Safety Evaluation Report With Open Items for the U.S. EPR

Chapter 19, "Probabilistic Risk Assessment and Severe Accident Evaluation"

CONTENTS

LIST OF FIGURES

LIST OF TABLES

19 PROBABILISTIC RISK ASSESSMENT AND SEVERE ACCIDENT EVALUATION

Chapter 19 of this report describes the Nuclear Regulatory Commission (NRC) staff review of the probabilistic risk assessment (PRA) and severe accident evaluation presented in the U.S. EPR Final Safety Analysis Report (FSAR), Chapter 19, "Probabilistic Risk Assessment and Severe Accident Evaluation."

FSAR Tier 2, Chapter 19, describes the methodologies used in performing the PRA and severe accident evaluations, and presents the analytical results and safety insights derived from those analyses. This chapter also addresses strategies for severe accident management, and identifies potential design improvements for risk reduction.

Section 19.1 documents the NRC staff evaluation of the PRA, Section 19.2 documents the NRC staff evaluation of severe accidents, and Section 19.3 provides applicable references.

19.1 Probabilistic Risk Assessment

19.1.1 Introduction

The PRA performed for the U.S. EPR is described in this section of the FSAR. The PRA consists of a Level 1 and Level 2 analysis of both internal events and external events.

FSAR Tier 2, Section 19.1.1, describes how the PRA is used in the design phase of the application to assess risk for comparison against the Commission's safety and containment performance goals.

FSAR Tier 2, Section 19.1.2 describes the quality of the PRA, including the technical adequacy of the PRA model, documentation, and maintenance of the PRA.

FSAR Tier 2, Section 19.1.3 describes the special design and operational features of the U.S. EPR that are intended to improve plant safety when compared to currently operating pressurized water reactors (PWRs).

FSAR Tier 2, Sections 19.1.4 and 19.1.5 provide the Level 1 and Level 2 PRA for internal events and external events, respectively, for operations at power; FSAR Tier 2, Section 19.1.6 provides the Level 1 and Level 2 PRA for events initiated from low power and shutdown conditions.

FSAR Tier 2, Section 19.1.7 identifies the specific applications of the PRA during the various phases of the application, construction, and operation, and FSAR Tier 2, Section 19.1.8 provides a summary of the conclusions and findings derived from the PRA.

19.1.2 Summary of Application

FSAR Tier 1: There are no FSAR Tier 1 entries for this area of review. However, the following FSAR Tier 1 sections provide information on systems that are designed to prevent the onset of, or mitigate, a severe accident and are referred to in FSAR Tier 1, Section 19.1:

- Section 2.2.4 emergency feedwater system (EFWS)
- Section 2.2.7 extra borating system (EBS)
- Section 2.3.1 combustible gas control system (CGCS)
- Section 2.3.2 core melt stabilization system (CMSS)
- Section 2.3.3 severe accident heat removal system (SAHRS)
- Section 2.4.14 hydrogen monitoring system (HMS)
- Section 2.5.3 station blackout diesel generators (SBODG)

FSAR Tier 2: The applicant has provided an FSAR Tier 2 description of the PRA, summarized here in part:

During the design phase of the U.S. EPR, the applicant utilized the PRA to assess risk for comparison against the Commission's safety goals (core damage frequency (CDF) less than 1E-4 per year (/yr) and large release frequency (LRF) less than 1E-6/yr) and containment performance goals (containment integrity be maintained for approximately 24 hours following onset of core damage for the more likely severe accident challenges and the conditional containment failure probability (CCFP) less than approximately 0.1 for the composite of all core damage sequences assessed in the PRA).

The scope of the PRA encompasses a Level 2 assessment, including an evaluation of core damage, containment response analysis, and determination of radiological release for internal and external events initiated from all plant operating modes. The application states that the detail represented in the PRA model is comparable with the level of plant design and operating detail available in the design certification phase. The technical adequacy of the PRA is assured through application of the American Society of Mechanical Engineers (ASME) PRA Standard and available NRC guidance, as referenced. A formal independent peer review of the PRA should be performed prior to its use during the plant's operation, which is captured as combined license (COL) Information Item 19.1-4 (see Table 19.1-20 of this report).

Changes in the design of the U.S. EPR plant are factored into the applicant's revisions of the PRA. Pending changes to the U.S. EPR design are evaluated for impact on the PRA. If a plant design change is determined to be significant relative to the PRA, the PRA model is updated in timely manner, without waiting for the routine update cycle; otherwise, the change will be incorporated into the next scheduled update of the PRA model.

The U.S. EPR design incorporates a number of key design and safety features derived from existing French and German reactors, which the applicant believes will result in an improved level of safety relative to the current fleet of operating PWRs. The FSAR lists specific design and operational improvements, including:

- Four trains of safety systems for increased redundancy and independence
- Standstill seal system (SSSS) to reduce the risk of a loss of coolant accident (LOCA) due to reactor coolant pump shaft seal leakage

- Full load rejection capability to reduce the chance of reactor trip and associated challenges to plant emergency power systems
- EBS for added shutdown capability in the event of failure to scram
- Large robust Containment Building designed to withstand maximum release of stored energy during severe accident conditions
- Core melt retention system designed to maintain containment integrity
- SAHRS for removing heat from containment during severe accident conditions

During the design process, the applicant utilized the PRA to identify plant system improvements for risk reduction. The applicant stated that specific improvements have been made to the SBODG design, the configuration of low head safety injection (LHSI) pump motor cooling, the reliability of the safety injection actuation signal, and diversity of SAHRS cooling water.

Initiating internal events for the Level 1 PRA are identified based on industry events, plus use of a failure modes and effects analysis (FMEA) from which accident sequence event trees are developed. The application includes analyses of plant transients, LOCA and interfacing systems LOCA, steam generator tube rupture and secondary side breaks, support system failures (including loss of offsite power), and anticipated transients without scram (ATWS) events. The application described the data utilized to characterize the events in the sequence and system models, and provided an analysis of human reliability.

The methodologies employed in the PRA are described by the applicant, including the event sequence analysis used to quantify CDF, the systems analysis codes used to model the accident phenomena, and the human reliability calculator used to quantify human failure probabilities.

The Level 1 PRA results in a calculated CDF less than 1E-6/yr. The loss of offsite power (LOOP) is the dominant contributor to CDF, followed by small LOCA (SLOCA).

The applicant maintains that PRA sensitivity analyses did not reveal any changes in plant design that would significantly reduce CDF.

The Level 2 PRA is performed using the Level 1 PRA core damage end states as its starting point. The physical phenomena associated with containment integrity are evaluated and are used to develop the containment event trees.

The Level 2 PRA results in a calculated LRF of 2.2E-8/yr and a CCFP of 0.076. The key Level 2 PRA insight is that LRF is dominated by Level 1 events that already pose a challenge to containment integrity, such as an inside containment steam line break sequence.

For external events, a PRA-based seismic margin analysis was performed by the applicant for seismic events, and the results were compared to a review level earthquake (RLE) defined to be 1.67 times the Safe Shutdown Earthquake (SSE), per NRC guidance contained in Commission paper SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs” (dated April 2, 1993, and SRM dated July 21, 1993).

Internal floods are evaluated for eight buildings that contain equipment credited in the internal events PRA with all credited equipment assumed to be lost due to the flooding. The CDF is

calculated to be less than 1E-7/yr. The LRF is calculated to be 1.1E-9/yr, and CCFP is calculated to be approximately 0.018.

Internal fires are conservatively evaluated assuming that all equipment in a fire area is lost due to the fire. The total CDF is calculated to be 1.8E-7/yr. The LRF is calculated to be 3.6E-9/yr, and CCFP is calculated to be approximately 0.02.

External flooding, fire events, and high winds events are assessed as being not significant risk contributors.

Low power and shutdown (LPSD) operating conditions are evaluated, including hot shutdown (Mode 4), cold shutdown (Mode 5), and refueling (Mode 6). The types of initiating events considered are loss of heat removal (loss of residual heat removal system) and loss of inventory events. The total CDF for the shutdown events is calculated to be 5.8E-8/yr. The LRF is calculated to be 5.7E-9/yr, and CCFP is calculated to be less than 0.1. The FSAR states that initiating events leading to loss of residual heat removal (RHR) contribute about 40 percent of the risk at shutdown conditions, with LOOP being the biggest single contributing event. The total LRF for shutdown conditions is shown to be approximately 10 percent of the LRF calculated for at-power internal events.

The FSAR identifies the following plant program and process interfaces with the PRA:

- Design Programs and Processes
- Maintenance Rule Implementation
- Reactor Oversight Process
- Reliability Assurance Program (RAP)

The applicant states that regulatory treatment of non-safety systems (RTNSS) is not required for the U.S. EPR design; therefore, no PRA interface is identified.

