAC to SB 1 has a significant impact on the plant response in the U.S. EPR PRA model:

- Results in a complete loss of the AC and DC buses in Division 1.
- Results in a loss of CCW flow to RCPs 1 and 2 (thermal barrier cooling and motor cooling).
- Results in a loss of charging pump Train 1.
- Results in a loss of cooling to the SCWS chiller (QKA20) in Train 2, and loss of HVAC to SB 2, and therefore, a potential loss of the AC, DC buses and EFW in Division 2.

Similarly, a complete loss of HVAC to SB 4 has significant consequences in the PRA model:

- Results in a complete loss of the AC and DC buses in Division 4.
- Results in a loss of CCW flow to RCPs 3 and 4 (thermal barrier cooling and motor cooling).
- Results in a loss of charging pump Train 2.
- Results in a loss of cooling to the SCWS chiller (QKA30) in Train 3, and loss of HVAC to SB 3, and therefore, a potential 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, result in a loss of two electrical divisions, if not recovered.

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.

Severe Accident 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 whose annual frequencies were calculated using fault trees, the point estimates (not mean values) were used as inputs in the CDF quantification. However, mean values were used in the uncertainty evaluation.

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 were not evaluated for the U.S. EPR because there is not yet sufficient detail regarding design or calibration practices to permit a meaningful assessment.

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 (DBA) 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 (EOP). 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 PSFs for procedures, 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:

- Nearly 4000 basic events (not including CCFs).
- Nearly 1500 fault trees
- Nearly 4800 fault tree gates.
- Nearly 200 CCF groups.
- Over 4800 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, all events, resulted in over 73,000 cutsets. The first 100 cutsets represented close to 50 percent of the total CDF; 95 percent of the CDF was represented by over 20,000 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® Professional software package. RiskSpectrum® is a product of Relcon 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. 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 Relcon AB is used to validate correct installation and operation of the code. RiskSpectrum® currently has more than 1000 users in 362 organizations in 41 countries. Worldwide, about 40 percent of the PRAs for nuclear power plants use RiskSpectrum® Professional.

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, MAAP 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.

MAAP 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 (F&B).

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 MAAP 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 code.

For Level 2, 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 the important sequences within a damage state bin.
- To assist in quantifying the containment event tree by aiding in understanding the important phenomena and resulting loads on containment 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, 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, MAAP 4 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 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 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. 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 the CH of the steam lines.

The S-RELAP5 model of the U.S. EPR used for these analyses is based on the model developed for the 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 (CBDTM), 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 PRA for Operations at Power

19.1.4.1.2.1 Risk Metrics

Total CDF from internal events is 2.8E-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 19.1.4.1.2.7.

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. 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 (close to 50 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 30 percent to the total CDF.
- LOOP events leading to seal LOCA contribute 5 percent to the total CDF.
- LOOP events leading to SBO conditions contribute close to 10 percent to the total CDF
- LOOP events leading to seal LOCA and SBO conditions contribute close to 5 percent to the total CDF.

The next biggest contributors to plant risk are SLOCA and general transient.

- 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 (signals or common injection check valves).

- General transient's relatively high contribution can be attributed to a high initiating event frequency.

19.1.4.1.2.3 Significant Cutsets and Sequences

Cutset contribution to the internal events CDF is equally distributed. Only twelve 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 12,000. 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 24 groups, representing over 50 percent of the CDF. One half of these groups are LOOP related, either started with a LOOP initiating events, or a consequential LOOP has occurred as a result of a different initiator. Seven of these groups are related to an SLOCA initiating event.

Many of the LOOP sequences are related to a subsequent loss of ventilation to SBs. As discussed in the system dependencies subsection, Section 19.1.4.1.1.3, a complete loss of HVAC to the electrical rooms in an SB is assumed to result in a loss of the affected equipment after about two hours (if compensatory manual actions are not implemented) and, if the loss of HVAC is in a division with an initially running CCW train (the base PRA model assumes that CCW Pumps 1 and 4 are initially running), a failure of the running CCW pump and failure of the associated CCW CH. A loss of CH1 would, for example, result in a loss of cooling to the SCWS chiller (QKA20) in Train 2, and loss of HVAC to SB 2 and, therefore, a loss of safety Division 2. Therefore, a loss of HVAC in one division with a running CCW pump would result in a loss of two divisions.

In Table 19.1-7, Groups 1, 18 and 24 represent a total loss of HVAC, which started with a LOOP event (an initiator or a consequential LOOP), and failure to start the air-cooled SCWS chillers, which, if a compensatory operator action is not implemented, would result in a loss of HVAC to Divisions 1 and 4. Since these are divisions with running CCW pumps, these failures will lead to a loss of HVAC to the other two divisions and a failure of all safety systems. Group 22 also represents a total loss of HVAC caused by a CCF to run air supply fans. A partial loss of HVAC, to two divisions, combined with the other failures, is represented in Groups 2 and 19. In this

table, which describes the top 100 cutsets, losses of HVAC contribute close to 25 percent of the CDF. In the overall results, HVAC losses contribute to over 40 percent of the total CDF. Because of their importance, Group 2, a more complex group with a partial loss of HVAC, is described in detail below.

Group Number 2 describes cutsets resulting from a LOOP event followed by failure to recover offsite power in two hours and a loss of one division of the SB ventilation system (i.e., HVAC), one EDG and one EFW from different divisions. The sequence of events is as follows:

- Offsite power is lost and not recovered in two hours. SAC Division 1 is in maintenance, and the SAC maintenance train is lost due to the LOOP IE (it is supplied from non-safety AC power).

- Loss of SAC Division 1, and operator failure to recover SB 1 cooling, are assumed to result in a loss of all Division 1 safety systems, within two hours. That leads to a loss of the (assumed) running CCW pump Division 1, and a loss of the CCW Common Header 1, because the ability to perform a switchover to the standby CCW pump Division 2 is also lost (a loss of Division 1 electric power, prevents isolation of the unavailable CCW pump).

- A loss of the CCW Common Header 1, results in a loss of SAC Division 2, and, if not recovered within the next two hours, a loss of all Division 2 safety systems. By this time, approximately four hours have elapsed since the accident, and two safety divisions have been lost. An additional chance to recover offsite power is conservatively not credited.

- If during this time EDG in Division 3 fails to run, a third division is disabled. In these cutsets the EFW Division 4 pump also fails to run, and no EFW pumps are available. One safety division (Division 4) is available for injection, but feed and bleed can not be initiated because a primary bleed function is disabled by a loss of Division 1. No cooling is available and this sequence leads to core damage.

Groups 3 and 21 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 4 and 20 represent a sequence leading to a total SBO, starting with a LOOP event (an initiator or a consequential LOOP), followed by a CCF of all EDGs and failure of two SBODGs to run. Group 5 is similar except that instead of one SBODG failure to run, one EFW pump in the other division is out for preventive maintenance. Again, no EFW or feed and bleed are available.

Group 6 and 15 represent sequences where a CCF of I &C software has led to core damage. In Group 6, a software CCF of the TXS operating system leads to a failure of

the entire protection system, disabling the start of EDGs or EFW pumps. In Group 15, a software CCF of protection system diversity Group B leads to a failure to isolate SGs after an SLBI, resulting in an uncontrolled blowdown of all four SGs. A few of the cutsets in SLOCA groups are also connected to a software CC failure of protection system diversity Group B, leading to failure of the safety injection actuation.

Groups 7 through 14 represent SLOCA cutsets (Group 7 is related to a LOOP-induced seal LOCA). Groups 8, 11 and 13 describe cutsets resulting from SLOCA events followed by a failure of all safety injection either because of a CCF of MHSI pumps and operator failure to initiate fast cooldown, or because of a CCF to open LHSI/MHSI common injection check valves, or because of a common cause plugging of the IRWST sump strainers. Groups 9 and 10 describe 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. In Group 10, MSRIVs are disabled by failures of two electrical divisions: Divisions 2 and 3, which is one of the division failure combinations that would disable MSRIVs. MSRIVs electrical dependencies are described in the system dependencies subsection in Section 19.1.4.1.1.3. 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.

Three remaining groups describe a few specific initiators.

- Group 16 represents cutsets resulting from an SGTR or an induced-SGTR followed by a failure to isolate the failed SG and operator failure to stop the leak by depressurizing the primary system and initiating RHR operation.

- Group 17 represents cutsets resulting from initiating events leading to a loss of main feedwater (MFW, LBOP, LOC) and the stuck control rods. These are ATWS events with MFW unavailable for whose pressure relief was not credited. One of these cutsets represents transient events with the stuck control rods and an operator failure to initiate boration with the EBS.

- Group 23 represents cutsets resulting from an SLBO, followed by a CCF to close MSIVs resulting in all four SGs uncontrolled blowdown, and with operator failure to initiate EBS and control reactivity.

- The important CDF sequences for internal events are presented in Table 19.1-127—U.S. EPR Important Sequences – Level 1 Internal Events. 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 Equipment 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 and air chiller unit trains. The most important SSC can be explained by a high LOOP contribution to the total CDF and by an importance of the HVAC system in the SB 1 and SB 4 (the location of the running CCW pumps).

- Table 19.1-9—U.S. EPR Risk-Significant Equipment based on RAW Importance - Level 1 Internal Events shows the risk-significant SSC based on the RAW importance measure. The two most important events are the EFW storage tanks and 250V DC buses. Their high RAW rank can be explained by their high reliability and by a high consequence of their failures. A failure (a leak) of an EFW tank, if not isolated, would disable all EFW; failure of the Division 4 DC Bus would disable all Division 4 after a LOOP, and would also disable fault isolations in this division (all breaks are assumed to occur in Division 4)

- 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 43 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 action based on RAW is, again, the operator failure to recover room cooling locally given the loss of ventilation, operator action to depressurize RCS and initiate RHR, and operator failure 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 to run SAC air exhaust or supply fans or the CCFs of the SCWS pumps to run, which again illustrates the importance of the HVAC system.

- 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, all I&C common-cause events (software, different diversity groups, different sensors, or sensor processors) have a high RAW. This is because a CCF of the signals could lead to an actuation failure of multiple safety systems. Manual actuations are not credited. Limited credit is given to the operator action to recover software common-cause related actuation failures.

- 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 RAW value larger than 420,000. 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 (a high RAW). Preventive maintenance importance measures illustrate importance of the various safety trains. Based on the RAW values presented in Table 19.1-14, SAC Division 1 and Division 4 have the highest importance, which could be attributed to a general HVAC importance and to the fact that SAC Division 1 and Division 4, as air cooled, are independent from the CCW headers.

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.

- 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.

- CCFs for I&C software are considered and assumed to be equal to 1E-05. Some limited credit is given to the operators to recover from these software CCFs (0.5).

- All year 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:

- For the IEs whose annual frequencies were calculated using fault trees, the point estimates (not mean values) were used as inputs in the CDF quantification. However, mean values were used in the uncertainty evaluation.

- 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.

- IEs representing losses of the CCW headers and trains are conservatively assumed to lead to a loss of the corresponding ESW train, even though this may not always be the case (a loss of one ESW train always leads to a loss of the corresponding CCW train, but not vice versa). This dependency is modeled correctly in the system fault trees, but because of the software limitations, was not captured in the IE model.

- 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.

- Breaks/failures are always assumed to occur in Train 4. For a running system, Train 1 and Train 4 are assumed to be running. These assumptions effect train-specific importance measures. The assumption on the running CCW trains results in an inclusion of the HVAC dependency between two safety divisions, and presents a higher risk configuration.

- 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. Because of that, some interdependencies between different HVAC divisions may not be completely captured in the PRA model.

- 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.

Most 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 nine groups. Table 19.1-15 illustrates the importance of operator actions, LOOP 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 33 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 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 approximately doubles. 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.

Two other modeling assumptions, such as a consequential LOOP probability for controlled shutdown or an RCP seal LOCA probability, show a not-negligible affect 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 15 times in the CDF to 5E-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, or on the assumptions about isolation of the EFW tanks leaks.

A simple sensitivity analysis (not reported in Table 19.1-15) was performed for the ISLOCA events, using mean values for the ISLOCA IE frequencies, versus point estimates. Since ISLOCA event contribution to the CDF is negligible, the effect of this change on the CDF was also negligible (less than one percent).

Table 19.1-15 shows only moderate improvements in CDF if some design changes are considered, or less conservative assumptions are made. The one design change which may be considered in the future (7 percent improvement) is to realign MSRIVs so that they would not require two electrical divisions for their operation.

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: 4.2E-07/yr.
- CDF Internal Events 5 percent Value: 3.1E-08/yr.
- CDF Internal Events 95 percent Value: 1.2E-06/yr.

This ninety-fifth percentile CDF value is more than an order 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 (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. For initiating events evaluated by fault trees, lognormal distribution was fit to the uncertainty distribution obtained from the RS run. Exceptions are IE frequencies for flooding and fire events, which are based on limited information, and, for their modeling, a constrained non-informative distribution (CNI) was used. This will be discussed in the corresponding sections for internal fire and floods.

- Failure Rates: Uncertainty distributions were obtained from the used data source.

- 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: Constrained non-informative prior (Beta) distribution was used, to account for the limited state of knowledge.

- Time Related Parameters: For time-related parameters, like preventive maintenance duration (and corresponding unavailability), lognormal distribution was used, an error factor was estimated from upper and lower bounds, corresponding to upper and lower time estimates.

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 or (3) three out of four EFW pumps 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, 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, (3) Operator recovery is required in 2 hours, or (4) Operator recovery is not possible. 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 50 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–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 (CET) 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.

Core Damage End States

There are two types of interfaces between the Level 1 and Level 2 PRA models. These include the CDESs and the systems credited in the event trees. 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 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 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 Level1- 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 needed support systems, several frontline systems are credited in the Level 2 CET that 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 Level 1 for containment heat removal by cooling the IRWST. In Level 2, 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 Level 1 and Level 2. In 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.

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

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 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.
- 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 RCS. Natural circulation is a result of small differences in gas density between various regions in the reactor vessel and 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 1/6th 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 relief or safety 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 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 RCS failure depends on:

- The temperature of the structure–The temperature is higher close to the RPV and may be 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 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. This failure mode is of most concern in Level 2, because it leads to the potential for large early release.

- 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 affect on other in-vessel and ex-vessel degraded core phenomena. Hydrogen production can be increased due to the flashing of the water in the bottom head of the reactor vessel which passes through the overheated core or by the discharge of accumulator water onto the overheated core. Further, the reactor coolant system pressure at the time of reactor vessel failure is near the containment pressure, thus affecting the potential for degraded core phenomena associated with high pressure reactor vessel failure events (e.g., core debris dispersion and direct containment air heating). Also, the fission product releases to containment are substantially increased due to the creation of a large blowdown from the RCS near the time of fission product release from the core.

It is important to note that the failure modes are mutually exclusive. Once 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 SGs remain pressurized, there is no risk of tube failure for any case analyzed. Hot leg rupture is, however, highly likely (>0.9). The location of hot leg rupture is predicted to be at the nozzle to hot leg pipe weld. This is important for some sequences because it leads to break flow discharge to 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 around 4E-04 for transients and up to 0.84 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 core melt and relocation. 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.

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 steam explosions in-vessel and ex-vessel. 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 upper head would fail 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 for 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 2.3E-05 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 EPR melt stabilization approach, it is assumed (also conservatively) 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 1 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). In order 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 maximum of 12 MPa on the pit wall with a metallic melt composition and a maximum of 9 MPa 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 161 MPa and 8 MPa, 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 conservatively rounded up to 5E-03.

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.

Too little flow, and the accident progression is 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 2192°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 SADV 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 to 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 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 reaction forces on 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) 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.

The potential consequences of overpressurization of the reactor pit are expected to be structural damage. The structural damage potentially resulting 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. Rocketing would be credible if, at the time of vessel failure, upward forces on the vessel exceed the hold-down capability of vessel supports by a margin sufficiently great so as to cause transfer of enough energy to the vessel such that it becomes an energetic missile able to fail the containment.