The application provides the following conclusions and summary of findings:

- The total CDF for internal events, internal flooding, and internal fire at power is calculated to be 5.3E-7/yr
- The total CDF for all events initiated from shutdown conditions is calculated to be 5.8E-8/yr
- The total LRF for internal events plus internal flooding and internal fire is calculated to be 2.6E-8/yr
- The total CCFP for internal events, internal flooding, and internal fire is calculated to be 0.05

For at-power internal events, the FSAR states that internal fires and floods make up 33 and 12 percent of the risk, respectively, and other internal events comprise 55 percent of the risk. The LOOP event is reported as the top contributor to at-power risk. At-power risk is shown to make up 90 percent of total plant risk.

ITAAC: There are no inspections, tests, analyses, and acceptance criteria (ITAAC) for this area of review. (ITAAC for the CGCS, CMSS, SAHRS, EFWS, EBS, SBODG, and HMS systems identified above in FSAR Tier 1 are covered in their respective FSAR sections.)

Technical Specifications: There are no technical specifications for this area of review.

19.1.3 Regulatory Basis

The relevant regulatory requirements and associated acceptance criteria for this area of review are given in NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants – LWR Edition," (SRP), Section 19.0, "Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors," Revision 2. Review interfaces with other SRP sections can also be found in Section 19.0 of NUREG-0800.

Requirements for this chapter are included in Title 10 of the *Code of Federal Regulations* (Title 10 CFR), Section 52.47(a).

1. 10 CFR 52.47, "Contents of applications; technical information," Section 52.47(a)(8): Provide the information necessary to demonstrate compliance with any technically relevant portions of the Three Mile Island (TMI) requirements set forth in 10 CFR 50.34(f), except 50.34(f)(1)(xii), f(2)(ix), and f(3)(v).

2. 10 CFR 52.47(a)(23): Provide a description and analysis of design features for the prevention and mitigation of severe accidents.

3. 10 CFR 52.47(a)(27): Provide a description of the design-specific PRA and its results.

Acceptance criteria adequate to meet the above requirements are set forth in NRC guidance documents as follows:

1. Relevant NRC policy statements published as 50 *Federal Register* (FR) 32138, "Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants," dated August 8, 1985 (specifically, Section B on new plant applications); 59 FR 35461, "Regulation of Advanced Nuclear Power Plants; Statement of Policy," dated July 12, 1994; and 60 FR 42622, "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement," dated August 16, 1995.

2. Regulatory Guide (RG) 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," and RG 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," as they relate to the scope and technical adequacy of the PRA.

3. Commission papers providing guidance on severe accident design features and the application of seismic margin analysis, specifically SECY-90-016, "Evolutionary Light-Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements" (paper dated January 12, 1990, and staff requirements memorandum (SRM) dated June 26, 1990); SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs" (paper dated April 2, 1993, and SRM dated July 21, 1993); and SECY-97-044, "Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design" (paper dated February 19, 1997, and SRM dated June 30, 1997).

4. Commission papers related to PRA quality, specifically SECY-00-0162, "Addressing PRA Quality in Risk-Informed Activities" (paper dated July 28, 2000, and SRM dated October 27, 2000), which addresses peer review, and SECY-00-0062, "Risk-Informed Regulation Implementation Plan," dated March 15, 2000, which discusses PRA standards.

19.1.4 Technical Evaluation

19.1.4.1 *FSAR Tier 2, Section 19.1.1: Uses and Applications of the PRA*

Through the review, the staff noted that for the U.S. EPR design, the applicant has used the PRA during the design phase. The scope of these uses includes the following:

- To determine how the risk associated with the design compares to the quantitative objectives established by the Commission that the CDF should be less than 1E-4/yr and that the LRF should be less than 1E-6/yr

- To determine how the risk associated with the design compares to the Commission's containment performance goals, which consist of two elements: (1) A probabilistic objective that the CCFP be less than one in 10 when weighted over credible core-damage sequences assessed in the PRA, and (2) 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 RAP

The staff confirmed that the applicant does not use the PRA for any formal risk-informed applications, such as risk-informed categorization and treatment of SSCs (10 CFR 50.69) or fire protection (10 CFR 50.48).

The staff identified COL Information Item 19.1-1 describing the uses of PRA during the COL phase as "[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."

As summarized above, the staff finds that the applicant has appropriately used and identified the uses of PRA in conformance with the SRP Chapter 19.0, Section I. The applicant has utilized PRA to identify and assess preventive and mitigative features, including operator actions, such that U.S. EPR operation will reflect a reduction in risk compared to existing operating power reactors. In addition, the applicant has also used PRA results and insights to support other programs such as the RAP and the Maintenance Rule Program, in conformance with the guidance provided in the SRP.

19.1.4.2 *FSAR Tier 2, Section 19.1.2: Quality of PRA*

The staff completed its review of the attributes of the U.S. EPR design-specific PRA to ensure the PRA is suitable for use in support of the design process and design certification. The staff issued about 30 requests for additional information (RAIs) that included approximately

370 questions to the applicant during its review of the FSAR Tier 2, Chapter 19. The staff reviewed the quality and completeness of the U.S. EPR design-specific PRA by evaluating the applicant's methods to achieve and maintain the PRA quality, including the scope, level of detail, and standards and guidance that the applicant has employed in developing a technically adequate PRA.

The staff's review of the applicant's use of models, techniques, methodologies, assumptions, data, quantification, uncertainty, sensitivity studies, and computational tools, as well as the applicant's programs and processes for ensuring quality in the PRA, included the evaluation of the applicant's responses to the RAIs that resulted from the review.

In addition, the staff audited supporting documents related to FSAR Tier 2, Chapter 19 at the applicant's facility in Rockville, Maryland. The staff audited a number of documents that describe the U.S. EPR PRA and severe accident analysis. These documents are first-tier references in FSAR Tier 2, Chapter 19 and include a level of detail higher than is required in the FSAR. The staff gained a better understanding of the basis underlying the PRA and severe accident analysis, and identified areas where additional information should be submitted to allow a licensing decision on the application. Publicly available staff reports were issued for these audits.

For the reasons described in the subsequent sections, the staff finds that the quality of the U.S. EPR design-specific PRA is appropriate with respect to scope, level of detail, and technical acceptability for its intended functions, such as supporting and improving the U.S. EPR design process, providing relative importance of sequences leading to core damage or containment failure, as well as identifying important structures, systems, and components (SSCs).

As explained in the subsequent staff evaluation, the staff finds that the U.S. EPR design-specific PRA has been developed in a manner consistent with current good practice and that the PRA elements are performed in accordance with the ASME/ANS PRA standard, which is endorsed in the appendices to RG 1.200, Revision 2. In addition, the U.S. EPR PRA appropriately reflects the dependencies of systems on one another and on operator actions, and reflects the current design to the extent needed to support the DC application. Therefore, the staff finds that the U.S. EPR design-specific PRA is of sufficient quality to be used in the following ways:

- to assess the risks associated with the U.S. EPR design
- to identify strengths and weaknesses of U.S. EPR design features
- to evaluate U.S. EPR containment failure
- to compare the risk results with the Commission's safety goal
- to provide an integrated perspective of the overall risk estimates for the design
- to identify major contributors to the estimated CDF and LRF
- to support other programs for certification purposes (e.g., RAP, Maintenance Rule Program (10 CFR 50.65))

19.1.4.2.1 PRA Scope

The U.S. EPR design-specific PRA includes an evaluation of the accidents that could lead to core damage, assessment of their frequencies, analysis of the containment response to these accidents, and characterization of the magnitude and frequencies of releases of radionuclides. The U.S. EPR design-specific PRA addresses all applicable internal and external initiating events and all plant operating modes. Most of the external events are screened from detailed analysis based on their applicability to the U.S. EPR design and in conformance with ANSI/ANS-58.21-203 with the exception of high wind, tornado, external flood, and external fire events, which are treated qualitatively. For seismic events, the applicant used PRA-based seismic margin analysis to assess the risk.

The applicant documented each element of the PRA in an evaluation report or calculation prepared according to the applicant's internal quality assurance procedures. Each PRA evaluation report was independently reviewed by the applicant's project team.

Based on the information presented above, the staff finds that the U.S. EPR design-specific PRA scope is in conformance with the SRP, and sufficient for the design certification.

19.1.4.2.2 Level of Detail

The U.S. EPR design-specific PRA was developed with the level of detail available during the design stage. The elements of the detailed design that were not available to support the U.S. EPR design-specific PRA during the design stage include:

- specific routing of piping
- routing of control and power cables
- specific location of some equipment within plant buildings
- emergency and other operating procedures

The applicant stated in the COL Information Item 19.1-9 that "[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 remain valid with respect to internal events, internal flooding, internal fire, human reliability analyses, PRA-based seismic margins, and other external events." PRA maintenance is addressed in Section 19.1.4.2.4 of this report.

Based on the foregoing, the staff concludes that the applicant's PRA is developed with a level of detail sufficient to reflect the as-designed plant and to assess the plant risk.