Direct Containment Heating

The postulated sequence of events for direct containment heating (DCH) 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 CCFP given a core damage accident is less than 0.1, the results in Reference 32 strongly suggest very 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 (DET) 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;
  - 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 vessel breach (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 as possible for the case of a high pressure vessel failure resulting in a complete breach of vessel (CBV) with a conditional probability of 0.02. However, the analysis of vessel failure modes indicated that the probability of the CBV failure mode was low, leading to an overall probability of 2E-04 when conditioned by the probability of a complete vessel rupture occurring. The expected point of failure was assessed to be the melt plug (gate). However, it should be noted that a containment failure due to vessel rocketing would be expected for the CBV failure mode. Cavity failure was also assessed as having a small probability of occurrence of 2.3E-06 in the case of the largest side tear failure of 1m equivalent diameter (as assessed in the vessel failure modes DET analysis).

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. 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. In the case of a 1m hole size, it was also seen that the rocketing forces would not exceed the hold-down forces, although the calculated margin was lower in this case; it is noted that the location of the 1m diameter (side tear) failure precludes rocketing in any case, since forces would be 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. Loadings 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 (≈2000 m/s, or ≈6600 ft/s) relative to the unburned gas. 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 that which corresponds to this 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 (DDT)). 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.

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 48 percent to 82 percent equivalent zircaloy oxidation.

This assessment of deflagrations in the U.S. EPR containment identified two 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 1.38E-04.

The above results were based on bounding assessments in terms of hydrogen and steam conditions (i.e., top of range hydrogen concentrations and steam concentrations close to inert conditions).

The probability of hydrogen deflagration leading to containment failure at the time of vessel failure was dismissed as being of negligible probability, as was the probability of a long-term hydrogen deflagration causing containment failure. 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 26 MAAP analysis cases. 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 lower equipment rooms or middle equipment rooms (MAAP nodes 3 and 5) = 0.016.

  – Assessed probability of containment failure due to flame acceleration loads = 0.016.

- Case 2. Transients at high pressure at approximately the time of Induced Hot Leg Rupture:

  - Assessed probability of local damage in middle equipment rooms (level 2 to 4) or upper equipment rooms (level 2 to 4) (MAAP nodes 6 and 10) = 0.00125.

  - Assessed probability of containment failure due to flame acceleration loads = 0.00125.

- Case 3. Transients at high pressure, at approximately the time of vessel failure:

  - Assessed probability of local damage in middle equipment rooms (level 2 to 4), upper equipment rooms (level 2 to 4), Level 1 upper equipment rooms, or staircase south (MAAP nodes 6, 10, 7, 23) = 0.0056.

  - Assessed probability of containment failure due to flame acceleration loads = 0.0056.

- Case 4a. Low pressure scenarios with short term fast MCCI following vessel failure:

  - Assessed probability of containment failure due to flame acceleration loads = 0.00045.

- Case 4b. Scenarios without recombiner damage/impairment, ongoing long-term MCCI (dry spreading area):

  - Assessed probability of containment failure due to flame acceleration loads = 0.0001.

- Case 4c. Similar to Case 4b but with damaged recombiners (75 percent efficiency):

  - Assessed probability of containment failure due to flame acceleration loads = 0.0005.

Where a destructive combustion mode was assessed to occur without leading to containment failure, the possibility of localized damage to recombiners was considered. This implies loss of some recombiners in the following scenarios: Case 1, Case 2 and Case 3. Cases 4a to 4c have no local consequences, since global failure was assessed a probability of 1.0 of the cases given the occurrence of an accelerated flame (making local consequences irrelevant).

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.

This evaluation identifies and decomposes the treated phenomena, which relies on the results of the analyses performed using MAAP4.07. The MAAP4.07 models the U.S.

EPR core melt retention device and the SAHRS, because these systems are key to the maintenance of containment integrity in the long term.

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, in order 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): 53.7 psi pressure increase.

- Upper bound (from FCHF=1.0 case): 62.4 psi pressure increase.

- Distribution type: symmetric triangular. The triangular 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., some concentration of probability as the tail values are close to incredible).

- 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:

TP/TR:	45 psia	30.5 psig	±7.3 psi
PL:	33.4 psia	18.9 psig	±7.3 psi
SL / ML / SS / LL	27.6 psia	13.1 psig	±7.3 psi

The results of the Monte Carlo simulation using 1 million samples show a conditional probability of containment failure of 0.0 for CDES PL, SL, ML, SS, LL, and 3E-06 for CDES TP/TR.

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 14.5 psi in 40hr, or 0.36 psi/hr. At 60 hr, the pressure is approx. 58 psia. Thus to reach the median failure pressure of 168.3 psig, or 182.7 psia, would take approximately

(182.7 – 58.0) / 0.36 + 60 = 404 hours, or about 17 days

The rate of ablation in the spreading area is approx. 0.5 m in 30 hours, or 0.017 m/hr. The thickness of the basemat below the spreading area is taken from the containment general arrangement drawing and is -22 – (-36.5) feet, or 14.5 feet, or 4.4 m. The time to penetrate the basemat is therefore, approximately:

(4.4 – 1.5) / 0.017 + 60 = 230 hr = 9.5 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, in cases where there is ongoing MCCI, basemat melt through is expected first. Therefore, containment overpressure is judged as very unlikely and 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 arrest 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 that the phenomenon of Hot Leg Rupture, will result in flooding of the reactor pit. Upon vessel failure, there is the possibility that part of the debris will quench and remain in the pit while the remainder of the debris transfers to the spreading area. In this case, no matter what the status of SAHRS, there is a risk of overpressurization of the containment because of boil off of the water in the pit. Containment overpressure could occur because the pit is not in the main cooling circuit of the SAHRS and is maintained at the same level as the spread area / IRWST, thus the pit is constantly replenished.

The coolability of the corium in the pit is highly uncertain, because the debris will form a very deep pool which is not likely to be coolable. Due to this high uncertainty a split fraction of 0.5 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.

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 provide further details on the headers included in each CET and the input events used. These tables are 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, long term overpressure or basemat failure due to core concrete interaction, and sprays for source term mitigation.

The linkage of the CETs to the Level 1 is via 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, 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, seven receive a direct transfer from the CDES link event trees. The eighth CET, the second stage CET for high pressure sequences, only receive 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 this 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, (except isolated SGTRs with pressurizer valves opened).
  - 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 IFSL 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
6. GROUP 6 V & A: CsOH + RbOH
7. GROUP 7 V & A: BaO
8. GROUP 8 V & A: La2O3 + Pr2O3 + Nd2O3 + Sm2O3 + Y2O3
9. GROUP 9 V & A: CeO2
10. GROUP 10 V & A: Sb
11. GROUP 11 V & A: Te2
12. GROUP 12 V & A: UO2 + NpO2 + PuO2

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.
- Importance of retention in Safeguard/Fuel Building for interfacing LOCAs.

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 2.5 to 3 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, RC702, RC801 and RC802.

The conditional containment failure probability (CCFP) 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.

RC402 and 404 are not included in the LRF because only one element (1) has a marginal value of 2.8 percent. Similarly, RC503 and 504 are not considered LRF, even though the guidance is slightly exceeded for a single element (Te). However, to be consistent wit the above guidelines on containment bypass, RC802 (interfacing system LOCA with credit for building deposition) is considered LRF, even though the Cesium and Iodine releases at 2.8 percent are marginal.

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. In order 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, 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, 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.

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.

The fragility curve is used to estimate containment failure probability 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.

Severe Accident Depressurization Valves (SADV)

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 severe accident depressurization valves (SADV). During power operation, the SADVs remain closed. During transient and accident conditions, the functions of the SADVs 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 SADVs 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 also passive, and requires no support systems to perform its functions.

Containment Isolation (CI) System

The containment isolation (CI) 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 (CI) valves:

- The electric motor-operated CI valves inside containment are supplied from Class 1E 480V busses and are backed up by the two hour batteries and EDGs.
- The electrical MOVs outside containment are supplied from Class 1E 480V buses normally backed up by the EDGs, and can also be supplied from a severe accident UPS (12-hour battery) with manual operator action. The severe accident power supply UPS (12-hour battery) is backed up by the SBODGs.
- 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 by passive means to stabilize molten core debris in the core melt retention system (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 three modes of SAHRS operation–passive and active cooling modes, which are used to cool the spreading area under severe accident conditions, and a recirculating mode that is used to cool the water in the IRWST under non-severe accident conditions.

The initial flooding of the spreading area is the result of a passive actuation of two flooding valves. The melting corium opens these 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.

With the flooding valves closed, the spreading area cooling line will recirculate water back to the IRWST. 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

19.1.4.2.2.1 Risk Metrics (LRF, CCFP)

Total LRF from internal events is 2.2E-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 CCFP from all internal events (at power) large release sequences is 0.076. This meets the NRC goal of less than approximately 0.1 CCFP.

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 66 percent of the LRF for internal events is from Release Category RC304. This Release Category represents containment failure before vessel failure with no MCCI occurring and with unavailability of the SAHRS spray for fission product scrubbing. Containment failure before vessel failure scenarios are due primarily to containment overpressure resulting from a steam line break sequence inside containment, with failure to isolate multiple steam generators. Continued blowdown of multiple SG with failure to isolate feedwater or failure to inject extra boration for reactivity control is expected to overpressurize containment. RC304 is conservatively assigned in this case as the availability of the spray is not explicitly evaluated for this sequence in the CET model. The second highest contributor to LRF is from Release Category RC702 and it accounts for greater than 20 percent of LRF. RC702 captures containment bypass due to steam generator tube rupture core damage sequences from Level 1 and induced steam generator tube ruptures from Level 2.

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 all of the cutsets contributing more than one percent to 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 RC304 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. Cutsets that contribute one percent or more to large release for internal events are described as follows.

Release Category RC304 – Cutsets 1 through 8:

These cutsets contribute approximately 39 percent to the internal events large release. These cutsets involve an SLBI with common cause I&C failures that lead to failure of the signals for MSIV and MFW isolation to multiple steam generators. These failures are assumed to lead to an uncontrolled reactivity event due to overcooling and a situation where the steam line break continues to supply steam to the containment as long as feedwater is supplied to the steam generators. The rate of steam addition to the containment during this event is assumed to exceed the capacity of the containment heat removal systems, and the containment is assumed to fail on overpressure.

Release Category RC304 – Cutsets 9 through 12:

These cutsets contribute approximately four percent to the internal events large release. This cutset group also involves an SLBI, but with CCF of MSIVs to isolate and failure of the operator to manual initiate boron injection with EBS. This is assumed to result in an uncontrolled reactivity event due to overcooling and consequent containment failure due to overpressure.

Release Category RC702 – Cutset 1:

This cutset contributes approximately six percent to the internal events large release. This cutset involves an induced steam generator tube rupture (due to excess pressure differential across the tubes prior to core damage) with failure of the operators to initiate RHR. Core damage is assumed to occur and the release is through the ruptured steam generator tube without scrubbing (feedwater not available).

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 57 percent of the LRF results from the ATI CDES. This contribution arises because of the steam line break inside containment sequence described in Section 19.1.4.2.2.3. Of the remaining contribution, 10 percent of the LRF comes from CDES involving SGTR, and 8 percent from core damage sequences involving loss of offsite power with the primary system at high pressure.

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 58 percent is steam line break inside containment. This contribution

arises because of the steam line break inside containment sequence described in Section 19.1.4.2.2.3. The second largest contributing initiating event is steam generator tube rupture (IE SGTR, 13 percent). The third largest contributor is loss of offsite power (IE LOOP, 12 percent). The fourth largest contributing initiating event is induced steam generator tube rupture (IE IND SGTR, 8 percent); note that this is an induced SGTR modeled as an initiating event in the Level 1 core damage sequence, rather than a severe accident induced SGTR due to high temperature and pressure.

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 event L2PH VECF-FA(H) contributes 17 percent of 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 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 VECF-FA(HL) which contributes one percent of LRF is similar to the event described above, except that it applies in the case of a hot leg rupture, which leads to a transient release of hydrogen from the primary circuit to the containment.

Other events appearing as LRF phenomenological contributors (L2PH CPIHLR-TR, TP=Y, L2PH LOCA-DEPRESS=N, L2PH INVREC(NR)=N) 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 a hot leg rupture, the probability of large small LOCAs naturally depressurizing before vessel failure. Note that it is assumed that failure of this depressurization has a probability of 1.0 (i.e., in the

absence of a hot leg rupture or manual depressurization, it is assumed that all small LOCAs will remain at high pressure).

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.

The insights from this table are discussed in the Sensitivity Analysis section that follows.

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. The major difference between the Level 1 and Level 2 results is the increased importance of the Train 4 MSIV. This difference is due to the importance of the unisolated SLBI sequences leading to containment overpressure in LRF.

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. The most prominent difference in the results is the importance of the 24V DC power racks. This could be attributed to the role that these I&C racks play in the automatic isolation functions following SLBI sequences that dominate the LRF, as well as in the SGTR isolation and CI function.

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.

Only twelve operator actions contribute more than one percent to LRF. Only three actions contribute more than five percent. 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 (1) 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. Regarding item (2), 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.

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. The importance of safety-related batteries in both the Level 1 and Level 2 analyses points to the role they play in supporting the active components the U.S. EPR systems. 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.

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.

19.1.4.2.2.5 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) in order 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, with or without the operation of sprays. Thus the Level 2 PRA sent these sequences directly to a release category indicating early, large containment failure.

Sequences involving containment failure due to loads from an accelerated flame originating in the lower, middle or upper equipment rooms prior to vessel failure contribute 18 percent to LRF. This is a small contribution overall, comparable to approximately one percent of the CDF. These failures 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 the SLBI sequence discussed in Section 19.1.4.2.2.2, Section 19.1.4.2.2.4, and Section 19.1.4.2.2.5 and SGTR sequences (initiated in Level 1), 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 related basic events for failure of the containment due to deflagration prior to vessel failure (L2PH VECF-H2DEF(HL) – deflagration fails containment after hot leg rupture. If assumed to always occur this event would lead to a seven times increase in LRF.

- Hydrogen combustion related basic events for failure of the containment due to loads from accelerated flames prior to vessel failure (L2PH VECF-FA(H) and L2PH VECF-FA(HL) – discussed in Section 19.1.4.2.2.4). If assumed to always occur, these events would lead to an 11 times or 9 times increase in LRF, respectively.

- The event L2PH STM EXP INV LP (containment failure due to in-vessel steam explosion), would, if assumed to always occur, lead to nearly a three-fold increase in LRF.

It can be noted that deflagration causing failure of the containment is close to being a physically unreasonable event. Its base probability of 1.38E-04 in case of hot leg rupture 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 benign 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.

Thermally-induced steam generator sequences do not play a significant role in LRF for internal events. However, given that sequences with a depressurized secondary side contribute nine percent of CDF, sensitivity studies were undertaken to study the factors influencing this contribution. The sensitivity to manual depressurization and availability of feedwater was therefore studied. 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 are presented in Figure 19.1-9—U.S. EPR Level 2 Internal Events Uncertainty Analysis Results - Cumulative Distribution for Internal Events LRF.

The uncertainty results are summarized below:

- LRF Internal Events Mean Value: 3.1E-08/yr.
- LRF Internal Events 5 percent Value: 5.8E-10/yr.
- LRF Internal Events 95 percent Value: 9.0E-08/yr.

This ninety-fifth percentile LRF value is more than an order of magnitude below the NRC goal of 1E-06/yr.

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, discrete distributions were 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 double delta. Thus, a probability is assigned for each of two deterministic outcomes for this type of basic event: there is a probability that the

event is sure to occur (relative frequency of one) and another that it is sure not to occur (relative frequency of zero). As discussed in Section 19.1.4.2.2.6, this is an appropriate paradigm for such events, since, generally, it is the case that they do not represent random occurrences. Rather they represent events that are expected to have deterministic, but unknown, outcomes. For each event, the probability of the "sure occurrence" outcome is, therefore, equal to the mean value of the basic events.

19.1.4.2.2.8 PRA Insights

The key insights from the Level 2 PRA for internal events are discussed below.