19.1.4.2.3 PRA Technical Adequacy

The applicant performed a self assessment of the U.S. EPR design-specific PRA against the ASME RA-Sb-2005, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," dated December 30, 2005, which the staff endorsed through RG 1.200, Revision 1, to demonstrate that its PRA is technically adequate to support the design certification. The 2005 edition of the ASME PRA Standard did not address internal fire events, external events, and low-power and shutdown modes; thus, for these events, the applicant employed the following NRC guidance to perform assessments commensurate with the uses of the PRA. As

practical, for internal fire analysis, the U.S. EPR PRA employed the guidance provided in NUREG/CR-6850, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities," dated September 2005. For seismic events, the U.S. EPR PRA followed the general approach delineated in American National Standards Institute (ANSI)/American Nuclear Society's (ANS) document Appendix B of ANSI/ANS-58.21-2003, "American National Standard External-Events PRA Methodology," dated December 2003, and SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs" (dated April 2, 1993, and SRM dated July 21, 1993). The Advisory Committee on Reactor Safeguard (ACRS) reviewed the draft version of ANSI/ANS-58.21 and documented its comments in the letter on February 9, 2001 to the Executive Director for Operations. The staff also reviewed the draft version of ANSI/ANS-58.21 and provided their comments to ANS on May 17, 2001. These standards employ seismic margin assessment techniques, which are permitted under SECY-93-087. For other external events, the U.S. EPR PRA for design certification used a screening method provided in NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities - Final Report," dated June 1991.

The staff finds that the assumptions and bounding treatment described above were applied consistent with the level of details available during the design stage. The staff reviewed FSAR Tier 2, Table 19.1-1, "Characterization of U.S. EPR design-specific PRA Relative to Supporting Requirements in ASME PRA Standard," and finds that the applicant properly characterized its findings relative to the capability categories addressed in the ASME PRA standard and reasonably described the quality state of the U.S. EPR design-specific PRA.

In addition to the self-assessment, the applicant conducted a peer review using Nuclear Energy Institute (NEI) 05-04, "Process for Performing Follow-on PRA Peer Reviews Using the ASME PRA Standard," dated January 2005, which the staff has endorsed in Appendix C of RG 1.200, Revision 2, to assess the technical adequacy of the U.S. EPR design-specific PRA. NEI 05-04 relates to ASME RA-Sc-2007, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," dated July 6, 2007. The staff audited the draft peer review report at the applicant's facility and noted the following:

- The U.S. EPR design-specific PRA peer review team consisted of seven PRA analysts, each with several years of experience in the field of PRA.

- The U.S. EPR design-specific PRA peer review was performed in three distinct phases, that is, off-site document gathering and review, on site-review and investigation, and off-site final documentation. The process consisted of a series of reviews for each ASME PRA Standard high level requirement (HLR) and supporting requirements (SRs).

- The U.S. EPR design-specific PRA peer review categorized its evaluation against the ASME PRA Standard SRs as "Met," "Not Applicable," "Not Met as Not Achievable," and, "Not Met on Basis of Technical Merit." In this compilation, an SR determined to be "Met" means that at least ASME PRA Standard Capability Category I is supported.

Note that the ASME PRA Standard presents the PRA quality requirements in three different capability levels called, "Capability Categories" I, II, and III. Table 1.3-1 of ASME RA-Sc-2005 describes the basis that was used to differentiate among the three "Capability Categories," on

the basis of the three criteria of "scope and level of detail," "plant-specificity," and "realism," with Category I being the lowest level.

In RAI 54, Question 19.01-13, the staff requested the applicant to provide the PRA peer review summary results. In a September 22, 2008, response to RAI 54, Question 19.01-13, the applicant provided (1) a summary of the supporting requirement assessment, (2) the capability category assessment of supporting requirements that are met, and (3) the fact and observation (F&O) totals as a function of PRA element. The response was constructed in a table format showing the results for all 10 technical elements that had been peer reviewed.

The results from the U.S. EPR design-specific PRA peer review show that, of the 328 written SRs, 225 SRs (68 percent) were characterized as "Met," 30 SRs (9 percent) were characterized as "Not Applicable," 41 SRs (13 percent) were characterized as "Not Met as Not Achievable," and 32 (10 percent) were characterized as "Not Met on Basis of Technical Merit." The significance of these results is discussed below.

In RAI 54, Question 19.01-14, the staff requested that the applicant identify the SRs that were classified as "Not Met as Not Achievable" and the basis of not being able to meet the standard. In a September 22, 2008, response to RAI 54, Question 19.01-14, the applicant provided a table showing all 41 SRs identified as "Not Met as Not Achievable" and provided the peer review team assessment that justified its conclusion. The main reasons for the assignment of being "Not Met as Not Achievable" identified by the peer review team are related to the unavailability of plant-specific data, detailed design information, procedures, and as-built walkdowns and confirmations.

In RAI 54, Question 19.01-15, the staff requested additional information on the SRs that were characterized as "Not Met on Basis of Technical Merits" and the resolutions of the F&Os generated by the peer-review team. In a September 22, 2008, response, the applicant specifically identified, explained, and outlined the disposition of these SRs and the corresponding F&Os prepared for these SRs. The applicant also provided a summary result from the PRA impact assessment corresponding to the F&O prepared for each SR.

For the 32 "Not Met on Basis of Technical Merit" SRs, the findings associated with each SR were evaluated and grouped into one of the following classes:

- Documentation: Twenty of the 32 "Not Met on Basis of Technical Merits" SRs were evaluated as "Not Met" due to incomplete PRA documentation.

- Limited Information: Nine of the 32 "Not Met on Basis of Technical Merits" SRs were evaluated as "Not Met" because only partial information was available at the design stage.

- Incomplete Model: Three of the 32 "Not Met on Basis of Technical Merits" SRs were evaluated as "Not Met" because of technical issues. The applicant identified the issues as follows:

    - SR IE-B3 – The PRA assumed that the plant response to a feed water line break (FWLB) is sufficiently similar to the response to the steam line break (SLB). The FWLB should be considered more of an over heating event and could challenge the safety valves, which potentially stick open. However, SLB is more of an overcooling event.

- SR IE-C3- The feed water line break frequency is not included in the steam line break frequency as assumed in SR IE-B3.

- SR IF-F3 – Some of the flood specific parameters associated with the internal flooding event in the annulus are missing uncertainty distributions.

The applicant further analyzed these three findings and determined that none of these findings would have a significant impact on the PRA results and insights.

In RAI 6, Question 19-119, the staff requested that the applicant provide the results of the Level 2 PRA peer review. In an August 8, 2008, response to RAI 6, Question 19-119, the applicant described this portion of the peer review. Specifically, as part of the overall review, the peer team reviewed the Level 2 PRA as part of the Large Early Release Frequency (LERF) element. There are seven ASME HLRs for LERF. The seven HLRs are further broken down into 42 SRs. Of these 42, 38 SRs were "Met" and 4 were "Not Met." For those SRs that were designated "Not Met," the applicant indicated that the principal reason was the unavailability at this stage of design of required plant-specific design information.

Item 4d in Interim Staff Guidance (ISG) Design Certification (DC)/COL-ISG-3, "PRA Information to Support Design Certification and Combined License Applications," dated June 2008, states that "Peer review of the DC PRA is not required prior to application." The staff observes that the applicant has chosen to conduct the peer review of the U.S. EPR PRA, which include obtaining insights of the degree to which the U.S. EPR PRA relates to the capability categories for the technical elements addressed in the PRA Standard. Although the staff has had an opportunity to examine the draft peer review report at the applicant's office and the report greatly assisted the staff in its review, the staff did not rely solely on the results of the peer review for its conclusion on the quality of the U.S. EPR PRA. The results of the peer review have only been used to provide the staff an added level of confidence in the U.S. EPR PRA models, results, and insights.

To ensure that the U.S. EPR PRA is of sufficient quality to support risk-informed applications, the staff identified COL Information Item 19.1-4 which states that "[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 staff finds that, as described above and in the following sections, the applicant has reasonably demonstrated that the U.S. EPR PRA is of sufficient technical quality and is adequate in terms of scope, level of detail, and technical acceptability to support the design certification application. For those aspects of the PRA identified by the staff or by the peer review team that deviated from accepted good practices, the applicant has justified that these deficiencies do not impact the PRA results or risk insights. For the staff's findings and peer review F&Os, the applicant has either modified the PRA or justified that these findings would have insignificant impacts on the U.S. EPR PRA. Therefore, the staff finds that the quality of the U.S. EPR design-specific PRA is adequate for supporting the U.S. EPR design certification.

19.1.4.2.4 PRA Maintenance and Upgrade

The applicant specified that the U.S. EPR design-specific PRA model and supporting documentation are maintained and updated consistent with the PRA Standard ASME RA-Sc-2007, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," and RG 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk

Assessment Results for Risk-Informed Activities," so that they continue to reflect the as-designed characteristics of the plant. The applicant indicated that a process is being implemented to perform the following:

- 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

In RAI 172, Question 19-270, the staff requested additional information on the process for performing timely PRA updates. In a February 13, 2009, response, the applicant stated that, when reviewing pending design changes and model improvements, the impacts on CDF and LRF would be estimated. Based on the estimated impact, the applicant will take one of the following approaches:

- If the effects of the change(s) since the last PRA model update are such that the PRA no longer reasonably reflects as-designed and as-to-be-built SSCs, and as-to-be operated conditions, then a PRA model update is implemented without waiting for the routine update cycle.
- 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 the 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 or control potential cumulative modeling impacts.