First, it is noted that the LRF is dominated by sequences entering from the Level 1 which represent a severe challenge to the containment or in which the containment function is already defeated (bypassed). These sequences are those discussed in Section 19.1.4.2.2.3 – (1) a steam line break sequence inside containment, with failure of three steam lines to isolate, failure to isolate feedwater and failure to provide boron injection for reactivity control, and (2) steam generator tube rupture core damage sequences from Level 1, including induced ruptures occurring before core damage.

Despite the above contributors, the CCFP of large release is 7.5 percent, below the NRC goal of 10 percent. If these contributors were absent, the conditional probability of large release would be below two percent, arising from phenomenological challenges. This implies a robust response of the U.S. EPR containment and accident mitigation features for avoiding large release. The key phenomenological challenge to the containment within the residual one to two percent conditional large release probability is due to short term localized hydrogen concentrations leading to potentially flame accelerating mixtures.

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 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.

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 margin assessment employed an approach described in SECY 93-087 (Reference 2). This assessment also followed guidance provided in ANSI/ ANS-58.21 (Reference 35), particularly Section 3.7 and Appendix B, as applicable to seismic margin assessment. The PRA-based seismic margin assessment allows potential vulnerabilities in the design (relative to margin above the safe shutdown earthquake (SSE)) to be identified so that measures could be taken to reduce the risk associated with seismic events.

The primary tasks in the PRA-based seismic margin assessment are as follows:

- Identify the seismic hazard.
- Evaluate the seismic fragility to obtain high confidence of low probability of failure (HCLPF) capacities for SSC.
- Incorporate seismic failures into the system and sequence models to identify their significance with respect to the potential for core damage.
- Assess an overall HCLPF capacity at a sequence level to identify the SSC that are limiting with respect to the potential for core damage.

The U.S. EPR PRA model developed for internal initiating events provides the framework for addressing potential failures induced by seismic events. This model also provides 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

For the U.S. EPR standard design, the site-independent broad-band smooth response spectra, based on the European Utility Requirements (EUR) spectral shapes for different site conditions are referred to as certified seismic design response spectra

(CSDRS). The CSDRS are anchored to 0.3 g peak ground acceleration (PGA), for both horizontal and vertical ground motion. Section 3.7 discusses the EUR spectral shapes.

The CSDRS for the U.S. EPR are shown in Figure 3.7.1-1. These are ground response spectra for EUR Control Motions—hard (EURH), medium (EURM), and soft (EURS) soils. 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, not including an analysis of soil effects, which is the responsibility of the COL applicant, as noted in Section 19.1.5.4. The 1.67 times the CSDRS is referred to as seismic margin earthquake (SME) in design certification. Figure 19.1-31 shows plots of the SME for soft, medium, and hard soil sites.

19.1.5.1.1.3 Seismic Fragility Evaluation

The calculations of the seismic margin for different SSC are performed using the seismic fragility analysis method; the median seismic capacity and variability are estimated. The fragility evaluation characterizes the capacities of SSC to withstand the ground motion due to an earthquake. Fragility is expressed as the conditional probability of failure of SSC as a function of earthquake size. The capacity of a component to maintain its function during and following strong ground motion and the uncertainties associated with that capacity were estimated, taking into account the seismic response at the component's location in a structure. The resulting fragilities are characterized by the median capacity, logarithmic standard deviations that account for randomness and uncertainty, and HCLPF capacity. Both the median capacity and the HCLPF capacity are expressed in terms of peak ground acceleration (PGA). The set of SSC for which fragility was estimated was defined through the development of a SEL, as discussed in the next section.

The seismic assessment included evaluating design information and qualification criteria to estimate the factors of safety (or margin) between the design capacity of a component and its actual capacity. This margin arises, for example, because the actual stress a component could experience might be much less than the allowable stress level, or because the equipment is tested to an enveloping spectrum while the actual floor response spectrum at that equipment location may be significantly lower. Table 19.1-106 shows HCLPF capacities assigned to structures and equipment modeled in this PRA-based SMA. An HCLPF capacity of 0.5 g PGA (1.67 times the SSE) is assigned to each SSC, not including an analysis of site-specific soil effects. Table 19.1-107 shows a sample fragility calculation that represents the process for documenting the SSC fragilities.

Section 19.1.5.4 describes the COL item to perform the site-specific SMA with an analysis of site-specific soil effects.

As noted previously, the HCLPF capacity is a measure of a component's 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 (A_m) for the component and two logarithmic standard deviations, accounting for variability due to uncertainty and randomness (β_U and β_R, respectively). This relationship is as follows:

$$HCLPF = A_m \exp [-1.65 (\beta_R + \beta_U)] \quad (A)$$

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.

The initiating events and event trees in the at-power and shutdown internal events model were reviewed to identify which events needed to be included in the seismic model to account for the types of sequences that could be important following an earthquake. The following consequential initiating events were identified and included in the seismic model:

- Seismic loss of offsite power (S LOOP).
- Seismic small LOCA (S SLOCA).
- Seismic loss of residual heat removal (RHR).
- Seismic LOCA in shutdown.
- Seismic uncontrolled level drop (ULD).
- Seismic interfacing systems LOCA (ISLOCA) in shutdown.

LOOP is the most likely plant initiating event that would result from a seismic event. The LOOP event tree developed for internal events was modified for use in the seismic model. In particular, events related to the restoration of offsite power and events that reflected the use of systems that are not seismically qualified were removed. For further completeness in defining the SEL and modeling of potential sequences, the LOOP model retained a transfer to an ATWS event tree for sequences involving failure of the reactor to trip. The S LOOP event tree is shown in Figure 19.1-10—Event Tree for Seismic Loss of Offsite Power (S LOOP).

The S SLOCA event tree accounts for LOCA sequences that could result from a seismic event (e.g., due to failure of multiple instrument impulse lines). The event tree for

internal events was modified to develop the S SLOCA event tree. The capacity of the RCS may be substantially higher than the SME, but the SLOCA model was developed to enhance completeness of the SEL and of the sequences considered. The S SLOCA event tree is shown in Figure 19.1-11—Event Tree for Seismic Small LOCA (S SLOCA).

The internal events shutdown even tress (Appendix 19B) were utilized directly in the shutdown SMA analysis.

Structures and other passive components not typically included in the internal events PRA were added to the SEL. Containment performance was considered and resulted in additions to the SEL.

Fault trees developed in the internal events PRA were modified to investigate system failure modes and dependencies, and to establish the SEL for fragility analysis. Seismic failures were addressed as follows:

- Basic events representing seismic failures of SSC for which fragility evaluations were performed were added at appropriate points in the fault trees.
- Seismic failures were treated as common events for all trains of a system. For example, the same basic event representing seismic failure of a pump was applied for all similar trains of a system. Complete correlation in that manner assumes that redundant components fail if one component fails.
- Systems not qualified for seismic loadings were set to a failure probability of 1.0. Thus, for example, the seismic model treats both offsite power and the SBODGs as unavailable following a seismic event. No credit is given for recovery of offsite power. Removal of these non-qualified systems allowed simplification of the models.
- Human failure events were retained in the fault-tree models, but were set to failure with a probability of 1.0. This allowed any potentially important events to be visible during the quantification process.

The solution of the integrated fault-tree and event-tree models to evaluate the seismic margin is addressed in the next section.

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 design of the U.S. EPR. 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

Loss of offsite power is the most important initiating event because equipment needed for offsite power to function (e.g., ceramic insulators) typically has low seismic capacity and its failure has effects on safety and non-safety systems. Loss of offsite power results in the loss of main and startup feedwater, the main condenser as a heat sink, and maintenance ventilation systems. The LOOP also presents a demand for the EDGs to supply power to the safety systems. The next section discusses the expected dominant seismic and non-seismic failures that contribute to the LOOP accident sequences.

For purposes of the seismic margins assessment, it is also assumed that a seismic event would lead to leakage from the RCS equivalent to an SLOCA. This assumption is made even though the RCS is expected to have a sufficiently high seismic capacity such that a failure resulting in an SLOCA would be unlikely. The seismically induced SLOCA is included so that a broader set of equipment will be considered in the SEL and associated fragility evaluations than would be the case if only systems needed to respond to a LOOP were included. The primary difference with respect to the cutsets obtained for the S LOOP sequences and those for S SLOCA was the requirement for cooling of the IRWST for the latter. This requirement added cutsets relating to seismic failure of the CCWS and LHSI/RHR to those obtained for LOOP scenarios.

Seismic failures of key structures that house safety-related systems are also considered as initiating events that are assumed to result in core damage. Structures were assessed to have relatively high capacities and were assigned HCLPF capacities larger than the SME based on calculations and generic information.

19.1.5.1.2.3 Significant Functions, SSC, and Operator Actions

The following addresses the accident sequences, which reflect seismic fragilities of systems and equipment, non-seismic failure of equipment, and operator actions.

Table 19.1-37—Summary of Cutsets for Seismic Sequences with LOOP summarizes the S LOOP cutsets; these are limiting with respect to the plant-level HCLPF capacity. These cutsets reflect the following contributions:

- Seismic failure of AC power cabinets (event AC), I&C cabinets (event I&C), emergency diesels-generators (event EDG), batteries (event BAT), ESW (event ESWS) or room cooling (event SAC) represent single element cutsets that limit the plant level HCLPF.

- Seismic failure of emergency feedwater (event EFW) and failure of the operators to initiate feed-and-bleed cooling (event OPE-FB-90M) constitute the first two-element cutset.

- Seismic failure of CCW (event CCWS) and a consequential RCP seal LOCA (event PROB SEAL LOCA) comprise the next two-element cutset.

- The next two cutsets include two seismic failures and failure of an operator action. One of the operator actions is to perform fast cooldown (failure event OPE-FCD-40M) to permit injection by LHSI following a seal LOCA and MHSI failure, and the other is to initiate feed-and-bleed cooling (event OPE-FB-40M).

- The last three cutsets include seismic failure of emergency feedwater (event EFW) and non-seismic failures of equipment and failure of operator action.

The seismic SLOCA results are similar to those presented in Table 19.1-37 for seismic LOOP sequences. These cutsets also include two types of single-element cutsets that reflect seismic failures; these include failure of CCWS and failure of LHSI. Either failure results in a loss of IRWST cooling, which is required in the long term following a LOCA. Since the HCLPF for the SLOCA initiating event is much higher than that for LOOP, these sequences are less significant and are not discussed further.

The S LOOP event tree includes a transfer to the ATWS event tree for scenarios involving failure of the reactor to trip. All ATWS cutsets include seismically induced binding of the control rods, such that they failed to insert. The most important cutset includes operator failure to initiate the EBS, which results in core damage. Since seismic failures leading to ATWS have capacities greater than the SME, these are not discussed further.

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 performed, the plant level HCLPF capacity is greater than SME, not including an analysis of soil effects.

- Seismic PRA model – although the seismic PRA model is quite extensive in that SLOCA and ATWS were included, as well as all success paths in the internal events PRA. 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.

- A COL applicant that references the U.S. EPR design certification will confirm that the design-specific U.S. EPR PRA-based seismic margin assessment is bounding for the specific site.

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, 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—U.S. EPR Locations Selected for the Flooding Analysis and Corresponding Flooding Frequencies. Because these frequencies are based on limited information, constrained non-informative distributions (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.

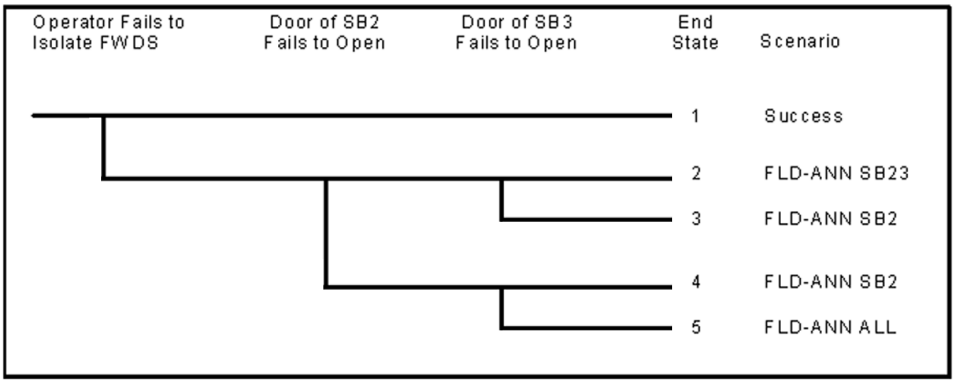
These distributions are shown associated with the flooding scenario frequencies, which will be discussed in the next section (see Table 19.1-39—Flooding Scenarios Description and Frequency Calculation).

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.

One of the more complex scenarios for which frequency was calculated using a simple event tree is the flood in the RB annulus. In this scenario, an operator action is credited to isolate a pipe break before a significant flood level occurs. In addition, two propagation possibilities were considered. The first propagation pathway accounts for the possibility that the doors between the RB annulus and SB 2 would fail open at a certain flood level. The second propagation pathway reflects the potential for the door between RB annulus and SB 3 to fail at a certain flood level. This operator action and these two propagation paths result in five possible outcomes (end states), as shown in the event tree.



1. Operator successfully isolates flooding before any undesirable consequences can occur.

2. Flooding propagates to both SB 2 and 3.

3. Flooding propagates to SB 2 only.

4. Flooding propagates to SB 3 only.

5. Unisolated flooding is contained inside the RB annulus and reaches the level of the electrical penetrations to the containment.

Rough estimates are used to assign probabilities of doors failing under a water pressure. If propagation occurs, the safety systems in the adjacent building are considered failed. If the flood is not isolated and it is contained in the annulus, the water level is assumed to reach containment penetrations. 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 with a probability of 0.5. If the connection boxes fail, it was also assumed that connection with the containment, including all instrumentation, is lost and core damage is assumed.

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.

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

All 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. 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 two categories: floods caused by a break in the emergency feedwater system (EFWS) (the third largest contributor) and floods caused by a break in any other system (the second largest contributor). The reason for this distinction is that a pipe break in the EFWS could potentially affect all four divisions of the EFWS, since four EFW tanks are cross-connected and, if not isolated, could all drain through the same break. 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 would disable one CCW common header.

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

In order to simplify discussion of the sequences related to the flooding scenarios, two flood-specific failure patterns are explained below:

1. A flood in SB 1 could result in a failure of the CCW CH 1, in the following sequence of events: the flood disables the Division 1 running CCW train and the corresponding switchover valves (assumed to fail open), thereby disabling a switchover to the CCW standby train. A loss of CH1 results in the failure of cooling to Division two SCWS chillers, and to two out of four OCWS chillers. As

explained in Section 19.1.4.1.1.3, this would lead to a complete loss of ventilation in SB 2, and, if not recovered, a total loss of Division 2. Therefore, a flood in SB 1 could result in a loss of two divisions. The similar is true for SB 4, which hosts another running CCW train.

2. A flood caused by a pipe break in the EFWS could result in the simultaneous draining of the four EFW tanks and a potential total loss of the EFW system if the operators fail to isolate the leaking train. In the same scenario, the EFW system would also be lost if a consequential LOOP occurs following the plant trip after the pipe break, because in this case no make-up would be available to the EFW tanks, since the make-up water would come from the DWS that requires non-safety power to operate.

The top 100 cutsets from the RS output for quantification of the flood CDF are evaluated in detail. One cutset dominates the flooding CDF, with a contribution slightly above 50 percent. This cutset is related to a flood contained in the annulus, as discussed in the previous sections and below. Apart from this outlier, cutset contributions to the internal flooding CDF are relatively evenly distributed. The second largest cutset accounts for about four percent of the flooding CDF; all other cutsets contribute less than one percent each. The number of cutsets that contribute to 95 percent of the flooding CDF is larger than 12,500.

The significant cutsets for the internal floods are shown in Table 19.1-41—U.S. EPR Important Cutsets - Level 1 Flooding. 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 12 groups, representing over 68 percent of the flooding CDF. These groups are discussed below:

Group 1 in Table 19.1-41 represents a single cutset that accounts for 50 percent of the internal flooding CDF: the flood contained in the annulus with failure of the connection boxes to the containment.

Groups 2, 3 and 4 represent a total loss of HVAC following a flood in the SB 1 or 4 or the TB. The events leading to complete failure of ventilation differ between the different groups, but follow the mechanisms and dependencies discussed in Section 19.1.4.1.1.3. In Groups 2 and 3, the PAS is also failed, and assumed to disable the maintenance SAC train, MFW, and SSS. In Group 3, a flood in the TB also disables these systems. A loss of HVAC in all SBs is initiated by a flood in one, hosting a running CCW train, followed by an independent failure of the ventilation in the second building hosting the other running CCW train. As discussed in the flood-

specific failure pattern 1 above, a loss of Divisions 1 and 4, associated with the running CCW trains, could, if not recovered in time, lead to a loss of two additional safety divisions. All EFW and the possibility to perform feed-and-bleed will be lost, leading to core damage.

Group 5 represents a sequence 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 CCF of the EFW pumps to start.

Groups 6, 8, 9 and 10 represent the RCP seal LOCA sequences following a flood in the SB 1 or SB 4 including the FB. As explained in flood-specific failure pattern 1 above, a flood in SB 1 or SB 4 results directly in a loss of CCW CH2 and consequently in a loss of seal cooling to two RCPs (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 (the SAHRS is unavailable due to the flood), or failure of MHSI to inject. In Table 19.1-41, which accounts for the top 100 cutsets, seal LOCA sequences contribute to 6.4 percent of the flooding CDF. Overall, a consequential seal LOCA accounts for about 30 percent of the flooding CDF.

Groups 7 and 12 represent sequences when floods caused by pipe breaks in the EFWS result in a complete loss of feedwater. Since the four EFW tanks are connected and are required for a successful core cooling during a 24-hour mission time, a break in any of the trains has the potential to drain the full inventory unless the operator isolates the break and initiates makeup with the demineralized water system (DWS). The DWS is a non-safety system that relies on offsite power. Therefore, a consequential LOOP following the flooding event will fail the makeup. Since it also fails the MFWS and the SSS, all feedwater is lost. Failure of feed-and-bleed, either due to an operator failure to initiate the action (Group 7) or due to a failure of required systems (Group 12, a CCF of all EDGs to run), results in core damage.

Group 11 represents a single cutset that combines a flood in SB 4, with independent failures of HVAC to Division 2, MHSI pump Division 1, and PAS (disables MFW and SSS). This leads to a failure of three divisions (2, 3 and 4), a failure of MSRTs because of electrical dependencies (see Section 19.1.4.1.1.3), and only one EFW train being available when two are needed to remove decay heat through MSSVs. Feed and bleed fails because the only available MHSI pump fails independently.

The important CDF sequences for internal floods are presented in Table 19.1-128—U.S. EPR Important Sequences – Level 1 Flooding Events. 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 Equipment based on FV Importance - Level 1 Flooding shows the top risk-significant SSC based on the FV importance measure. The MHSI pump trains 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 (Groups 6, 8, 9, 10 in Table 19.1-41), and require safety injection.

Table 19.1-43—U.S. EPR Risk-Significant Equipment 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 the RCP seal isolation MOVs (i.e., nitrogen and leakoff valves) and the SSSS. This can be explained by the importance of those components in preventing an RCP seal LOCA following a flood in SB 1 or SB 4. Since these floods are assumed to propagate to the FB, they could simultaneously fail one CCW common header (CH) and the CVCS, thereby disabling thermal barrier cooling and the seal injection to two RCPs. A single failure of an RCP seal isolation MOV or the SSSS could result in a seal LOCA.

Table 19.1-44—U.S. EPR Risk-Significant Human Actions based on FV Importance - Level 1 Flooding shows the risk-significant human actions based on the FV importance measure. The most 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 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 initiate a feed and bleed for transient events. Its importance could be explained by multiple flooding sequences leading to a total loss of feedwater. It is also important to note that the operator failure to isolate a FWDS break in the annulus is modeled as part of the initiating event frequency, therefore it is not shown in these tables. If it was included in the model, this action would be expected to have a significant contribution to the internal flooding CDF.

Table 19.1-46—U.S. EPR Risk-Significant Common Cause Events based on RAW - Level 1 Flooding shows the risk-significant common-cause events based on the RAW

importance measure. The most important common-cause event based on the RAW value is a CCF of normal HVAC air exhaust or supply fans and associated SCWS pumps to run. This reflects the importance of ventilation dependencies in the plant risk in general. The RAW of these CCF is especially high for flooding events because the dominant scenario, apart from the annulus, leads to a failure of one division and to a possible loss of HVAC to another division.

Table 19.1-47—U.S. EPR Risk-Significant Common Cause I&C Events based on RAW Importance - Level 1 Flooding shows the significant common-cause I&C events based on the RAW importance measures. The most important common-cause I&C failure is the CCF of the TXS Operating System. The software common cause failure of the TXS operating system is assumed to fail the entire protection system and would result in a failure of multiple systems and functions which are required to mitigate the effect of a flooding initiating event.

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 that the annulus connection boxes could withstand a flood and 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, expansive

time is needed to flood a building up to ground level, so operator isolation is likely to succeed if automatic isolation failed.

- Pipe breaks in the EFWS are treated as flooding events with the potential to drain all four EFW tanks. It is assumed that the operators would have the ability to manually isolate an EFW pipe break occurring in any of the four SB with isolation valves in another unaffected SB, and to initiate DWS makeup to the tanks of the intact EFW trains

- The probability that the connection boxes of the electrical penetrations that run through the annulus will fail if submerged is estimated to be 0.5. This number represents the limited state of knowledge regarding the design of those penetrations. This assumption has a very high importance, because the failure of the penetrations is assumed to lead directly to core damage.

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 shows a lower sensitivity to most parameters that impact internal events CDF, such as HEPs, common cause factors, success criteria, and assumptions on offsite and onsite power. This could be explained by the following: the flooding CDF is dominated by one scenario, flooding of the annulus, which is not sensitive to evaluated assumptions.

The assumption on seal LOCA probability is a notable exception; the flooding CDF is sensitive to this assumption. This is consistent with the high importance of components and assumptions related to the mitigation of seal LOCAs, as noted in Section 19.1.5.2.2.3. This is caused by the second and third dominant scenarios, in which a flood affects simultaneously SB 1 or SB 4 and the FB, disabling both CCW CH 1 or 2 and the CVCS directly leading to a loss of seal cooling. The internal flooding CDF is not sensitive to the probability of the CVCS requiring a switchover to IRWST. This can be explained by the fact that the CVCS is directly failed by a flood extending to the FB.

The importance of seal LOCA sequences could also be attributed to a conservative assumption of not crediting a recent design change that allows a crosstie of the RCP thermal barrier cooling to different CCW common headers.

The impact on the CDF of the assumptions specific for the flooding events modeling is also studied. The assumption on the isolation of an EFW shows only a mild impact on the flooding CDF, because the failure of isolation and make-up to the EFWS is dominated by the probability of a consequential LOOP, which would disable the make-up option.

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: 8.8E-08/yr.
- CDF Internal Flooding Events 5 percent Value: 3.1E-09/yr.
- CDF Internal Flooding Events 95 percent Value: 2.2E-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 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 annulus. It accounts for 50 percent of the overall flooding CDF. This high contribution to the plant risk highlights a vulnerability of annulus pipe break events. It is also the result of conservative assumptions made due to the lack of a detailed design of the annulus electrical penetrations.

Flooding in the SB 1 or SB 4 is dominated by the seal LOCA scenarios, because this flood causes a complete loss of seal cooling to two of the RCPs, and a single failure in the isolation of the RCP seals results in a seal LOCA with a probability estimated to be 0.2. Seal LOCA sequences contribute to more than 30 percent of the flooding events CDF. This corresponds to 60 percent of the risk from sequences other than the flood in the annulus.

Dependencies between support systems also play a significant part in the internal flooding CDF. The sequences where systems fail on total or partial loss of the HVAC

represent about 12 percent of the flooding events CDF. This corresponds to 24 percent of the risk from sequences other than the flood in the annulus.

The flood due to the EFWS pipe break has a relatively low contribution to CDF because of a low pipe-break frequency, but has a relatively high conditional core damage probability due to the potential drainage of all EFWS tanks.

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 1.1E-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 CCFP from all flooding (at power) large release sequences is approximately 0.018. This meets the NRC goal of less than approximately 0.1 CCFP.

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 10 percent of the internal events LRF (1.12E-09 versus 2.17E-08). Approximately 76 percent of the flooding large release is from Release Category RC304. RC304 captures containment failure before vessel failure and these flood-initiated failures are primarily due to early containment failure by hydrogen flame acceleration-induced containment rupture. Approximately 18 percent of the flooding LRF is from Release Category RC702. These containment failures are primarily due to induced steam generator tube rupture with depressurized steam generators. Approximately 3.7 percent of the flooding LRF is from Release Category RC205, which involves containment isolation failure with melt released from vessel, without MCCI, melt flooded ex-vessel without containment sprays. Approximately 2 percent of the flooding LRF is from RC201, which involves a large containment isolation failure with successful melt retention in-vessel.

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, all of the 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 early containment failure by hydrogen flame acceleration induced containment rupture in Release Category Flood RC304, followed by induced steam generator tube rupture with a depressurized secondary side of the steam generator in Release Category Flood RC702. Cutsets that contribute one percent or more to large release for internal events are described below.

Release Category RC304 – Cutset 1:

This cutset contributes approximately 46 percent to the flooding events LRF. This cutset is a flooding event caused by a pipe break in the reactor building annulus which is assumed to impact electrical penetrations and connection boxes, resulting in failure of all sensors and signals from inside containment with an assumed probability of 0.5. Given the loss of signals, this event is assumed to result directly in core damage. This scenario results in a high pressure core damage end state, and the containment fails before vessel rupture due to hydrogen flame acceleration loads.

Release Category RC702 – Cutsets 1 and 2:

These cutsets contribute approximately seven percent to the flooding events LRF. This cutset group describes a flooding event in the pump room of SB 4 resulting in loss of CCWS common header 2 (CH2). With SAC1 in maintenance, PAS failure and operator failure to recover room cooling results in the loss of ventilation in Division 1, 2 and 3. A two-inch diameter equivalent seal LOCA occurs on loss of seal injection or loss of bearing cooling and failure to trip the RCPs. The failure of PAS fails MFW and SSS, all EFW trains are lost because of the loss of ventilation. Primary bleed fails because of loss of Division 1. This results in a core damage end state at high pressure and an induced steam generator tube rupture with the secondary side depressurized and feedwater unavailable.

Release Category RC702 – Cutsets 3 and 5:

These cutsets contribute approximately 3.5 percent to the flooding events LRF. The sequence of events for these cutsets is similar to RC702-1 and 2, with a flood in the pump room of SB 4 resulting in the loss of CCWS CH2. With SAC1 in maintenance, PAS failure and operator failure to recover room cooling results in the loss of ventilation in Division 1, 2 and 3. A 0.6-inch diameter equivalent seal LOCA occurs on loss of seal injection or loss of bearing cooling and failure to trip the RCPs. The failure of PAS fails MFW and SSS, all EFW trains are lost because of the loss of ventilation. Primary bleed fails because of loss of Division 1. This results in a core

damage end state at high pressure and an induced steam generator tube rupture with secondary side depressurized and feedwater unavailable.

Release Category RC304 – Cutset 2:

This cutset contributes approximately three percent to the flooding events LRF. This cutset involves a flood in the pump room of SB 4 that results in the loss of CCWS CH2. With SAC1 in maintenance, PAS failure and operator failure to recover room cooling results in the loss of ventilation in Division 1, 2 and 3. The failure of PAS fails MFW and SSS, all EFW trains are lost because of the loss of ventilation. Primary bleed fails because of loss of Division 1. This results in a core damage end state at high pressure and an induced hot leg rupture. The containment fails before vessel rupture due to hydrogen flame acceleration induced rupture on overpressure.

Release Category RC205 Cutset 1:

This cutset contributes approximately three percent to the flooding events LRF. This cutset is a flooding event caused by a pipe break in the RB annulus which is assumed to impact electrical penetrations and connection boxes, resulting in failure of all sensors and signals from inside containment. Given the loss of signals, this event is assumed to result directly in core damage with an assumed probability of 0.5. This scenario results in a high pressure core damage end state, the automatic containment isolation signal fails due to the loss of signals from inside containment, and the operators fail to initiate manual CI signal with containment sweep ventilation small flow line ventilation initially open.

Release Category RC702 – Cutset 4:

This cutset contributes approximately one percent to the flooding events LRF. This cutset begins with a flood due to a pipe break in EFW train 4, flooding the SB 4 pump room and the fuel building. The flood in the pump room of SB 4 results in the loss of CCWS CH2. With SAC1 in maintenance, with PAS failure, and with the operator failure to recover room cooling, the result is the loss of ventilation in Division 1, 2 and 3. A seal LOCA occurs on loss of seal cooling and failure to trip the RCPs. The failure of PAS fails MFW and SSS, all EFW trains are lost because of the loss of ventilation. Primary bleed fails because of loss of Division 1. This results in a core damage end state at high pressure and an induced SGTR with secondary side depressurized and feedwater unavailable.

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 CDES contributing above 0.5 percent to LRF for flooding events all involve high pressure core damage sequences. Sixty four percent of the frequency is associated with transient type end states, TR and TR1 CDES. Seal LOCAs with a depressurized secondary side (SSD and SS1D) account for 28 percent of LRF. Seal LOCAs with a pressurized secondary side (SS and SS1) account for eight percent of LRF. As noted in the discussion of internal events, a depressurized secondary side, especially in the case of a small LOCA (or seal LOCA) raises the probability of an induced SGTR due to increased circulation of hot gases in the primary loop. However, it should also be noted that, as mentioned in Section 19.1.5.2.2.3, many flood initiators lead to the possibility of seal LOCAs. While these events may have a depressurized secondary side due to operator actions performing a full secondary cooldown to achieve conditions for LHSI injection, core damage does not necessarily mean that no feedwater is available to the SGs, since failure of safety injection itself is another possible failure path.

Table 19.1-53—U.S. EPR Initiating Event Contributions - Level 2 Internal Flooding shows the contribution of the flooding initiating events to LRF.

Three of the major flooding scenarios can lead to core damage sequences involving seal LOCAs. These initiators are IE FLD-SAB14 FB, IE FLD-EFW and IE FLD-TB. The annulus flood, IE FLD-ANN ALL can only lead to transient CDES. Thus the former initiators show more susceptibility to induced SGTR.

Table 19.1-54 through Table 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.

For flooding initiating events, the hydrogen combustion related basic events L2PH VECF-FA(H) (i.e., very early containment failure before vessel failure due to hydrogen combustion with flame acceleration) is dominant (75 percent of LRF). The variant of this event used in the case of hot leg ruptures, L2PH VECF-FA(HL), is also present (10 percent of LRF).

The event L2PH ISGTR-SS2D=Y contributes about 15 percent of LRF (i.e., equivalent to less than 0.5 percent of CDF). This is the conditional probability of a thermally-induced SGTR occurring for two-inch equivalent seal LOCA sequences. The U.S. EPR provisions for emergency depressurization of the primary circuit contribute to keeping this contributor small, despite the onerous characteristics of the incoming core damage sequences from Level 1. This is also similar to the case of fire events. The analogous

event L2PH ISGTR-SS0.6D=Y (for 0.6 inch equivalent seal LOCAs) contributes 5 percent of LRF.

A more detailed discussion of the contributors is provided in the section on fire events in Section 19.1.5.3.3.3, and is not repeated here.

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.

This table shows a strong consistency with the results of the Level 1 analysis contained in Table 19.1-42. 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 importance of the EFWS, the LHSI check valve, and the Stand Still Seal in the Level 1 analysis carries over into the Level 2 results.

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.

As with the FV results, this table shows a strong consistency with the results of the Level 1 analysis contained in 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. Also prominent are the elements of the RCP seals, as is the highly reliable EFW storage tank.

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.