The applicant stated in the COL Information Item 19.1-5 that "[a] COL applicant that references the U.S. EPR design certification will describe the applicant's PRA maintenance and upgrade program."

Since the applicant committed to update and upgrade the U.S. EPR design-specific PRA to reflect plant modifications on a frequent and timely basis if there are changes to the design, the staff finds the applicant's PRA maintenance and upgrade program to be practical and consistent with the Statement of Consideration [72 FR 49405] which states that the Commission intends PRA maintenance and PRA upgrade to be consistent with how they are defined in the ASME RA-Sc-2007 PRA Standard.

19.1.4.2.5 PRA Update and Enhancements

The U.S. EPR design-specific PRA represents the state of the design as submitted for certification, except that the U.S. EPR design-specific PRA model is an evolving model. Accordingly, some design changes will be addressed in future revisions to the PRA model.

In RAI 289, Question 19-329, the staff requested additional information related to the applicant's plans to incorporate these design changes, as well as any potential future changes, in the PRA. Item 8 in ISG DC/COL-ISG-3 states that "PRA maintenance should commence at the time of application for both DC and COL applicants. This means that the PRA should be updated to reflect plant modifications if there are changes to the design." In addition, 10 CFR 52.47(a)(27) states that the design certification FSAR includes a "description of the design-specific [PRA] and its results." Therefore, the staff expects that the PRA be maintained during the application process such that it remains design-specific and that the FSAR at the time of certification describes this design-specific PRA. This process ensures that integrated effects of individual changes are reviewed by the staff and that the FSAR reflects both qualitative and quantitative (e.g., importance ranking) insights related to the design. The applicant was asked to describe the method of tracking items for which PRA updates are needed (e.g., design changes, peer review findings, model errors). The staff also requested that the applicant discuss when the next routine update of the PRA (and, as needed, to the FSAR description of the PRA and presentation of results) is planned, and at what point the revised detailed documentation will be available for the staff to audit.

RAI 289, Question 19-329, associated with the above request, is being tracked as an open item.

Design changes to be addressed in future revisions to the PRA model are described below. Each design change has been evaluated by the applicant to determine whether significant changes to the PRA results and insights would be expected when the individual change is incorporated.

19.1.4.2.5.1 *Modification of Manual Actuation of Safety Systems*

This change will remove the direct linkage of system-level manual actuations from the safety information and control system (SICS) to the priority actuation and control system (PACS) and will route the system-level manual actuation signals through the Protection System (PS). Component-level actuations will be provided via the process automation system/diverse actuation system (PAS/DAS).

The applicant indicates that this design change will warrant modeling of PS dependence with the appropriate human actions. If the PS fails, component-level actuations, which may take longer to perform, will be necessary; and the human error probabilities (HEPs) for these actions would be expected to increase. However, only cutsets that involve a PS failure would be affected. The staff reviewed the cutsets provided by the applicant in a July 16, 2009, response to RAI 227, Question 19-285, and determined that PS failures appear in cutsets that contribute a very small fraction of total at-power CDF. Therefore, the staff concludes that this individual change will not significantly impact the PRA results and conclusions.

19.1.4.2.5.2 *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.

Regarding the impact on PRA, this change induces a revision to the common-cause failure (CCF) model in the PS fault trees to account for the functional dependence. The applicant states that this change neither improves nor worsens the PRA results, because the CCF model does not distinguish between four channels of the same parameter and eight channels of the same parameter. The applicant states that 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. The applicant indicates further that this design change does not impact the functional diversity that is provided by other trip parameters. The staff finds the applicant's assessment to be consistent with the description of the PRA model and concludes that this individual change will not significantly impact the PRA results and conclusions.

19.1.4.2.5.3 *Steam Generator Tube Rupture Mitigation Response*

This design change removes the signal for 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 a SG tube rupture (SGTR), automatic PCD will occur with safety injection system (SIS) actuation on low RCS pressure. This design change also modifies the timing of isolation of the affected SG and main steam relief train (MSRT) reset (on high SG level or high SG activity) to coincide with PCD initiation rather than waiting for PCD to finish.

The applicant evaluated the potential impact of this design change on the PRA. Relative to the first part of this design change, the applicant states that 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. The applicant's analyses show that the low RCS pressure setpoint will be actuated eventually, even if CVCS is running. Furthermore, the applicant states that 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.

For the second part of this design change, the applicant states that 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. The applicant states that early isolation also minimizes secondary side contamination, and reduces offsite releases during cooldown. Further, the applicant states that, 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.

The first part of this change affects only a backup action. The second part of this change is expected to reduce containment bypass because less reactor coolant would be lost through the ruptured tube. Therefore, the staff concludes that the impact, if any, of this individual change on the PRA results and conclusions would be beneficial (i.e., risk would be reduced).

19.1.4.2.5.4 *Emergency Feedwater Flow Control via Safety Automation System*

The initiation signal for EFWS is generated by the PS. In this design change, flow control following actuation is performed by the safety automation system (SAS).

The applicant states that the flow control valve in each EFWS train (separate from the level control valve) is normally partially closed to protect against overfeed in the case of a steam line

break. In order to achieve the full credited EFWS flow, the flow control valve must open. Independent or common-cause failures of these valves to open (including SAS failure) are not currently included in the model. The staff reviewed the independent and common-cause failure probabilities of the EFWS pumps, motor-operated valves (MOVs), and the SAS trains. The staff has determined that SAS failure is much less likely than pump failure. Further, the CCF probability of the MOVs could be comparable to the CCF probability of the pumps. The staff reviewed the cutsets provided by the applicant in a July 16, 2009, response to RAI 227, Question 19-285, and determined that EFWS pumps appear in cutsets that contribute a very small fraction of total at-power CDF. Based on this information, the staff concludes that these additional EFWS failure modes would not significantly impact the PRA results and conclusions.

19.1.4.2.5.5 *Station Blackout 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 station blackout (SBO) buses to Divisions 2 and 3.

The PRA model credits alternate feed from Division 1 to Division 2 and from Division 4 to Division 3 in SBO conditions and in non-SBO conditions. The applicant states that this change affects only how these functions will be executed, not their availability or the context in which they are performed. The staff considers it reasonable to assume that operator actions, which the applicant states dominate the failure probability of the functions, would not be significantly affected by this change given that equipment availability and factors that shape human performance (i.e., “the context” stated by the applicant) are not expected to change. Therefore, the staff concludes that this individual change will not significantly impact on the PRA results and conclusions.

19.1.4.2.5.6 *Thermal Barrier Cooling from Component Cooling Water System Common Headers*

In RAI 26, Question 19-164, the staff requested clarification of the PRA model for cooling of the reactor coolant pumps (RCPs) by the component cooling water system (CCWS) common headers. In a September 25, 2008, response to RAI 26, Question 19-164, the applicant indicated that either the Common 1b or 2b headers of CCWS could provide thermal barrier cooling to all four RCP seals. However, the PRA model assumes that common header 1b cools the thermal barriers of RCPs 1 and 2, and common header 2b cools the thermal barriers of RCPs 3 and 4. This discrepancy was not originally discussed in FSAR Tier 2, Section 19.1.2.4. In RAI 138, Question 19-247, the staff requested that the applicant evaluate the impact of this design change on the PRA results and insights, and revise the FSAR accordingly. In a December 19, 2008, response, the applicant provided the following text for inclusion in the FSAR:

> 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.

The staff confirmed that Revision 1 of the U.S. EPR FSAR, dated May 29, 2009, contains the changes committed to in the RAI response.

In the response to RAI 138, Question 19-247, the applicant also stated that fires and floods were modeled with conservative assumptions to show that a more detailed evaluation would not change the conclusion that overall CDF and LRF meet the U.S. EPR design objective. Subsequently, the applicant revised the sensitivity study to correct an error and remove asymmetries in the model. The numerical results of the sensitivity case were updated in a September 1, 2009, response to RAI 257, Question 19-316(i). The staff reviewed the results presented in the responses to RAI 138, Question 19-247, and RAI 257, Question 19-316(i), which show that the design change would reduce overall CDF and LRF. The staff agrees that this design change would reduce overall CDF and LRF. Accordingly, the staff agrees that the absolute CDF and LRF will continue to be below the established thresholds when this design change is incorporated in the PRA.

In RAI 197, Question 19-279, the staff requested a more detailed description of the planned PRA changes. In an April 10, 2009, response, the applicant clarified that this design change affects the seal LOCA contribution to the internal events, fire, and flooding CDF. Additionally, the applicant provided revised values of the seal LOCA contribution in a September 1, 2009, response to RAI 257, Question 19-316(i). The staff confirmed that in Revision 1 of the U.S. EPR FSAR, dated May 29, 2009, the applicant amended Table 19.1-108, "U.S. EPR PRA Based Insights," to indicate that the seal LOCA contribution to fire and flood CDF was reduced. This qualitative statement was not affected by the updated values provided in the response to RAI 257, Question 19-316(i). The applicant stated that the PRA and input to other programs will be updated in accordance with the maintenance and update process described in FSAR Tier 2, Section 19.1.2.4, which the staff finds adequate as set forth in Section 19.1.4.2.4 of this report.

19.1.4.2.5.7 *EFWS Header Isolation*

The EFWS design documented in Revision 0 of the FSAR included normally open valves connecting the suction piping from all four EFWS storage pools, meaning that a leak in a single pool or pipe could disable the entire EFWS. This design was reflected in the event tree top event "EFWS PBF" "(EFWS pressure boundary failure)." For success of this top event, FSAR Tier 2, Section 19A stated that four of four pools must maintain integrity or the operators must maintain inventory after the leak.

In RAI 83, Question 10.04.09-1, the staff requested information related to physical separation of the EFWS trains. In a December 29, 2008, response, the applicant described a change to the EFWS design to include normally closed supply header isolation valves. Operator action outside the control room is now needed to open the valves, but two pools provide sufficient inventory for more than 6 hours. The staff's assessment of this design change is addressed in Section 10.4.9 of this report.

In RAI 197, Question 19-274, the staff requested that the applicant evaluate the design change and either incorporate it in the PRA or discuss it in FSAR Tier 2, Section 19.1.2.4. In an April 10, 2009, response, the applicant provided the following text for inclusion in the FSAR:

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.

The staff confirmed that Revision 1 of the U.S. EPR FSAR, dated May 29, 2009, contains the changes committed to in the RAI response.

In a sensitivity study, the applicant included the two operator actions described above (i.e., train interconnection and tank refill), resulting in a total CDF increase by five percent, with the most effect seen in the internal events and internal flooding models. The increase is tied to the new operator actions, but the vulnerability of the interconnected tanks has been removed from the design, representing a qualitative safety improvement. In addition, failure of a single EFWS tank is no longer expected to be as significant a contributor.

In RAI 227, Question 19-296, the staff requested additional information related to the operator action needed to refill an EFWS tank. In a July 6, 2009, response to RAI 227, Question 19-296, the applicant clarified that the operator can refill an EFWS tank using either the demineralized water distribution system (DWDS) or the fire water distribution system (FWDS), a task that is expected to be moderately complex and performed under high stress. Equipment failures of the DWDS and FWDS are not included for this scenario, because five 100-percent pumps are available and are not expected to fail by a common cause.

In RAI 227, Question 19-297, the staff requested the applicant to provide EFWS fault trees that show the planned changes to the model. In a July 6, 2009, response, the applicant provided preliminary fault trees for the interconnection and tank refill operations. The staff reviewed the description provided by the applicant and the preliminary fault trees. The staff concludes that the planned approach is consistent with the rest of the internal events PRA, and is, therefore, acceptable.

19.1.4.3 *FSAR Tier 2, Section 19.1.3: Special Design/Operational Features*

FSAR Tier 2, Section 19.1.3, "Special Design/Operational Features," addresses the design and operational features intended to improve plant safety, thus reducing risk when compared to currently operating nuclear power plants. This information relates to two acceptance criteria from SRP Section 19.0, as summarized below:

- For designs that have evolved from the technology of currently operating plants, the results of the PRA should indicate that the design represents a reduction in risk compared to operating plants. The staff should perform a broad (qualitative and quantitative) comparison of risks, by initiating event category, between the

proposed design and operating plant designs to identify the major design features that contribute to the lower risk of the proposed design compared to existing designs.

- The staff should determine that the applicant has adequately demonstrated that the design properly balances preventive and mitigative features.

19.1.4.3.1 Reduction of Risk Compared to Operating Plants

FSAR Tier 2, Section 19.1.3 primarily provides information to support the acceptance criterion described above, that the design represents a reduction in risk compared to operating plants. To demonstrate this reduction in risk, the applicant created Table 19.1-2 in the FSAR Tier 2, "Features for U.S. EPR that Address Challenges for Current PWRs [Pressurized Water Reactors]." These challenges are taken from NUREG-1560, "Individual Plant Examination [IPE] Program: Perspectives on Reactor Safety and Plant Performance," dated December 1997, and NUREG-1742, "Perspectives Gained from the Individual Plant Examination of External Events (IPEEE) Program," dated April 2001. These reports summarize the insights gained from the IPE and IPEEE evaluations performed in response to Generic Letter (GL) 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities," dated November 23, 1988, and its supplements. The challenges listed in this table are discussed below, with references to other portions of this safety evaluation that address the topics in further detail.

19.1.4.3.1.1 *Station Blackout*

The availability of alternating current (ac) electrical power is essential for the safe operation and accident recovery of nuclear power plants. A total loss of ac power as a result of complete failure of both offsite and onsite ac power sources (that is, offsite power and the emergency diesel generators (EDGs)) is referred to as an SBO. The existing PRAs of currently operating plants indicate that accidents initiated by a loss of all ac power contribute more than 70 percent of the total CDF at some plants. In typical SBO situations, the affected plant must achieve safe shutdown by relying on components that do not require ac power. Additionally, failure of RCP seal cooling during an SBO can result in a LOCA through the seals without active injection available to cool the core. Thus, seal failure probabilities, direct current (dc) battery depletion times, and characteristics of offsite power restoration have historically been important contributors to SBO risk.

The U.S. EPR design incorporates several features designed to reduce the likelihood of a LOOP. The ac power design provides normal power to plant systems through multiple transformers in the switchyard, removing the requirement for a fast transfer from generator power to offsite power (thereby a possible LOOP caused by fast transfer failure) after a turbine trip. Additionally, the U.S. EPR reactor and turbine are designed to automatically run back after a full load rejection caused by a grid-centered LOOP, allowing the main generator to supply plant loads and avoiding a reactor trip.

The U.S. EPR design also incorporates features designed to improve the onsite ac power supply. The design includes four EDGs, reducing the impact of any single EDG failure on overall risk. However, CCF of four EDGs is still a risk-important failure (as identified in the discussion of importance studies below). To reduce the importance of a CCF of all four EDGs, two SBODGs were added to the design. The applicant states that the SBODGs are independent and diverse from the EDGs, and are assumed not to fail for the same reason as a common-cause EDG failure. This assumption is important to overall risk, as demonstrated by the discussion of sensitivity studies in the evaluation of FSAR Tier 2, Section 19.1.4.1.

In RAI 26, Question 19-162, the staff requested that the applicant provide additional information on the diversity between the EDGs and the SBODGs. In an August 15, 2008, response, the applicant committed to revise the FSAR to state that the EDG and SBODG diversity is based on their "different model, control power, HVAC, engine cooling, fuel system, [and] location." The applicant also committed to include this diversity assumption as Item 5 in FSAR Tier 2, Table 19.1-108, "U.S. EPR PRA Based Insights." The staff confirmed that Revision 1 of the U.S. EPR FSAR, dated May 29, 2009, contains the changes committed to in the RAI response. The design of the EDG and SBODG systems is evaluated in Sections 8.3 and 8.4 of this report, and the staff's evaluation of the PRA implications is documented in the evaluation of FSAR Tier 2, Section 19.1.4.1.

19.1.4.3.1.2 *Response to Loss-of-Coolant Accidents*

The U.S. EPR design also incorporates features that support an improved response to postulated LOCAs. These features mainly relate to recirculation of cooling water and depressurization of the reactor coolant system (RCS). The U.S. EPR response to LOCAs is discussed in more detail in the evaluation of FSAR Tier 2, Section 19.1.4.1.

Many current plants depend on manual switchover to sump recirculation supply to emergency core cooling system (ECCS) pumps when the refueling water storage tank (RWST) inventory nears depletion. The U.S. EPR has an in-containment refueling water storage tank (IRWST), as described in FSAR Tier 1, Section 2.2.2, and FSAR Tier 2, Chapter 6. The IRWST has a minimum water volume controlled by technical specifications (TS) and provides a water source for the SIS, SAHRS, and CVCS. Reactor coolant that exits in the RCS during a LOCA drains to the IRWST through four openings in the containment heavy floor. The injection source for the ECCS pumps is always the IRWST, and a switchover is not necessary. Therefore, the operator action to perform the switchover (or system components, important for current plants where the switchover is automated) is not a contributor to the U.S. EPR risk.