Similar to LRF results, the list of important human action events for floods is dominated by Level 1 core damage operator actions. The reasons for this are discussed in Section 19.1.4.2.2.4. However, unlike fires and internal events, the list does not exclusively contain Level 1 actions: the action OPF-L2-CI-30M (i.e., failure of manual backup for containment isolation) is present, contributing 3 percent of LRF.

It should be noted that the operator actions with the "=Y" suffix representing success events are included into the model to allow a more accurate CDF calculation.

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.

The LRF results show particular sensitivity to OPF-SAC-2H and OPE-FB-90M. This is because they are implicated in a large number of incoming core damage sequences. The RAW for actions related to operator trip of the RCPs are also significant. This can be explained by the importance of the seal LOCA sequences in the flooding LRF.

Similarly, sensitivity based on RAW is seen for OPF-L2-CI-30M.

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. Also prominent are the common cause failure of the elements of the SIS which plays an important role in both the Level 1 and Level 2 event analysis.

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.

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 not dominated by the specific Level 1 sequence types discussed in Section 19.1.4.2.2.2 andSection 19.1.4.2.2.3, the observed sensitivity to individual phenomenological events is greater for floods. The following event can lead to a significant decrease in LRF if set equal to 0.0:

- L2PH VECF-FA(H) – very early containment failure due to flame acceleration loads in high pressure sequences. This event has a significant effect because of its large contribution to a small LRF value.

Several events can lead to a significant increase in LRF if set equal to 1.0:

- L2PH VECF-FA(H) and L2PH VECF-FA(HL), which can increase the LRF by factors of 47 and 9 respectively if set equal to 1.0. The (HL) variant represents very early containment failure due to flame acceleration loads in sequences where an induced hot leg rupture occurs.

- L2PH VECF-H2DEF(HL) and L2PH VECF-H2DEF(H) can increase LRF by factors of 30 and 5 respectively if set equal to 1.0. These events represent hydrogen deflagrations failing containment after hot leg rupture or in a high pressure sequence.

- The event L2PH STM EXP INV LP (containment failure due to in-vessel steam explosion in low pressure sequences), would, if assumed to always occur, lead to a 30 times increase in LRF.

The observations made in Section 19.1.4.2.2.6 (internal events) regarding flame acceleration and in-vessel steam explosion are also relevant in the case of floods. The deflagration events were evaluated as being close to a physically unreasonable probability level, 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. Sensitivity to steam explosions arises because, if not excluded from the model, these events are applicable to a large proportion of core damage sequences.

Thermally-induced steam generator sequences play a significant role in LRF for flood events. Flood sequences involving seal LOCAs are significant LRF contributors. 38 percent of LRF involves consequential seal LOCAs from flooding events and 29 percent of LRF also involves a depressurized secondary side of the steam generators. These proportions slightly exceed the corresponding contributions of these sequences to CDF (seal LOCAs contribute 26 percent of CDF, and 13 percent of CDF involves seal LOCAs with a depressurized secondary). In view of this information, sensitivity studies were undertaken to study the factors influencing the induced SGTR contribution to LRF for floods. The sensitivity to manual depressurization and availability of feedwater was therefore studied. It was found that, for the case of flood events, neither the unavailability of primary depressurization nor the unavailability of

feedwater individually had a large impact on the frequency of RC702. However, the combined impact of both being unavailable had a significant impact on both the RC702 frequency and on LRF. The sensitivity study with combined unavailability of depressurization and feedwater suggested a five times increase in LRF.

19.1.5.2.3.6 Uncertainty Analysis

The results of the uncertainty evaluation for the Level 2 Flooding Events LRF are presented in Figure 19.1-14—U.S. EPR Level 2 Flood Events Uncertainty Analysis Results - Cumulative Distribution for Flood Events LRF.

The uncertainty results are summarized below:

- LRF Internal Flooding Events Mean Value: 1.2E-09/yr.
- LRF Internal Flooding Events 5 percent Value: 1.0E-12/yr.
- LRF Internal Flooding Events 95 percent Value: 1.2E-09/yr.

This ninety-fifth percentile LRF value is more than two orders of magnitude below the NRC goal of 1E-06/yr.

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, discrete distributions were 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

As also discussed in Section 19.1.4.2.2.4 for internal events, sequences involving containment failure due to loads from an accelerated flame originating in the lower, middle or upper equipment rooms prior to vessel failure are visible contributors to LRF, the specific contribution being 75 percent in the case of internal floods. The key features of the analysis of accelerated flames and their impact on containment are discussed in Section 19.1.4.2.2.4 and not repeated here.

In the absence of the specific challenges and bypasses of containment seen in the internal events analysis, the results for LRF for flooding events are dominated by severe accident phenomenological issues. The specific issue for floods is the possibility of an accelerated flame arising from hydrogen combustion in the lower or middle equipment rooms during the in-vessel phase of a high pressure core melt. Further background discussion on the analysis of this issue is provided in Section 19.1.4.2.2.4.

Incoming sequences from the Level 1 feature flood-induced seal LOCAs in conjunction with a depressurized secondary side. The phenomena of thermally-induced steam generator tube rupture, which was assessed as having a large probability for equivalent two-inch LOCAs (seal or otherwise) with a depressurized secondary side and an absence of feedwater to the steam generators (therefore also features in the results approximately 15 percent contribution to LRF) but is not dominant. The contribution of this phenomenon is discussed in Section 19.1.4.2.2.3. Sensitivity studies showed a significant increase in LRF due to this phenomena only in the bounding case of assumed concurrent unavailability of feedwater and depressurization functions; individual unavailabilities were not significant.

The importance results for floods show only one operator action from the Level 2 model as contributing. This action is the operator manual backup for containment isolation. LRF shows sensitivity to this action based on its RAW.

Despite the dominance of a single phenomenological issue for LRF, it is noted that LRF is less than approximately two percent of CDF for flooding events. Other phenomenological challenges were not identified as leading to significant probabilities of large release.

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 all 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-AC, which includes the AC switchgear room and cable floor of SB 1.
- 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:

- The Plant-Specific Spatial Database.
- 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 fifteen 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. Fire initiating events and their contributions are illustrated in Figure 19.1-15. As can be seen from Table 19.1-65 and Figure 19.1-15, 10 out of 15 fire initiating events contribute less than one percent of the internal fire CDF. The fire in the AC 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 two biggest contributors to fire risk are the fire in the MFW/MS valve room and the fire in the MCR. The 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 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 fourth 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 fifth fire scenario that contributes more than one percent to the internal fire risk is a fire in the mechanical division (pump room) of an SB. This scenario 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.

19.1.5.3.2.3 Significant Cutsets and Sequences

In order to simplify discussion of the sequences related to the fire scenarios, two fire-specific failure patterns are explained below:

1. A fire in SB 1 could result in a failure of the CCW CH 1, in the following sequence of the events: the fire disables the Division 1 running CCW train and the corresponding switchover valves, thereby disabling a switchover to the CCW standby train. A loss of CH1 results in the failure of cooling to Division 2 SCWS chillers, and to two out of four OCWS chillers. As explained in Section 19.1.4.1.1.3, this would lead to a complete loss of ventilation in SB 2, and, if not recovered, a total loss of Division 2. Therefore, a fire in SB 1 could result in a loss of two divisions. The same is true for SB 4, which hosts another running CCW train.

2. A fire in the switchgear room of SB 1 or SB 4 directly results in the failure of the primary bleed function. In order to succeed, the bleed function requires either three out of three PSRVs to open, which requires the four electrical divisions, or one out of two SADVs to open, which requires Division 1 and Division 4. A fire in the switchgear room of SB 4, therefore, prevents both combinations.

The top 100 cutsets from the RS output for quantification of the fire CDF are evaluated in detail. Two cutsets dominate the fire risk, with individual contributions of about 15 percent to the fire CDF. Due to the lack of detailed design and procedures, conservative assumptions were made for the fires in the MFW/MS valve room and the MCR, and the importance of those cutsets could be attributed to these assumptions. Other than these two outliers, 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 2300.

The significant cutsets for the internal fires are shown in Table 19.1-66—U.S. EPR Important Cutset Groups - Level 1 Fire 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 12 groups, representing over 76 percent of the fire CDF. These groups are discussed below:

Groups 1 and 9 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 an MSRIV, then two MSIVs fail to close due to the fire. In Group 1, failure to align the RHR or failure of the RHR results in core damage. In Group 9, independent failure of a third MSIV to close results in the blowdown of three SGs and an overcooling event. The failure to control reactivity with the EBS leads to core damage.

Group 2 represents a single cutset: fire in the MCR and failure of the operators to transfer control to the RSS in adequate time.

Groups 3, 6, and 12 represent a total loss of HVAC following a fire in an SB pump room, the Switchgear Building and the CSR, respectively. The events leading to a complete failure of ventilation differ between the different groups but follow the mechanisms and dependencies described in Section 19.1.4.1.1.3. In Group 3, the PAS is failed, and assumed to disable the maintenance SAC train, MFW, and SSS. In Group 12, a consequential LOOP also disables these systems. A loss of HVAC in all of the SBs is initiated by a fire in one, hosting a running CCW train, followed by an independent failure of the ventilation in the second building hosting the other running CCW train. As discussed in the first fire-specific failure pattern 1 above, a loss of Divisions 1 and 4,

associated with the running CCW trains, could, if not recovered in time, lead to losses of two additional safety divisions. All EFW and possibility to perform feed-and-bleed will be lost, leading to core damage.

Groups 4, 5, 7 and 11 represent the RCP seal LOCA sequences resulting from a fire in the switchgear room of SB 1 or SB 4. As explained in the first fire-specific failure pattern 1 above, a fire in the switchgear room of SB 1 or SB 4 results directly in a loss of CCW CH 2, and consequently in a loss of thermal barrier cooling to the seals of two RCPs. 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 cooling to two affected RCPs. A failure to isolate seals for one of these two RCPs, leads to a seal LOCA with an assumed probability of 0.2. The PCD function fails because the MSRTs are not available, and the primary bleed fails because of the loss of Division 4. In Table 19.1-66, which summarizes the top 100 cutsets, the seal LOCA sequences represent 30 percent of the fire CDF. Overall, a consequential seal LOCA accounts for about 43 percent of the fire CDF.

Group 8 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 secondary cooldown to succeed. Feed-and-bleed is disabled by the fire.

Group 10 represents a single cutset 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 11 percent of the overall fire risk.

The important CDF sequences for internal fires are presented in Table 19.1-129—U.S. EPR Important Sequences – Level 1 Fire Events. 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 Equipment based on FV Importance - Level 1 Fire Events shows the top risk-significant SSC based on the FV importance measure.

The EDG trains, the cooling tower fan trains, and the air-cooled SCWS chiller trains have the highest FV. The presence of EDG trains highlights the importance of consequential LOOP events following a fire. The cooling tower fan trains are needed for long term cooling in seal LOCA sequences, which represent a large part of the fire risk. The air-cooled SCWS chillers importance reflects the importance of ventilation dependencies.

Table 19.1-68—U.S. EPR Risk-Significant Equipment based on RAW Importance - Level 1 Fire Events shows the top risk-significant SSC based on the RAW importance measure. The most important components are 6.9kV divisional switchgears, 480V load centers, 24V DC I&C Power Rack, and 480V MCCs. This dominance of electrical and I&C components is partly due to the fact that the scenario which dominates the fire risk (i.e., fire in the switchgear room of SB 1 or SB 4) directly results in the failure of all buses for one division. Failure of buses in another division could have a significant impact on the mitigating systems like the MSRTs that require a specific combination of two divisions to perform their function.

Table 19.1-68—U.S. EPR Risk-Significant Equipment based on RAW Importance - Level 1 Fire Events shows the risk-significant human actions based on the FV importance measure. The most important operator actions are operator failure to recover room cooling locally, failure to initiate RHR cooling in four hours and failure to transfer to the RSS following an MCR fire. The first action reflects the importance of ventilation dependencies in the plant risk in general. The second and third actions are required in order to mitigate the two most important fire sequences (i.e., a fire in the MFW/MS valve room with MSIVs failure to isolate and a fire in the MCR).

Table 19.1-70—U.S. EPR Risk-Significant Human Actions based on RAW Importance - Level 1 Fire Events shows the risk-significant human actions based on the RAW importance measure. Only four 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 four hours, operator failure to recover room cooling locally, 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 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 CCF of normal air exhaust or supply fans, the CCF of SCWS pumps to run and the CCF of LHSI/MHSI common injection check valves to open. The importance of the first two common cause events reflects the general importance of ventilation dependencies, while the risk significance of the last event is due to the significant contribution of 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 Fire Events shows the significant common-cause I&C events based on the RAW importance measure. The most important common cause I&C failure is the CCF of the TXS Operating System. The software CCF of the TXS operating system is assumed to fail the entire protection system and would result in a failure of multiple systems and functions which are required to mitigate the effect of a fire initiating event.

Table 19.1-73—U.S. EPR Risk-Significant PRA Parameters - Level 1 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 to predict the MS line isolation for the fires in the MFW/MS valve room, and the parameters used in the modeling of an RCP seal LOCA. 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.

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 most parameters that impact 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 11 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 a higher sensitivity to assumptions on the seal LOCA probability and 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.

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 assumption on the probability that the total loss of seal cooling to an RCP and the failure to isolate this RCP seal will result in a seal LOCA (PROB SEAL LOCA = 0.2) has a high importance value in the internal fire risk, because of the high occurrence of seal LOCA sequences among the dominant fire scenarios. For the same reason, an assumption on the probability that CVCS switchover to the IRWST may be required also has a high importance value in the internal fire risk.

The importance of seal LOCA sequences could also be attributed to a conservative assumption of not crediting a recent design change that allows a crosstie of the RCP thermal barrier cooling to different CCW common headers.

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. The modeling assumption on a complete separation of the safety and non-safety divisions in the CSR is also found to have a high 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: 9.5E-09/yr.
- CDF Internal Fire Events 95 percent Value: 7.0E-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 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 40 percent of the overall fire CDF. This dominance highlights the reliance of some important safety functions (e.g., steam relief via MSRTs, or primary bleed) on a multiple number of electrical divisions. It is also the result of the modeling assumptions on the running train of CCW.

Seal LOCA sequences are important to the fire risk. They also contribute to over 40 percent of the overall fire CDF. If the CVCS switchover to the IRWST is required, the dominant fire scenario would result directly in a total loss of seal cooling to two of the RCPs, and a failure to isolate RCP 4 seals.

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 3.6E-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 CCFP from all fire events (at power) large release sequences is 0.02. This meets the NRC goal of less than approximately 0.1 CCFP

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 15 percent of the internal events LRF (3.6E-09 versus 2.2E-08). Approximately 80 percent of the LRF for fire events comes from Release Categories RC303 and RC304. RC303 and 304 capture containment failure before vessel failure, and these fire initiated failures are primarily due to early containment failure by hydrogen flame acceleration induced containment rupture. Approximately 17 percent of the fire events LRF is from Release Category RC702. These containment failures are primarily due to thermally induced SGTR during the severe accident for sequences with a depressurized secondary side of the SG. Several fire initiators (e.g., fires in the switchgear or safeguard building) result in the possibility of seal LOCAs, thus some sequences entering from the Level 1 have seal LOCAs and a depressurized secondary side and these are key contributors to LRF for fires.

Approximately 1.2 percent of the fire events LRF is from Release Category RC205, which involves containment isolation failure with melt released from vessel, without MCCI-melt flooded ex-vessel without containment sprays.

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. Cutsets that contribute one percent or more to large release for internal events are described below.

Release Category RC303 – Cutset 1:

This cutset contributes approximately 11.7 percent to the fire events LRF. This cutset is a fire in the MFW/MS valve room which causes spurious opening of an MSRIV. MSIVs 3 and 4 are postulated to fail open due to the fire and this leads to two steam generators blowing down simultaneously. Operator failure to align RHR leads to core damage. After core damage occurs, the operator successfully depressurizes the primary system, and the containment fails before vessel rupture due to hydrogen flame acceleration loads.

Release Category RC304 – Cutset 1:

This cutset contributes approximately 11.2 percent to the fire events LRF. This cutset captures a fire occurring in the MCR and the operators fail to evacuate and transfer control of the plant to the remote shutdown station in sufficient time to prevent core damage. This results in a high pressure sequence that stays pressurized until vessel failure. The containment fails before vessel rupture due to hydrogen flame acceleration loads.

Release Category RC702 – Cutsets 1 and 2:

These cutsets contribute approximately eight percent to the fire events LRF. These cutsets involve a fire in the pump room of SB 4, which results in the loss of CCWS CH2. A seal LOCA occurs on loss of seal injection or bearing cooling, and with SAC1 in maintenance, PAS failure and operator failure to recover room cooling, the loss of ventilation in Division 1, 2 and 3 results. The failure of PAS fails MFW and SSS, and all EFW trains are lost because of the loss of ventilation. Primary bleed fails because of the loss of Division 1. An induced SGTR results from the high pressure core damage scenario with the secondary depressurized and feedwater unavailable.

Release Category RC304 – Cutsets 3 and 4:

These cutsets contribute approximately 4.7 percent to the fire events LRF. These cutsets are similar to Fire RC303 in that they both result in early containment failure from hydrogen flame acceleration loads. In these cutsets a fire in the switchgear room

of SB 4 results in the loss of CH2 and prevents CVCS to switch suction to IRWST. Seal cooling to RCP 4 is lost and RCP 4 leakoff valves fail to close on loss of Division 4, resulting in a seal LOCA. A loss of control power in Division 1 or 2 disables the secondary cooldown function, and primary bleed fails because of the loss of Division 4. This results in a high pressure core damage sequence, which results in containment failure due to hydrogen flame acceleration loads.

Release Category RC304 – Cutset 2:

This cutset contributes approximately 3.3 percent to the fire events LRF. This cutset involves a fire in the pump room of SB 4, which results in the loss of CCWS CH2. With SAC1 in maintenance, the PAS failure and operator failure to recover room cooling results in the loss of ventilation in Division 1, 2 and 3. The PAS fails MFW and SSS, all EFW trains are lost because of the loss of ventilation. PBL fails because of the loss of Division 1. This results in a high pressure core damage sequence that results in an induced hot leg rupture, and containment fails before vessel rupture due to hydrogen flame acceleration loads.

Release Category RC304 – Cutsets 5 and 7:

These cutsets contribute approximately 2.8 percent to the fire events LRF. These cutsets involve a fire in the switchgear room of SB 4 and a consequential LOOP results in the loss of CH2 and fails CVCS. Seal cooling to RCP 4 is lost and RCP 4 leak-off valves fail to close on loss of Division 4, resulting in a seal LOCA. LOOP and EDG failure result in a loss of Division 2, failing the secondary cooldown function. The operators fail to cross connect electrical trains 1 and 2 and PBL fails because of the loss of Division 4. This results in a high pressure core damage sequence that remains pressurized until vessel failure. The containment fails before vessel rupture due to hydrogen flame acceleration loads.

Release Category RC 702 – Cutsets 3 and 4:

These cutsets contribute 2.7 percent to the fire events LRF. These cutsets involve a fire in the pump room of SB 4, which results in the loss of CCWS CH2. A seal LOCA occurs on loss of seal injection or bearing cooling. With SAC1 in maintenance, the PAS failure and operator failure to recover room cooling results in the loss of ventilation in Division 1, 2 and 3. Loss of PAS fails MFW and SSS, all EFW trains are lost because of the loss of ventilation. PBL fails because of the loss of Division 1. This results in a high pressure core damage sequence that results in an induced SGTR with secondary depressurized and feedwater unavailable.

Release Category RC 304 – Cutset 6:

This cutset contributes 1.2 percent to the fire events LRF. Fire in the pump room of SB 4 results in the loss of CCWS CH2. With SAC1 in maintenance, consequential LOOP

and operator failure to recover room cooling results in the loss of ventilation in Division 1, 2 and 3. Loss of offsite power fails MFW and SSS, and all EFW trains are lost because of the loss of ventilation. PBL fails because of the loss of Division 1. This results in a high pressure core damage sequence that results in an induced hot leg rupture and containment failure before vessel rupture due to hydrogen flame acceleration loads.

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.

This table shows that over 50 percent of the sequences involve seal LOCA CDES (SS and SS1D). It also shows that 30 percent of the sequences (TRD and SS1D 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. However, it should also be noted that many fire initiators lead to the possibility of seal LOCAs; while these events may have a depressurized secondary side due to operator actions performing a full secondary cooldown to achieve conditions for LHSI injection, core damage does not necessarily mean that no feedwater is available to the SGs, since failure of safety injection by itself is another possible failure path.

Table 19.1-78—U.S. EPR Initiating Events Contributions - Level 2 Internal Fires shows the contribution of the fire initiating events to LRF.

The listing of fire initiating event contributions to LRF shows a dominance of high pressure core damage sequences. Of the listed initiators, only IE-FIRE-PZR directly involves a LOCA, but with only one 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-AC, IE FIRE-SAB-MECH, IE FIRE-SWGR all correspond to fire initiators for which seal LOCAs are a possibility. As discussed, the increased possibility of a thermally induced steam generator tube rupture 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 release location of hydrogen into the containment from the primary circuit following core damage.

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 event L2PH VECF-FA(H) contributes approximately 80 percent of LRF (i.e., equivalent to approximately 1.5 percent of CDF). This event is also important for internal events and is discussed in detail in Section 19.1.4.2.2.4. The event represents the likelihood of containment failure occurring due to loads from an accelerated flame originating in the lower or middle equipment rooms.

The event L2PH VECF-FA(HL) which contributes approximately two percent of LRF (equivalent to <0.1 percent of CDF) is similar to the event described above, except that it applies in the case of a hot leg rupture, which leads to a transient release of hydrogen from the primary circuit to the containment.

The event L2PH ISGTR-SS2D=Y contributes 13 percent of LRF (i.e., equivalent to less than 0.5 percent of CDF). This is the conditional probability of a thermally-induced SGTR occurring for equivalent two-inch equivalent seal LOCA sequences. The U.S. EPR provisions for emergency depressurization of the primary circuit contribute to keeping this contributor small, despite the onerous characteristics of the incoming core damage sequences from Level 1. An analogous event, L2PH ISGTR-SS0.6D=Y (for 0.6 inch equivalent seal LOCA) contributes four percent of LRF.

Other events appearing as LRF phenomenological contributors (L2PH CPIHLR-TR,TP=Y, L2PH LOCA-DEPRESS=N, L2PH CPIHLR-SS,SL=Y) 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 a hot leg rupture (for TR, TP, SS and SL CDES) and the probability of the upper bound small LOCAs naturally depressurizing before vessel failure. It is assumed that failure of this depressurization has a probability of 1.0 (i.e., in the absence of a hot leg rupture or manual depressurization, it is assumed that all small LOCAs will remain at high pressure).

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 importance of the EFWS in the Level 1 analysis carries over into the Level 2 results.

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.

Only eleven operator actions contribute more than one percent to LRF. Eight of these actions contribute more than five percent. 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. 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. Also prominent is the common cause failure of the SIS injection check valves. The failure of these normally reliable valves fails all injection to the core, both in the Level 1 and Level 2 event tree analyses.

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 that 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.

Since the LRF results for fires are not dominated by the specific Level 1 sequence types discussed in Section 19.1.4.2.2.2 and Section 19.1.4.2.2.3, the observed sensitivity to individual phenomenological events is greater for fires. The following event can lead to a significant decrease in LRF if set equal to 0.0:

- L2PH VECF-FA(H) – very early containment failure due to flame acceleration loads in high pressure sequences. This event has a significant effect because of its large contribution to a small LRF value.

Several events can lead to a significant increase in LRF if set equal to 1.0:

- L2PH VECF-FA(H) and L2PH VECF-FA(HL), which can increase the LRF by factors of 50 and 17 respectively if set equal to 1.0. The (HL) variant represents very early containment failure due to flame acceleration loads in sequences where an induced hot leg rupture occurs.

- L2PH VECF-H2DEF(HL) and L2PH VECF-H2DEF(H) can increase LRF by factors of 15 and 16 respectively if set equal to 1.0. These events represent hydrogen deflagrations failing containment after hot leg rupture or in a high pressure sequence.

- The events L2PH STM EXP INV LP and L2PH STM EXP INV HP (containment failure due to in-vessel steam explosion in low and high pressure sequences respectively), would, if assumed to always occur, lead to 11 and 14 times increases in LRF respectively.

The observations made in Section 19.1.4.2.2.6 (internal events) regarding flame acceleration and in-vessel steam explosion are also relevant in the case of fires. The deflagration events were evaluated as being close to a physically unreasonable probability level, 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. Sensitivity to steam explosions arises because, if not excluded from the model, these events are applicable to a large proportion of core damage sequences.

Thermally-induced steam generator sequences play a significant role in LRF for fire events. Fire sequences involving seal LOCAs are significant LRF contributors. Fifty-two percent of LRF involves consequential seal LOCAs from fire events and 17 percent of this LRF also involves a depressurized secondary side of the steam generators. These proportions slightly exceed the corresponding contributions of these sequences to CDF. Seal LOCAs contribute 42 percent of CDF, and only one percent of CDF involves seal LOCAs with a depressurized secondary. In view of this information, sensitivity studies were undertaken to study the factors influencing the induced SGTR contribution to LRF for fires. The sensitivity to manual depressurization and availability of feedwater was therefore studied. It was found that, for the case of fire events the unavailability of primary depressurization had a negligible impact on the RC702 frequency. Both the unavailability of feedwater individually and the combined impact of both being unavailable had a larger impact on both the RC702. However, this sensitivity was not significant when viewed in terms of its impact on LRF, which was increased by less than two times.

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 are presented in Figure 19.1-19—U.S. EPR Level 2 Fire Events Uncertainty Analysis Results - Cumulative Distribution Function for Fire Events LRF.

The uncertainty results are summarized below:

- LRF Internal Fire Events Mean Value: 3.8E-09/yr.
- LRF Internal Fire Events 5 percent Value: 3.6E-13/yr.
- LRF Internal Fire Events 95 percent Value: 3.3E-09/yr.

This ninety-fifth percentile LRF value is more than two orders of magnitude below the NRC goal of 1E-06/yr.

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, discrete distributions were 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.

19.1.5.3.3.7 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 severe accident phenomenological issues. The specific issue for fires is the possibility of an accelerated flame arising from hydrogen combustion in the lower or middle equipment rooms during the in-vessel phase of a high pressure core melt. Further background discussion on the analysis of this issue is provided in Section 19.1.4.2.2.4.

As also discussed in Section 19.1.4.2.2.4 for internal events, sequences involving containment failure due to loads from an accelerated flame originating in the lower, middle or upper equipment rooms prior to vessel failure are visible contributors to LRF. The key features and assumptions of the analysis of accelerated flames are discussed in Section 19.1.4.2.2.4 and not repeated here.

The phenomena of thermally-induced steam generator tube rupture, which was assessed as having a large probability for equivalent two-inch seal LOCAs in conjunction with a depressurized secondary side and an absence of feedwater to the SGs, also features in the results (i.e., 13 percent contribution to LRF). Seal LOCAs are a contributor to the fire CDF, as discussed in Section 19.1.5.3.2.3. Sensitivity studies show that LRF did not significantly increase due to this phenomenon even in the bounding case of assumed concurrent unavailability of feedwater and depressurization functions.

Despite the dominance of a single phenomenological issue for LRF, it is noted that LRF is only approximately two percent of the CDF for fire events.

Other phenomenological challenges were not identified as leading to significant probabilities of large release.

19.1.5.4 Other Externals Risk Evaluation

The design certification scope of external event screening includes an assessment of high winds 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 including a site-specific PRA-based SMA for soil effects (including sliding and overtuning, liquefaction, and slope failure).

19.1.5.4.1 High Winds and Tornado Risk Evaluation

All U.S. EPR Seismic Category I structures are designed to meet the following standards for high winds 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 145 mph. This value bounds all locations within the U.S. except the extreme southern tips of Louisiana and Florida (SEI/ASCE 7-05).

Tornado 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 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). These design-basis tornado wind characteristics are bounding for all U.S. regions within the contiguous 48 states.

Tornado 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) as specified in NUREG-0800, Section 3.5.1.4. The design basis 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 Generating Buildings (EPGB).
- Essential service water (ESW) Pump Structures.
- ESW Cooling Water Structures.

- Fuel Building (FB).
- Vent Stack (VSTK).

Based on the U.S. EPR design, a tornado or high wind event will not have a significant impact on safety-related equipment. The most limiting impact from a tornado 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 and Tornado Evaluation Conclusion

The preceding high winds 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 and tornado hazards. Therefore, the risk from high wind and tornado events is judged not significant.

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. Therefore, the risk from external flooding events is judged not significant.

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. Therefore, the risk from external fire and smoke events impacting plant operations is judged not significant.

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) describes the set of initiating events.

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). Because only one train of heat removal is required to prevent heat up and two, three or four RHR trains are normally available/running during various POS, multiple trains have to fail to cause this initiating event. The RHR system, as well as its support systems, including offsite power, are included in the analysis.

- Diversions and leaks in operating RHR – Flow diversions and leaks (SLOCA) 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).
- SG Relief during SBO – Only one SG volume is required to cope for two hours of SBO during shutdown versus all four in the power operation model.
- 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" models plant response to a LOCA inside containment while in POS CA or CB. The LOCA initiating event model includes pipe break, as well as RHR flow diversion.

Event Tree "SD LOCA D E" models plant response to a LOCA inside containment while in POS D or E. The LOCA initiating event model includes pipe break, as well as flow diversion 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.

Accident Sequence Quantification

The LPSD PRA model is quantified using the same data and common cause parameters as the at-power PRA model. The event trees and fault trees were developed and solved using the RiskSpectrum® computer code. The RiskSpectrum® model for the LPSD PRS constitutes a detailed set of event trees and fault trees. The model whose results are described in this section consists of the following:

- Nearly 3000 basic events (not including CCFs).
- Nearly 1200 fault trees.
- Over 3600 fault tree gates.
- Over 130 CCF groups.
- Over 4400 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 LPSD, all POSs, resulted in over 90,000 cutsets. The first 100 cutsets represented over 65 percent of the total CDF; 95 percent of the CDF was represented by over 8,000 cutsets.

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 (RCS makeup success, but no 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 CA 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 CAD and CBD.

- 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 (2 percent) 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 5.8E-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. 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, the shutdown initiating events which dominate shutdown core damage frequency are uncontrolled level drop in states CBD and DU, LOCA in state CBD, and loss of RHR in state CBD. 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 37 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 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. 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 16 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 8000. 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. 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 15 groups, representing over 65 percent of the CDF. Almost half of these groups are LOOP related (i.e., started with a LOOP/Loss of RHR initiating event). Seven of these groups are related to an SLOCA initiating event. In Table 19.1-92, Groups 1 and 2 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, followed by a long term operator failure to isolate leak and prevent a slow RCS drain outside containment.

Groups 3 and 4 are similar to Groups 1 and 2. They 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 cold leg injection check valves, common to all injection trains.

Groups 5, 6, 7, 9 and 10 all represent a loss of RHR cooling due to a LOOP event during POS CAU, CAD, CBD, and CBU, followed by a CCF of all EDGs to run. Since CCW trains are not supplied from SBO DGs, the only way to cool the plant is by the EFW pump in Division 1 (only SGs 1 and 2 are assumed to be 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 8 and 11 represent a loss of RHR cooling due to a LOOP event during POS CAU, 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 12 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.

Group 13 and 14 represent a LOCA in POS CBD and DU, due to an inadvertent opening of a LHSI overpressure protection safety valve and an operator failure to isolate. Core damage occurred because of a CCF of cold leg injection check valves, common to all injection systems.

Group 15 represents a LOCA outside containment in POS E and CBD, caused by a pipe break in an operating RHR train, followed by a failure of both manual and auto isolation.