Also, the U.S. EPR design provides the ability to depressurize the RCS to allow medium head safety injection (MHSI) and LHSI system operation following a LOCA for which RCS pressure remains high. The MSRTs are used to perform an automatic partial cooldown, as described in FSAR Tier 2, Section 7.3.1.2.4. After an SIS signal, the pressure setpoint required to open the main steam relief isolation valves (MSRIVs) is lowered according to a predefined cooldown gradient. The MSRIVs open and the main steam relief control valves (MSRCVs) modulate to maintain SG pressure at the setpoint. The partial cooldown actuation signal is required to be available by TS (Limiting Condition for Operation (LCO) 3.3.1, Table 3.3.1-2). This automatic partial cooldown allows MHSI to inject and eliminates the need to depressurize manually to allow safety injection. If MHSI fails, a manual fast cooldown is possible. The staff issued RAI 7, Question 19-60, requesting that the applicant provide additional information on the fast cooldown operation. In a June 16, 2008, response, the applicant clarified that the fast cooldown involves opening the MSRT pathways on all four SGs, and that two of the four trains of steam relief and secondary cooling (via the startup and shutdown feedwater system (SSS) or EFWS) must function for success following a small LOCA.

19.1.4.3.1.3 *Potential for Reactor Coolant Pump Seal Failure*

Another important risk contributor at current plants is the potential for RCP seal failure on a loss of seal cooling, leading to a LOCA. When the loss of seal cooling is caused by a station blackout (as discussed above), safety injection to restore RCS inventory may not have the power needed to function. Therefore, the U.S. EPR design includes improvements to reduce

the likelihood of RCP seal failure. RCP seal failures are discussed in more detail in the evaluation of FSAR Tier 2, Section 19.1.4.1.

The major design improvement in the U.S. EPR relative to current plants is the SSSS. As described in FSAR Tier 2, Section 5.4.1.2.1, the standstill seal is a metal-to-metal contact activated by compressed nitrogen when either seal cooling is lost, or the shaft seals fail, or a station blackout occurs. In RAI 7, Question 19-56, the staff requested additional information on the seal failure model, including the assumed SSSS failure probability. In a June 16, 2008, response, the applicant clarified that the SSSS failure probability is assumed to be 1.0E-3. In RAI 53, Question 19-206, the staff requested that the applicant describe the SSSS actuation signals and provide additional supporting information for the assumed SSSS failure probability. In a September 22, 2008, response, the applicant provided additional information on the actuation signals, specifically stating that automatic actuation is caused by detection of total loss of seal cooling and failure of RCP seal numbers 1 and 2. The applicant also provided additional justification for the failure probability, clarifying that the valves and support systems for the SSSS are modeled explicitly, and that the 1.0E-3 failure probability includes only failure of the mechanical seal itself. This information shows that the SSSS model is detailed enough to reflect the design, includes a failure probability that is acceptable as a screening value at the design stage (and can be updated as plant experience is obtained), and it does not omit the effect of support system failures. Therefore, the staff concludes that the modeling approach is acceptable.

Also, cooling to the RCP seals is provided by independent and diverse means. CCWS provides cooling to all four RCP thermal barrier heat exchangers via either the 1.b or 2.b common headers. The four CCWS pumps can supply these common headers; if one CCWS or essential service water system (ESWS) train fails, an automatic switchover allows cooling of the common headers using the available train (FSAR Tier 2, Section 9.2.2.3.1). Multiple trains of CCWS represent an improvement over current plants for thermal barrier cooling. However, as stated in a June 16, 2008, response to RAI 7, Question 19-58, the PRA currently assumes that common header 1.b provides thermal barrier cooling to RCPs 1 and 2, and common header 2.b provides cooling to RCPs 3 and 4. As discussed above, this item has been added to the list in FSAR Tier 2, Section 19.1.2.4 of design changes not yet incorporated in the PRA. Once the design change is incorporated in the PRA, the seal LOCA contribution to CDF would decrease significantly, as described above in Section 19.1.4.2.5.6 of this report. **RAI 289, Question 19-329, which was discussed previously, is being tracked as an open item**.

As in current plants, CVCS also provides seal injection to the RCPs via the charging pump; one pump is normally operating and a standby pump is available (FSAR Tier 2, Section 9.3.4.2.2). If all cooling to the RCP shaft seal is lost, the pressure boundary is maintained by an automatic trip of the affected RCP with automatic closure of the standstill seal and the associated leak-off lines to and from each seal stage after the RCP has stopped (FSAR Tier 2, Section 5.4.1.2.1).

19.1.4.3.1.4 *Transients with Total Loss of Heat Removal*

In current plants, auxiliary feedwater (AFW) is used to remove heat from the RCS via the SGs. If AFW fails, the operators can initiate feed-and-bleed cooling of the primary system via safety injection and the remote manual opening of one or more power-operated relief valves (PORVs). Both AFW and feed-and-bleed failures have been significant contributors to overall plant risk in current plant PRAs. Therefore, the U.S. EPR design includes several improvements to enhance both secondary heat removal reliability and feed-and-bleed cooling.

The U.S. EPR design includes four trains of EFWS housed in separate buildings, each with a water storage pool that is part of the SB structure (see FSAR Tier 2, Section 10.4.9). Both supply and discharge headers allow cross-connection between trains. This design reduces the impact of any single EFWS train failure on overall risk compared to the currently operating plants, where, operator action is required to interconnect the normally isolated EFWS trains when one train fails, to ensure that adequate water inventory is available for injection.

Also, the U.S. EPR design includes the SSS, an additional startup motor-driven feedwater pump (see FSAR Tier 2, Section 10.4.7). This pump is used to provide feedwater to the SGs until approximately five percent load, when the main feedwater (MFW) pumps are started. During normal operation, it is set to start on failure of all MFW pumps. The SSS is credited in the PRA to provide SG inventory makeup for events that require heat removal via the SGs.

Finally, the ability of the operators to provide feed-and-bleed cooling of the RCS is improved compared to current plants. The primary depressurization system (PDS) includes three pressurizer safety relief valves (PSRVs) and two severe accident depressurization valves (SADVs). These diverse sets of valves are available to establish a bleed path, where current plants may have only two PORVs. Also, the four trains of safety injection reduce the impact of any single train failure on overall risk. The IRWST improvement related to LOCA response described above also improves the ability to feed and bleed.

Failures of the EFWS and safety injection systems remain important in the U.S. EPR design-specific PRA model. These failures are discussed more in the evaluation of FSAR Tier 2, Section 19.1.4.1.

19.1.4.3.1.5 *Steam Generator Tube Rupture*

The primary safety significance of SGTR events is the potential for a direct path for a loss of radioactive coolant from the RCS through the SG to outside the containment. Other systems that penetrate the containment and interface with either the RCS or the containment have two containment isolation valves that close automatically or are locked closed. The SG safety and atmospheric valves open automatically and, as required by the ASME Code, the safety valves cannot be isolated. An SGTR could also increase the probability of core damage. because the reactor coolant leaking from a SG tube cannot be recirculated. SGTR events are discussed in more detail in the evaluation of FSAR Tier 2, Section 19.1.4.1.

To address the risks associated with SGTR, the U.S. EPR design includes an MHSI system with a pump shutoff head below the pressure at which the main steam safety valves (MSSVs) are designed to open. FSAR Tier 1, Table 2.2.3-3 states that the maximum shutoff head of the MHSI pump with the large miniflow line closed is 9.7 MPa (1,407 psia). According to TS, the lift setpoints for the two MSSVs must be between 9.764 MPa (1,416.2 psig) and 10.368 MPa (1,503.8 psig) for the first valve and between 9.965 MPa (1,445.3 psig) and 10.581 MPa (1,534.7 psig) for the second valve (Surveillance Requirement (SR) 3.7.1.1). Therefore, once the reactor has depressurized to allow MHSI operation, the potential for a release from the RCS through an MSSV is reduced.

As discussed in FSAR Tier 2, Section 7.3.1.2.14, the SG containing the tube rupture is isolated if signals are present for both a partial cooldown (discussed above), and either high SG water level or high main steam activity. The SG isolation signal increases the MSRT opening setpoint; closes the main steam isolation valves (MSIVs) bypass valves, and SG blowdown valves; and isolates MFW, EFWS, and the SSS. Although current plants may have a feedwater isolation signal on high-high SG level (an example is included in NUREG-1431, “Standard Technical

Specifications: Westinghouse Plants," dated December 2005), operator action is often required to isolate the affected SG. This automatic isolation represents an earlier and more complete action and therefore a design improvement.

The improvements related to LOCA response discussed above (i.e., IRWST and means of depressurization) also improve the ability to mitigate an SGTR. In addition, the ability to depressurize the RCS via the depressurization valves mentioned above provides another mechanism to reduce pressure and allow safety injection following an SGTR.

19.1.4.3.1.6 *Potential for Internal Flooding*

At the time of the IPEs, several PWRs were vulnerable to internal flooding, especially from the Turbine Building (TB). To minimize the risk from internal flooding, the U.S. EPR design includes physical separation of the four divisions of safety systems. FSAR Tier 2, Section 3.4.1 provides more information on internal flooding protection. Specifically, walls below the 0-foot elevation have no doors and a minimal number of penetrations, separating the divisions and providing flood barriers. Above the 0-foot elevation, doors between divisions are watertight and certain openings direct water flow to the lower building levels in the same division. In the Reactor Building (RB), water is stored at the lower level of the annulus and in the IRWST with a maximum level below safety-related SSCs. The staff's evaluation of FSAR Tier 2, Section 19.1.5.2 relates to the internal flooding risk assessment.