All "important" CDF sequences, with a sequence frequency greater than one percent of shutdown core damage frequency (as presented in Section 19.1.6.2.1), are shown in Table 19.1-130—U.S. EPR Important Sequences – Level 1 Shutdown. For each 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 19.1-98 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 Equipment 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 trains, the first SIS isolation check valves, CVCS low pressure reducing station MOVs, and the SBO DG trains. The importance of these SSC can be explained by a high LOOP and "level drop" 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 electrical system, including 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 the CVCS low pressure reducing station, operator failure to isolate RHR flow diversion in state CB, 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., software, different diversity groups, different sensors, or sensor processors) have a high RAW. This is because a CCF of the signals could lead to an actuation failure of multiple safety systems. Limited credit is given to the operator action to recover software common-cause-related actuation failures.

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 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.

- Maintenance on the SG systems is assumed to be performed on two SGs, which are assumed not available in states CAD and CBD. Maintenance on all other trains is assumed to occur in state E. One division is assumed out for maintenance during that state.

- 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 (F&B), which is conservative for shutdown (two of two is expected to be adequate and one of two 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.

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.

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 CCFs than the at-power CDF. 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. This resulted in a 48 percent increase in the LPSD CDF.

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: 9.9E-08/yr.
- CDF LPSD Operation 5 percent Value: 5.2E-09/yr.
- CDF LPSD Operation 95 percent Value: 2.2E-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 represented in the shutdown 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 close to 40 percent of the shutdown risk. The dominant contributor to these initiating events is a LOOP during shutdown states. LOCAs in shutdown and the ultimate level drops in shutdown, contribute approximately 30 percent each to the LPSD CDF.

If the assumptions on the POS durations are to be neglected, the highest risk states are CBD and DU. These 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 risk-significant 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 depressurization has occurred through the operator initiating feed and bleed; in that case, the corresponding CDES is PL and is directed to low pressure CET.

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, the hatch must be closed prior to core damage 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, the ability to close the hatch is credited. The initial actions are performed inside the containment; therefore, the habitability of the containment (i.e., local temperature no higher than 122°F) 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 Level 1 and Level 2. In 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, Level1 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 the consequential LOOP is no longer an issue. LOOP recovery during the three time frames defined in the Level 2 PRA is credited the same as 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 dependant 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:

Because the likelihood of SG tube threatening temperatures and pressures arising under shutdown conditions is lower, compared to at-power conditions, but not negligible; it was concluded that the induced SGTR (ISGTR) should be retained in the model but with a reduced probability. For sequences entering the CET from CDES TR,

a probability of zero was used for POS CA and CB, based on extrapolation of the MAAP runs for POS CB. For sequences entering the CET from CDES SL and SS, a reduced value of ISGTR was calculated. This reduced probability was based on the probability of loop seal clearance determined in the at-power analysis. This approach is judged to be conservative because loop seal clearance was found to be a major driver of ISGTR in the at-power analysis.

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 48 percent to 82 percent equivalent Zircaloy oxidation.

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 and it was concluded that the IRWST volume (i.e., containment node 2) was the only node resulting in a susceptible flame acceleration mixture. The high combustible gas concentration in the IRWST is because of the RHR safety valve discharge in this volume.

One difference to be noted compared to at power is that no damage to the recombiners is assumed in early flame acceleration loads because they are not located in the IRWST volume where the combustible gas discharge occurs.

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 global 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 8.7E-06.
- Hydrogen flame acceleration loads: high pressure core damage transient resulting in a probability of containment failure of 3.2E-02.

Time at vessel failure:

- Hydrogen deflagrations loads: an evaluation of the hydrogen loads based on the global AICC pressure resulted in a negligible probability of containment failure.
- Hydrogen flame acceleration loads: the combustible gas concentration did not indicate any susceptibility to flame acceleration.

Time frame after vessel failure:

- Hydrogen deflagrations loads: containment failure probability is considered to be negligible. This is concluded because the oxygen leakage back into containment (resulting in de-inerting the containment atmosphere) is not expected.
- Hydrogen flame acceleration loads:
  - low pressure containment failure due to hydrogen loads in the spreading area following rapid hydrogen production from concrete ablation (Molten Core Concrete Interaction (MCCI)) before passive flooding is actuated.
  - containment failure due to hydrogen loads in the spreading area following hydrogen production from concrete ablation (MCCI) with failure of passive flooding.

The at power containment failure probabilities are conservatively used for these two cases.

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 338°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 following 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 in the containment.

Ex-Vessel Steam Explosions:

The at-power conditions leading to ex-vessel steam explosions are considered to be bounding because the release rate of corium and depth of water in the reactor pit are not expected to be exceeded at shutdown. Furthermore, the unlikelihood of hot leg rupture under the shutdown conditions results in a probability of water spillage in the reactor pit at vessel failure negligible.

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:

- 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-Condensibles, 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-condensibles 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-condensibles 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 non-condensibles generation 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 eight containment event trees (CET). 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:

- Distinctions between the different POS (i.e., C, D, E) are achieved by having 1 CET for each POS, except for high pressure CETs that are only applicable to state C. This is because POS C is the only state where the RCS can be pressurized.
- In the first stage CET for high pressure, the functional event indicating a high pressure of the RCS in small LOCA sequences is removed. In shutdown all small LOCA sequences are conservatively assumed to remain pressurized.
- The low pressure CET (See Figure 19C-4) for POS E is modified not to account for the success of the containment isolation. This is because the equipment hatch closure is not possible in state E.
- 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.

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 5.7E-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 0.099. This meets the NRC goal of less than 0.1.

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 50 percent of the LRF from shutdown events come from two release categories: RC201 (26.6 percent) and RC802 (27.3 percent). The release category RC201 represents containment failure due to isolation failure with melt retained in the vessel. Containment isolation failure in shutdown also includes failures due to an open containment hatch. The release category RC802 represents containment bypass due to ISLOCAs events in shutdown (RHR line ruptures outside containment). The two next largest contributors to the LRF come from RC204 (17.3 percent) and RC303 (15.8 percent). The only other two not-negligible LRF contributors are RC205 (8.1 percent) and RC304 (4.8 percent). These four release categories are discussed in two groups below.

Release category RC303 represents containment rupture before vessel breach with containment spray. Release category RC304 represents containment rupture before vessel breach without containment spray. In the shutdown sequences, containment rupture before vessel breach is occurring due to hydrogen flame acceleration. At power, the RC304 is dominated by ATWS type sequences due to unisolable multiple steam line breaks inside containment.

Release category RC204 represents containment failure due to isolation failure with melt released from the vessel and flooded with containment spray. Release category RC205 represents containment isolation failure with melt released from the vessel and flooded without containment spray. In total, containment isolation failures RC201, RC204, and RC205 contribute over 50 percent to LRF, which is not unexpected for shutdown events where there is less restriction on containment isolation and containment can be open.

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 that describes a state with RHR cooling, the water level at midloop (i.e., the lowest for the state) and the RPV head on. This high contribution is associated with a high CDF in that state. The highest CCFP of 1 is associated with POS E, where containment is open and not re-closable. The lowest CCFP of 0.026 is associated with POS D, where containment is assumed to be closed.

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: LOCA

during Shutdown State CBd (18.6 percent), RHR ISLOCA during Shutdown State E (13.9 percent) and Loss of RHR in Shutdown State CAd (10.2 percent). 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—POS CA Release Category Contributions to Shutdown LRF, Figure 19.1-33, and Figure 19.1-34 through Figure 19.1-35 illustrate release category contributions to the LRF in different POSs. As seen in the figures, containment isolation failures, ISLOCAs, and containment ruptures due to early hydrogen flame acceleration are the main LRF contributors in the POS CA and CB. Hydrogen flame acceleration is not a concern in the POS D and E. Containment is open and not reclosable in POS E, ISLOCAs present the highest LRF contributor due to a higher contribution to the CDF in that state. 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. LOCA in POS CB, Loss of RHR in POS CA and CB and ISLOCA in POS E contribute more than 80 percent to the total LRF.

19.1.6.4.3 Significant Cutsets and Sequences

Cutset contribution to the shutdown events LRF is equally distributed. Only six of the top cutsets contribute more than 1 percent to the total LRF. The number of cutsets that contribute to 95 percent of LRF is over 30,000. These insights show that there are no outliers in the shutdown events LRF.

The significant cutsets for internal events are illustrated in Table 19.1-120—U.S. EPR Important Cutset Groups - Level 2 Shutdown. In Table 19.1-120, the first hundred cutsets are grouped based on their similar or 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 LRF, cumulative percentage contributions to the total CDF, and a selected representative cutset, with corresponding basic events and their descriptions.

As shown in Table 19.1-120, the top 100 cutsets are grouped into 22 groups, representing over 50 percent of the LRF. The largest group (RC 802, 26.7 percent) represents RHR ISLOCAs sequences due to RHR pipe breaks outside containment in different shutdown states, containment is bypassed and the release is not scrubbed.

Group #2 (RC204, 6.1 percent) represents LOCA sequences in POS CB and failure to close containment hatch in 1 hour. Group #3 (RC303, 4.1 percent) represents a loss of RHR due to a LOOP sequences in POS CA and CB, with very early containment failure due to hydrogen flame acceleration. Group #4 (RC303, 3.2 percent) represents LOCA sequences in POS CB with a failure of all injection and very early containment failure due to hydrogen flame acceleration. Group #5 (RC204, 2.6 percent) represents LOCA sequences in POS E with failure of all injection; the containment is open in POS E. Group #6 (RC205, 2.1 percent) represents LOCA sequences in POS CB and failure to close containment hatch in 1 hour with SAHR spray not available. All other cutsets groups inTable 19.1-120 contribute less than 1 percent to the shutdown LRF.

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 CDES with the highest contribution to LRF is "IS" (28.8 percent) representing ISLOCA sequences due to RHR pipe break outside containment. The "not depressurized" LOCA CDES SL(CB) and transient CDES TR(C) contribute together over 43 percent to the LRF. The fourth most important CDES is PL(CB), including LOCA sequences after a "bleed" initiation (i.e., opening of the pressurizer safety valves) that contributes 13 percent to the LRF.

Table 19.1-122—U.S. EPR Risk-Significant Phenomena based on FV Importance - Level 2 Shutdown, Table 19.1-123—U.S. EPR Risk-Significant Phenomena based on RAW Importance - Level 2 Shutdown, Table 19.1-124—U.S. EPR Risk Significant Level 2 Human Actions based on either FV or RAW Importance - Level 2 Shutdown, and Table 19.1-125—U.S. EPR Risk Significant Components based on FV Importance Measure Related to Level 2 Specific Importance - Level 2 Shutdown show 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 19.1-122 also shows the risk-significant Level 2 phenomena based on the FV importance measure. The phenomena with the highest FV are the "Very early containment failure due to H2 flame acceleration" (FV = 19.8 percent), and "In vessel recovery default success for depressurized cases" (FV=18.2 percent). The last event does not represent a direct containment failure event; rather, it represents phenomenological occurrences during the sequences that have an indirect impact on containment performance. The other events in Table 19.1-122 also represent various phenomenological occurrences.

Table 19.1-123 shows the risk-significant Level 2 phenomena based on the RAW importance measure. Only three containment failure events have shown to be important based on the RAW ranking. The event with the highest RAW value is a containment failure due to in-vessel steam explosion. This high value could be

contributed to a very low probability of the event (5.6E-6). The second most important event is a "Very early containment failure due to H2 flame acceleration;" that event is identified as a significant contributor to the LRF frequency in shutdown, with both importance measures, FV and RAW, above screening criteria.

Table 19.1-124 shows the risk-significant Level 2 human actions. 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 (i.e., probability of failure is set to 1), the action to close the hatch in 1 hour, without power.

Table 19.1-125 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 that did not show as important in the shutdown CDF calculation. Insights from these tables show that components related to SAHR, RHR HL isolation, PRZ relief valves, and their support systems that did not show as important in the shutdown CDF calculation are now showing as important due to their contribution to the LRF.

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 shut down states was used, which is conservative when estimating times available to close the hatch.

- Induced RCS ruptures (i.e., IHLR and 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. Only six of the top cutsets contribute more than 1 percent to the total LRF, and over 30,000 cutsets are included in 95 percent of 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.

- Components related to SAHR, RHR HL isolation, PRZ relief valves, and their support systems, that did not show as risk significant in the SD CDF calculation, are risk significant due to their contribution to the LRF.

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.

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 5.3E-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 5.8E-08/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 2.6E-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 0.05. This meets the NRC goal of less than approximately 0.1 CCFP.

Mean values and associated uncertainty distributions can be found in Section 19.1.8.4.

The total LRF from shutdown events is 5.7E-9/yr which is also well below the NRC and U.S.EPR probabilistic design goals. The resulting CCFP for shutdown events is 0.099 which also meets the NRC CCFP goal of 0.1.

The total CDF from both at power events and shutdown events is 5.9E-07. Correspondingly, the total LRF for both at power and shutdown events is 3.2E-08. The

resulting overall CCFP remains at 0.05. 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 55 percent to the total risk, fires 33 percent and floods 12 percent.

The distribution between the different plant operating states is illustrated in Figure 19.1-38—POS Contributions to Total LRF. At-power risk contributes 90 percent to the total risk. States CBD and DU dominate shutdown risk.

The distribution between the different POS for Total LRF (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 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. The general LOOP initiating event (which is not SBO or RCP LOCA related) dominates the total risk. Fire in SB 1 or SB 4 switchgear room is the second largest contributor, followed by SLOCA, fire in the MCR and flood in the RB annulus.

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 83 percent to the total risk, fires 13 percent and floods 4 percent. The largest contributors are SLBI (47 percent) and SGTR (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. Early containment failures in the Release Category 300 family contribute approximately 75 percent to total LRF. Steam Generator Tube Ruptures contribute approximately 20 percent to the total LRF. Containment isolation failures contribute approximately 4 percent, and interfacing system LOCAs contribute approximately 1 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.

Systems ranked based on the contribution to the total CDF at-power are illustrated in Figure 19.1-28—U.S. EPR System Ranked by Importance (FV) - Level 1 Total. The electrical system and ventilation system have the highest contribution to overall risk as could be concluded from the discussions in the earlier sections. The RCS, including RCP seals, also has a very high contribution.

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, consequential LOOP value, 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: 7.4E-07/yr.
- CDF Internal, Fire & Flood Events 5 percent Value: 8.7E-08/yr.
- CDF Internal, Fire & Flood Events 95 percent Value: 2.0E-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 are 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.

- LRF Internal, Fire & Flood Events Mean Value: 3.6E-08/yr.

- LRF Internal, Fire & Flood Events 5 percent Value: 7.1E-10/yr.
- LRF Internal, Fire & Flood Events 95 percent Value: 1.1E-07/yr.

This ninety-fifth percentile at-power LRF value is more than one order of magnitude below the NRC goal of 1E-04/yr.

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. ANSI/ANS-58.21-2003, "External Events in PRA Methodology Standard," American National Standards Institute/American Nuclear Society, 2003.

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. ANP-10309P, Revision 0, "U.S. EPR Digital Protection System Technical Report," AREVA NP Inc., November 2009.

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 1, "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report," AREVA NP Inc., December 2009.

59. ANP-10290, Revision 1, "Environmental Report Standard Design Certification," AREVA NP Inc., September 2009.

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 satisfy Capability Category III. Elements of the PRA that cannot generally meet at least Category II until later stages of design, construction and operation include the following: ● Plant-specific operating experience is not available for review, although experience of current plants was considered (IE-A3, IE-A7). ● Operators are not yet available to be interviewed (IE-A6). ● Initiating event frequencies reflect generic data (IE-C1). ● The ability to capture plant-specific information in the assessment of recovery actions is limited (IE-C9).
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 satisfy Capability Category III. Elements of the PRA that cannot generally meet at least Category II until later stages of design, construction and operation include the following: ● The functions and structure of the accident-sequence models reflect expectations of plant-specific operating practices, based on those of current plants (AS-A5).
Success Criteria (SC)	Success criteria reflect design-specific calculations performed using the MAAP4 and SRELAP5 computer codes. These calculations are generally equivalent to the requirements for Capability Category III. An exception is as follows: ● 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 at least Capability Category II because of the state of the design include the following: ● Since the plant has not yet been constructed, it is not possible to collect information on the as-built, as-operated systems (SY-A2). ● 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). ● Plant walkdowns cannot be conducted until the plant is constructed (SY-A4). ● The ability to address spatial and environmental hazards is limited for a plant in the design phase (SY-B8). ● There is not yet operating procedures or actual system operating experience that can be documented (SY-C2).