19.1.4.3.1.7 *Potential for Internal Fire*

As part of the IPEEE, a majority of nuclear power plants identified improvements to reduce fire risk. These plants improved operational procedures and training; improved maintenance procedures; and upgraded safety systems, support systems, and fire protection systems. Similar to the approach to internal flooding described above, the U.S. EPR design reduces fire risk by designing divisional separation into the layout of the plant. Also, the digital instrumentation and control (I&C) design includes fiber-optic wiring that reduces the likelihood of hot shorts and spurious actuation of equipment, which are important issues at current plants. The fire protection strategy for the U.S. EPR is described in detail in FSAR Tier 2, Section 9.5.1. The staff's evaluation of FSAR Tier 2, Section 19.1.5.3 below relates to the internal fire risk assessment.

19.1.4.3.1.8 *Impact of Seismic Events*

The U.S. EPR design also includes improvements to reduce the impact of seismic events. Two examples of these improvements are related to block walls and electromagnetic relays.

Seismic risk assessments of current plants identified block walls as significant contributors to seismic risk or controlling elements in the derivation of the maximum seismic acceleration that results in a HCLPF. Unreinforced masonry block walls can fall and impact safety-related equipment. FSAR Tier 2, Section 3.8.4.1.10 states that no masonry walls are used in Seismic Category I structures of the U.S. EPR. Therefore, block walls are not a seismic risk contributor for the U.S. EPR.

At current plants, a large number of relays are used to control devices such as pumps, valves, and circuit breakers. In addition, much of the control logic for system initiation and control is accomplished with relays. Therefore, seismic-induced relay chatter, or the opening and closing of relay contacts because of seismic acceleration, can cause a loss of equipment or indication.

Because the U.S. EPR uses digital I&C, the number of electromechanical relays and, therefore, the seismic risk impact is significantly reduced.

The staff's evaluation of FSAR Tier 2, Section 19.1.5.1 below relates to the seismic risk assessment.

19.1.4.3.1.9 *Phenomena Associated with High-Pressure Melt Ejection*

Direct containment heating (DCH) refers to the process whereby, under certain accident scenarios, molten core debris is ejected under high pressure from the reactor vessel into the containment atmosphere. The subsequent rapid heating of the containment atmosphere, in conjunction with possible hydrogen combustion, can lead to early containment failure. DCH was identified as one of the important contributors to early containment failure for PWRs in NUREG-1150, "Severe Accident Risks: an Assessment for Five U.S. Nuclear Power Plants," dated December 1990, and in the IPEs.

In the U.S. EPR design, multiple approaches to depressurize the RCS are available, as discussed above in Section 19.1.4.3.1.2 of this report. This capability reduces the probability of core damage while the RCS is at high pressure. If high-pressure melt ejection does occur, the containment design includes a core melt spreading area and limited pathways for dispersion of debris to the upper containment. Additionally, the containment can withstand a significant pressure and temperature transient; as stated in FSAR Tier 2, Section 3.8.1.1, the containment is designed for an internal pressure of 0.4275 MPa (62 psig) and a maximum temperature of 154 degrees Celsius (°C) [309.2 degrees Fahrenheit (°F)]. Further discussion of high-pressure melt ejection is provided in FSAR Tier 2, Section 19.2.3.3.4.

The staff's evaluation of the U.S. EPR design features for severe accident mitigation, including avoidance of high-pressure melt ejection, is presented in the evaluation of FSAR Tier 2, Section 19.2.3 below.

19.1.4.3.1.10 *Possibility of Early Failure due to Hydrogen Burns and Rapid Steam Generation*

Another issue assessed at current plants is the potential for early containment failure because of hydrogen burns or rapid steam generation after core damage. Hydrogen is generated during a severe accident, chiefly because of fuel cladding oxidation, and can burn or explode if not properly controlled. Also, if water from a LOCA or other source accumulates in the reactor cavity, molten fuel can transfer its energy to the coolant after vessel failure and potentially cause an energetic steam explosion.

To reduce the risk of containment failure due to hydrogen burns, the U.S. EPR design includes a CGCS that consists of passive autocatalytic recombiners (PARs), rupture and convection foils, and mixing dampers, as described in FSAR Tier 2, Section 6.2.5. The PARs are distributed throughout containment to combine hydrogen and oxygen, and the foils and dampers are designed to promote global convection and containment mixing.

The U.S. EPR reactor cavity is also designed to limit the potential for a steam explosion. First, the reactor cavity is not expected to accumulate water after most LOCAs. Water would accumulate only as a result of a break at the weld between the RCS piping and the reactor vessel nozzles. In addition, SAHRS flooding of the core melt spreading area after vessel failure is performed at a low flow rate that would quench the melt and cause a pressure transient below the design pressure of the containment.

These design features are described further in the evaluation of FSAR Tier 2, Section 19.2.3 below.

19.1.4.3.1.11 *Potential for Accidents that Bypass Containment*

Discharge of reactor coolant outside containment is risk-significant because of both the offsite radiological consequences and the loss of RCS inventory that cannot be retrieved for recirculation. The two main types of containment bypass are an SGTR, described in Section 19.1.4.3.1.5 of this report, and an ISLOCA. The ISLOCA is a class of accidents in which a break occurs in a system connected to the RCS, causing a loss of the primary system inventory. This type of accident can occur when a low-pressure system, such as the residual heat removal system (RHRS), is inadvertently exposed to high RCS pressures beyond its capacity. In NUREG-75/014, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," dated October 1975, and NUREG-1150, Volume 1, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants – Final Summary Report," December 1990, the NRC described the ISLOCA outside containment as an event of low core damage frequency, but as one of the main contributors to radioactive release.

The U.S. EPR design features to reduce the risk impact of an SGTR are discussed in Section 19.1.4.3.1.5 of this report. The EBS, CVCS, and RHRS are connected to the RCS and are, therefore, potentially susceptible to an ISLOCA. As explained in FSAR Tier 2, Section 19.2.2.5, all three of these systems are designed to withstand RCS design pressure [17.582 MPa (2,550 psia), according to TS]. Specifically, EBS is designed to inject a boron solution against any credible RCS pressure, so its design pressure is significantly higher than RCS pressure (relief valve setpoint of 24.993 MPa (3,625 psig) in FSAR Tier 2, Table 6.8-1). The CVCS design pressure is 24.993 MPa (3,625 psig), as stated in FSAR Tier 2, Table 9.3.4-1. According to FSAR Tier 2, Section 5.4.7.2.2, the portions of RHRS from the RCS to the second reactor coolant pressure boundary (RCPB) isolation valves are designed to the RCS design pressure, while the remaining portions of the SIS/RHRS are designed so that the ultimate rupture strength exceeds that of the full RCS operating pressure.

The staff's evaluation of these design features in FSAR Tier 2, Section 19.2.2 is presented below.

19.1.4.3.1.12 *Potential for Late Failure of Containment*

Finally, the U.S. EPR design considers the potential for late failure of containment due to a loss of heat removal or hydrogen combustion. The combustible gas control approach, which applies to both early and late containment failure, is described in Section 19.1.4.3.1.10 of this report. FSAR Tier 2, Section 6.2.2, states that containment heat removal is achieved by LHSI cooling of the IRWST, into which the spilled and condensing reactor coolant flows after blowdown of the RCS. The four-train redundancy of the LHSI system reduces the impact of any single LHSI division failure on the ability to cool containment. The U.S. EPR design does not credit active cooling by containment fan coolers or sprays. Additionally, CMSS and SAHRS increase the ability to cool the core debris and reduce the likelihood of core-concrete interactions that could fail the containment basemat. These features are described in the evaluation of FSAR Tier 2, Section 19.2.3 below. The containment performance capability is described in the evaluation of FSAR Tier 2, Section 19.2.4 below.

19.1.4.3.2 Balance of Preventive and Mitigative Features

Additionally, the information provided in FSAR Tier 2, Section 19.1.3 is intended to support the acceptance criterion described above (see Section 19.1.4.3 of this report), that the applicant has adequately demonstrated that the design properly balances preventive and mitigative features. FSAR Tier 2, Section 19.1.3.1 presents nine features designed to prevent accidents, while FSAR Tier 2, Sections 19.1.3.2 and 19.1.3.3 present seven features designed to mitigate the effects of accidents. Additionally, four of the twelve challenges noted in FSAR Tier 2, Table 19.1-2 deal with accident mitigation. Many of these features are discussed in Section 19.1.4.3.1 of this report. The number of features in each category provides assurance that the applicant has considered both preventive and mitigative features in its design.

19.1.4.4 *FSAR Tier 2, Section 19.1.4: Safety Insights from the Internal Events PRA for Operations at Power*

19.1.4.4.1 FSAR Tier 2, Section 19.1.4.1: Level 1 Internal Events PRA for Operations at Power

The information in FSAR Tier 2, Section 19.1.4.1 relates to the following regulatory requirement:

> 10 CFR 52.47(a)(27): Provide a description of the design-specific PRA and its results.