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.
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 at least Capability Category II include the following: ● 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-C2 through DA-C13; DA-D1 & DA-D4).
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 at least Category II include the following: ● Plant information reflecting as-built, as-operated conditions does not yet exist (IF-A3). ● Walkdowns cannot be conducted until the plant is constructed (IF-A4, IF-B3a). ● Some sources of flooding will account for plant/site-specific features not yet available (IF-B1). ● In general, conservative assumptions were made with respect to propagation pathways and areas that could be affected (IF-C1 & IF-C2).
Quantification (QU)	The quantification was performed by solving the overall core-damage model using the linked fault-tree approach. The quantification satisfies at least Category II for each of the supporting requirements.
LERF (LE)	A detailed assessment of containment response and release frequency has been conducted. The assessment satisfies at least Capability Category II for the supporting requirements, except for such aspects as system failure analysis and human reliability analysis, as addressed for technical areas SY, HF and DA above.

Table 19.1-2—Features for U.S. EPR that Address Challenges for Current PWRs
Sheet 1 of 5

Risk-Important Challenges for Current-Generation PWRs	U.S. EPR Features
Features Relating to Potential for Core Damage	
SBO ● Frequency of losses of offsite power ● Reliability of onsite emergency power ● Limited life for station batteries ● Potential for leakage from RCP seals	Reduction in potential for LOOP: ● Normal alignment of auxiliary power to switchyard (no need for fast transfer after reactor trip). ● Multiple auxiliary transformers for both safety-related and non-safety-related switchgear. ● Capability of turbine-generator runback to house loads on full-load rejection. Redundancy and diversity of onsite emergency power sources. ● Four emergency diesel-generators. ● Two SBO diesel-generators, diverse from emergency diesel-generators. ● Careful design of cross-ties: cross-ties available for selected loads important to PRA.
Response to LOCAs ● Manual action to switch to sump recirculation ● Reliability of SISs ● Need for low-pressure pumps to supply suction to high-pressure pumps during sump recirculation following SLOCA ● 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: ● IRWST eliminates need for switchover for sump recirculation. ● Low-pressure pumps not required to support MHSI suction in long term. ● Four trains of each SIS (MHSI, LHSI, and accumulators). Availability of alternative means for cooling: ● Four trains of emergency feedwater (EFW), each feeding a SG, with four-train redundancy for forced cooldown. ● 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. ● 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 5

Risk-Important Challenges for Current-Generation PWRs	U.S. EPR Features
Potential for RCP seal failure ● Reliance on CCW and service water for seal cooling and seal injection ● Operator action to trip RCPs to reduce potential for seal failure ● Materials used in seal construction	Enhanced capabilities to maintain RCP seal integrity: ● Four-train redundancy for cooling water systems, reducing likelihood of loss of thermal barrier cooling. ● Stand still seal system that serves as backup mechanical seal, reducing potential for seal LOCA-type events ● Automatic tripping of RCPs given total loss of seal cooling (thermal barrier cooling and seal injection)
Transients with total loss of heat removal ● Reliability of auxiliary feedwater systems ● Availability of means to depressurize reactor for feed-and-bleed cooling ● Reliability of operator action to initiate feed-and-bleed cooling	Improved systems for secondary heat removal ● Four-train redundancy for Emergency Feedwater ● Separate (non-safety-related) startup and shutdown feedwater system Enhanced ability to achieve feed-and-bleed cooling ● Two different means for establishing bleed paths: three PSVs or two dedicated depressurization valve trains ● Four-train redundancy for injection via MHSI ● Larger pressurizer and greater inventory in SGs provides increased time for operator response ● 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 5

Risk-Important Challenges for Current-Generation PWRs	U.S. EPR Features
SGTR ● Potential for loss of RCS inventory and development of pathway to atmosphere due to stuck-open main steam safety/relief valve ● Availability of means to cool down RCS to limit loss through broken tube ● Ability to make up to refueling water storage tank for long term inventory control	Enhanced ability to avoid challenging main steam safety valves (MSSVs) ● Four-train redundancy for emergency feedwater ● Automatic isolation of all feedwater to faulted generator ● Enhanced ability to perform partial cooldown of RCS via MSRTs Improved reliability and choices for achieving safety injection ● Four-train redundancy for MHSI and LHSI ● Enhanced ability to depressurize RCS via PSVs or dedicated depressurization valve trains
Potential for internal flooding ● Risk-Significant equipment susceptible to flooding from turbine building ● Limited separation and physical barriers between divisions of safety systems	Substantially improved protection against internal floods ● All safety trains located in separate buildings, without communication between buildings ● 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 19.1.4.1.3
Potential for internal fire ● Limited separation and fire barriers between divisions ● Limited options for response to fire in MCR ● Common location of essential cables and controls (e.g., in cable-spreading room) ● Potential for spurious operations induced by fires affecting control cables	Substantially improved protection against internal fires ● All safety trains located in separate buildings, without communication between buildings ● 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 19.1.4.1.3 ● Enhanced capability for action via remote shutdown panel in the event of MCR evacuation ● Separation and fire barriers between divisions of control and power cables ● Use of fiber optic cables eliminates potential for effects of “hot shorts” in these cables

Table 19.1-2—Features for U.S. EPR that Address Challenges for Current PWRs
Sheet 4 of 5

Risk-Important Challenges for Current-Generation PWRs	U.S. EPR Features
Impact of seismic events ● Inadequate anchorage, especially for electrical cabinets, batteries, and other equipment ● Effects of relay chatter ● Unreinforced masonry block walls ● Flooding due to failures of non-safety systems (e.g., condenser circulating water) ● Building interactions	Substantially improved protection against earthquakes ● Location of all safety systems within qualified structures ● Elimination of unreinforced masonry block walls as fire barriers ● Use of digital systems for instrument and control functions, this eliminates or reduces the electro-mechanical relays ● Elimination of potential for flooding of safety equipment due to failures in non-safety systems ● Careful attention to potential interactions between buildings
Features Relating to Containment Response and Release Potential	
Phenomena associated with high-pressure melt ejection ● Accidents proceeding to core damage at high RCS pressure ● Geometries of reactor cavities conducive to transport of core debris to containment atmosphere ● Potential for direct impingement of core debris on side wall of containment	Reduced potential for high-pressure melt ejection ● Enhanced capability for partial depressurization to prevent core damage ● Depressurization via dedicated depressurization valve trains available after onset of core damage to achieve low RCS pressure Limited potential for impact by high-pressure melt ejection ● Cavity design to direct core debris to core melt spreading area ● Limited pathways for dispersion to upper areas of containment ● Large, robust containment capable of accommodating significant loadings
Possibility of early failure due to hydrogen burns and rapid steam generation ● Accumulation of hydrogen in containment atmosphere before and immediately after vessel breach ● Blowdown prior to vessel failure ● Rapid steam generation due to interaction of core debris with water in reactor cavity	Enhanced ability to withstand early containment loadings ● Large, robust containment capable of accommodating significant loadings ● Availability of catalytic recombiners to prevent accumulation of hydrogen ● Cavity design that limits potential for energetic interaction of core melt and water

Table 19.1-2—Features for U.S. EPR that Address Challenges for Current PWRs
Sheet 5 of 5

Risk-Important Challenges for Current-Generation PWRs	U.S. EPR Features
Potential for accidents that bypass containment ● Interfacing-systems LOCAs due to exposure of low-pressure piping to RCS pressure ● Significant contribution from SGTRs	Reduced potential for core damage due to bypass events ● LHSI system designed to maintain integrity even when exposed to full RCS pressure ● Reduced potential for core damage due to SGTRs, as described above
Potential for late failure of containment ● Long term overpressurization due to lack of containment heat removal ● Potential for generation of combustible and non-condensible gases due to interactions of core-debris with containment basemat ● 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 ● Containment heat removal via four-train LHSI system, with SAHRS as long term, non-safety backup ● Provisions for active cooling of core debris to prevent molten core concrete interactions ● Availability of catalytic hydrogen recombiners ● 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
Loss of vital low-voltage AC bus	Included implicitly in 31BDA
Loss of vital DC bus	Not modeled; to be addressed when design of DC power system is finalized
Total loss of service water or component cooling	Included explicitly via several specific events representing losses of service water or CCW
Partial loss of service water or component cooling	Included explicitly via several specific events representing losses of service water or CCW
Loss of UHS	Included explicitly via several specific events representing losses of service water or CCW
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			
GTR—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, 23.7)	NUREG/CR-6928 (Reference 19)
LOC—loss of main condenser, including MSIV closure, loss of condenser circulating water, etc.	8.1E-02	Gamma (20, 247)	NUREG/CR-6928
LOMFW—total loss of main feedwater	9.6E-02	Gamma (1.33, 13.8)	NUREG/CR-6928
Loss-of-Coolant Accidents (LOCA)			
SLOCA—small LOCA (0.6 to 3-in equivalent diameter)	1.4E-03	Gamma (1.4, 1014)	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	Lognormal (EF = 16)	NUREG-1829 (Reference 44)
LLOCA—large LOCA (>6-in equivalent diameter)	1.3E-06	Gamma (0.42, 3.16E+5)	NUREG/CR-6928
SGTR			
SGTR	3.6E-03	Gamma (0.5 , 14.1)	NUREG/CR-6928
IND SGTR—SGTR induced by a steam line break	1.2E-06	Lognormal (EF=32)	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; frequency includes conditional failure of mitigation	4.2E-10 PE: 4.1E-10	Lognormal fit (EF = 55)	Lognormal fit to Design-specific fault-tree analysis
ISL-CVCS HPTR—ISLOCA due to rupture of tube in high pressure letdown cooler; frequency includes conditional failure of mitigation	1.5E-08 PE: 9.2E-10	Lognormal fit (EF = 370)	Lognormal fit to Design-specific 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 REDS—ISLOCA due to spurious opening of reducing station; frequency includes conditional failure of mitigation	1.9E-09 PE: 3.7E-10	Lognormal fit (EF = 240)	Lognormal fit to Design-specific fault-tree analysis
ISL-CVCS INJ—ISLOCA due to break in charging line; frequency includes conditional failure of mitigation	8.2E-11 PE: 6.3E-12	Lognormal fit (EF = 100)	Lognormal fit to Design-specific fault-tree analysis
ISL-SIS LHSI—ISLOCA in injection line from LHSI; frequency includes conditional failure of mitigation	2.4E-10 PE: 3.5E-11	Lognormal fit (EF = 120)	Lognormal fit to Design-specific fault-tree analysis
ISL-SIS MHSI—ISLOCA in injection line from MHSI; frequency includes conditional failure of mitigation	2.4E-10 PE: 3.5E-11	Lognormal fit (EF = 120)	Lognormal fit to Design-specific fault-tree analysis
ISL-SIS RHR—ISLOCA in RHR suction line; frequency includes conditional failure of mitigation	4.8E-11 PE: 7.9E-12	Lognormal fit (EF = 170)	Lognormal fit to Design-specific fault-tree analysis
Secondary Side Breaks			
SLBO—steam-line break outside containment (downstream from MSIV)	2.1E-03	Gamma (1.5, 728)	NUREG/CR 5750 (excluding leaks) (Reference 13)
SLBI—steam-line break inside containment	1.0E-03	Lognormal (EF = 32)	NUREG/CR 5750
MSSV—spurious opening of main steam safety valve	1.0E-03	Lognormal (EF = 32)	Frequency for SLBI applied
Support System Failures			
LOOP—loss of offsite power	1.9E-02	Gamma (0.84, 44.0)	NUREG/CR-6890 (Reference 21)
LOCCW-CH1L—leak from CCWS CH 1 or CH2 of CCWS	2.0E-01	Lognormal fit (EF = 38)	Lognormal fit to Design-specific fault-tree analysis
LOCCW1—loss of an initially operating CCWS train and failure of switchover to standby train	2.9E-03	Lognormal fit (EF = 5)	Lognormal fit to Design-specific fault-tree analysis
LOCCW12—loss of both CCWS trains serving the same CH	4.6E-03	Lognormal fit (EF = 4)	Lognormal fit to Design-specific fault-tree analysis

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
LOCCW12 PM2—loss of both CCWS trains serving the same CH, including maintenance unavailability for standby train	1.8E-02	Lognormal fit (EF = 4)	Lognormal fit to Design-specific fault-tree analysis
LOCC14-CH1—Loss of both initially operating trains and loss of cooling to 1 CH (failure to switchover)	1.8E-05	Lognormal fit (EF = 8)	Lognormal fit to Design-specific fault-tree analysis
LOCCW14-CH12—Loss of both initially operating trains and loss of cooling to both CHs (failure to switchover)	3.6E-07	Lognormal fit (EF = 50)	Lognormal fit to Design-specific fault-tree analysis
LOCCW1L—leak in an initially operating CCWS train and failure to isolate	5.3E-04	Lognormal fit (EF = 8)	Lognormal fit to Design-specific fault-tree analysis
LOCCW-ALL—total loss of CCWS (four divisions)	2.7E-06	Lognormal fit (EF = 28)	Lognormal fit to Design-specific fault-tree analysis
LBOP—loss of closed cooling water or auxiliary cooling water, resulting in a loss of balance-of-plant	5.1E-02	Lognormal fit (EF = 3)	Lognormal fit to Design-specific fault-tree analysis
31BDA—loss of one division of emergency AC power (6.9 kV switchgear 31BDA)	3.5E-02	Lognormal fit (EF = 9)	Lognormal fit to Design-specific 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 • Inventory control for LOCAs, SGTR, and feed-and-bleed cooling
Low-head safety injection (LHSI)	• Four independent trains, physically separated in different SB • Inventory control for LLOCA; backup to MHSI for small and MLOCAs, given cooldown of RCS • Cooling of IRWST inventory via recirculation • Cross-connections enhance availability during maintenance without sacrificing independence
Accumulators	• Four separate accumulators (one for each RCS cold leg) • Reflooding of core following LLOCA; additional inventory control for small and medium LOCAs
IRWST	• Single tank, integral to the containment structure • Suction source for CVCS, MHSI,LHSI and SAHR • Collects discharge from RCS (e.g., during LOCA), preventing need for change in mode for SISs • 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 • Manual backup to reactor shutdown systems
Chemical and volume control system (CVCS)	• Two-train, non-safety system • Inventory control for RCS leaks, avoiding challenges to safety systems
Stand still seal system for RCPs	• Pneumatic seal, backup to normal multi-stage seals • Deployed when RCPs trip on a loss of seal cooling
Systems Providing Heat Removal	
Main feedwater system (MFWS)	• Three -trains with motor-driven pumps; all normally in service during power operation • Continued secondary heat removal following reactor trip
Startup and shutdown system	• Single motor-driven pump • 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 • Cross-connections for pumps permit any train to draw suction from any tank, and discharge to any SG • 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 • Six main steam bypass valves on common line downstream from MSIVs • Path from any SG to any relief valve provides heat removal if MSIVs are open • PCD and FCD accomplished via MSRTs. • 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 • 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 • SAHR takes suction from IRWST • The SAHR discharge depends on the primary operating modes, which could be one of the following: • backup to LHSI for cooling of IRSWT • 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.

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 • Six non-safety trains of electrical distribution, supplied normally with offsite power from three auxiliary transformers • Four emergency diesel-generators in two separate diesel buildings • Two SBO diesel generators separated from and of diverse design with respect to the emergency diesel-generators • Continued supply of offsite power to plant auxiliaries following reactor trip, without need for fast transfer • 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) • Two trains for support of severe-accident functions, with batteries rated for 12-hr discharge
CCWS	• Four independent divisions, each housed within separate SB • 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. • 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 • 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 • 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 • Provides cooling to the SB HVAC, that includes cooling to ac and dc switchgear rooms and EFW pump rooms. • Trains 1 and 4 of Safety Chilled Water are air-cooled whereas trains 2 and 3 are cooled by the CCW common headers. • 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