In addition, this information relates to four acceptance criteria from SRP Section 19.0, as summarized below:

- The staff should ensure that the applicant has used the PRA results and insights, including those from uncertainty analyses, importance analyses, and sensitivity studies, in an integrated fashion to identify and establish specifications and performance objectives for the design, construction, testing, inspection, and operation of the plant. Specifically, PRA results and insights are input to ITAAC; TS; RAP; RTNSS; and COL action items.

- For designs that have evolved from current plant technology, the results of the PRA should indicate that the design represents a reduction in risk compared to operating plants. The staff should perform a broad (qualitative and quantitative) comparison of risks, by initiating event category, between the proposed design and operating plant designs to identify the major design features that contribute to the lower risk of the proposed design compared to existing designs.

- The staff should consider the impact of data uncertainties on the risk estimates. In addition, the staff should review the applicant's risk importance studies to obtain insights about the systems, components, and human actions that contribute the most in achieving the low risk level assessed in the PRA, as well as the failures that contribute the most to the assessed risk. The staff should also review the applicant's sensitivity studies performed to determine (1) the sensitivity of the estimated risk to potential biases in numerical values, (2) the impact of the lack of detail, and (3) the sensitivity of the estimated risk to previously raised issues.

- The staff should confirm that the assumptions made in the applicant's PRA during design development and certification, in which a specific site may not have been identified or all aspects of the design may not have been fully developed, are identified in the design certification application such that they can be addressed by the COL application.

19.1.4.4.2 Description of PRA and its Results

10 CFR 52.47(a)(27) requires that the design certification application include a description of the design-specific PRA and its results. This requirement is intended to be a qualitative description of insights and uses, as well as some quantitative PRA results, such that the staff can perform the review, ensure risk insights were factored into the design, and make the evaluation findings described in the SRP.

Therefore, the staff has focused its evaluation of the PRA and its results on the information provided in FSAR Tier 2, Chapter 19 and in the applicant's responses to the staff's RAIs. The staff performed several audits of the applicant's PRA documentation at the applicant's office, to obtain background understanding on the structure and application of the PRA. All information that was needed from the detailed PRA documentation to reach a safety decision; however, was requested from the applicant on the docket using the RAI process. As appropriate, the applicant made changes to the FSAR to reflect the staff's information requests.

For the Level 1 internal events PRA for operations at power, 10 CFR 52.47(a)(27) has been satisfied by the description of the PRA methodology and results presented in FSAR Tier 2, Section 19.1.4.1; tables providing information on initiating events, systems, cutsets, importance measures, and sensitivity studies; and figures presenting dependencies, initiating event contributions, and uncertainty results. A summary of this information is provided in the following sections.

The quality of the PRA development process was discussed above in the evaluation of FSAR Tier 2, Section 19.1.2; the discussion of the other acceptance criteria in the following sections addresses specific details of the PRA.

19.1.4.4.2.1 *PRA Methodology*

FSAR Tier 2, Section 19.1.4.1.1, "Description of the Level 1 PRA for Operations at Power," provides a detailed description of the applicant's approach to developing the internal events PRA. The methodology includes identifying the initiating events, analyzing the accident sequences, modeling the plant systems, assembling a databank of unavailability and failure events, performing a human reliability analysis (HRA), and quantifying the full model.

Initiating Events Assessment. The applicant identified events that could initiate an accident sequence by reviewing available data sources[1], performing an FMEA of U.S. EPR systems, considering pipe break frequencies, and evaluating potential LOCAs outside containment. The resulting initiating events are grouped into several categories: plant transients, with varying

[1] These sources include NUREG/CR-5750, "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995," dated February 1999, and Electric Power Research Institute (EPRI) TR-016780, "Advanced Light Water Reactor Utility Requirements Document [ALWR URD]."

availability of balance of plant (BOP) systems; LOCAs; ISLOCAs; SGTRs; secondary side breaks; and failures of support systems, such as cooling water, power, and ventilation.

FSAR Tier 2, Table 19.1-4 shows the final set of initiating events with the mean frequency and information source for each. In RAI 2, Question 19-06, the staff requested clarification of the frequencies used in the PRA. In an April 30, 2008, response, the applicant stated that, for initiating events evaluated with fault trees, point estimates, and not mean values, were used in the CDF point estimate calculation. Mean values were used as the inputs to the CDF mean value quantification in the uncertainty evaluation. If mean values are used instead of point estimates for initiating event frequencies, the change in the CDF point estimate is less than 1E-8/yr. Based on this additional information and the demonstrated small effect on the PRA results, the staff concludes that this treatment appropriately addresses the possible implications of the state-of-knowledge correlation on the initiating event frequencies and is acceptable.

Several initiating events, familiar from operating plant PRAs, are not included explicitly in the set of initiating events presented by the applicant:

- LOCAs caused by failure of the PSRVs to reseat (after possibly opening during a transient) are included as part of the small LOCA frequency. Therefore, they are implicitly addressed by the model.

- RCP seal LOCAs are not modeled as an initiating event, but as a possible consequence of failed seal cooling.

- ATWS events are modeled with an event tree, but are not included in the list of initiating events, since the ATWS follows the reactor trip signal caused by one of the other initiating events.

- Very small LOCAs are not modeled, because the analysis assumes that the charging system can maintain RCS inventory. In RAI 53, Question 19-193, the staff requested a justification of this exclusion. In a September 22, 2008, response, the applicant provided the following justification: The frequency of a very small LOCA combined with CVCS failure is about 0.2 percent of the U.S. EPR small LOCA frequency and that small LOCAs contribute only 9 percent of the total CDF. Because of this small contribution, the staff concludes that the justification for the treatment of very small LOCAs is acceptable.

- Vessel ruptures are not modeled as initiating events. In RAI 53, Question 19-194, the staff requested a justification of this exclusion. In a September 22, 2008, response, the applicant indicated that the frequency used by the current generation of operating plants (1E-7/yr) was based on engineering judgment, and that inclusion of this initiating event without a realistic frequency estimate would dominate the risk results and lead to non-conservative importance measures. Various programs (e.g., the material surveillance program described in FSAR Tier 2, Section 5.3.1.6) exist to give the staff reasonable assurance that vessel integrity will be maintained. Because the ECCS may not be sufficient to mitigate a postulated vessel rupture, core damage is assumed to result. The staff agrees that this sequence would dominate the internal events PRA without providing any additional risk insights (e.g., systems needing increased maintenance or better design). If the sequence were included, the total CDF would be expected to remain well below the Commission's goal of 1E-4/yr, and the severe accident

mitigating features would remain available to reduce the likelihood of offsite consequences. Therefore, the staff concludes that excluding vessel ruptures from the PRA is acceptable.

- Feedwater line breaks inside containment (FLBI) are modeled as a subset of the steam line break inside containment (SLBI) initiator, since the success criteria and mitigation strategy are similar. In RAI 7, Question 19-66, the staff requested a more detailed discussion of the modeling of feedwater line breaks. In a June 16, 2008, response, the applicant provided additional justification for using generic data for SLBI without adding a contribution for FLBI, based on conservatism in the SLBI frequency. In RAI 53, Question 19-195, the staff requested further information on potentially different mitigating strategies for and consequences of the two events. In a November 12, 2008, response, the applicant showed that, if FLBI were modeled separately, the FLBI-specific CDF would be approximately 2.2E-9/yr. This value is about 17 percent of the SLBI-specific CDF and less than one percent of the internal events CDF point estimate. Also, the frequency of an FLBI-induced small LOCA (stuck-open PSRV) is more than four orders of magnitude less than the small LOCA frequency used in the PRA model. Because of this small contribution, the staff concludes that the treatment of FLBI is acceptable.

- Feedwater line breaks outside containment (FLBO) are modeled as a subset of the loss of main feedwater (LOMFW) initiating event. In RAI 7, Question 19-66, the staff requested a more detailed discussion of the modeling of feedwater line breaks. In a June 16, 2008, response, the applicant provided additional justification for using generic data for LOMFW without adding a contribution for FLBO, based on potential conservatism in the LOMFW frequency. Industry data indicates that the frequency of feedwater line breaks is about 10 percent of the assumed LOMFW frequency. Given that LOMFW initiators contribute less than two percent to internal events CDF, the staff concludes that the small increase in the initiating event frequency that FLBO might add would not affect the results and insights of the PRA. Therefore, the applicant's assumption that FLBO events can be treated as a subset of LOMFW is acceptable.

- Loss of a vital dc bus is currently not modeled, and the applicant plans to address this when the power system design is finalized. In RAI 2, Question 19-36, the staff requested clarification on the modeling of bus failures. In an April 30, 2008, response, the applicant stated that a loss of a dc bus is unlikely to result in an initiating event, because it does not affect normally operating equipment. Loss of a division of emergency ac power is explicitly addressed by the model. The staff observes that, even if a transient occurred as a result of the bus failure, the redundancy of trains provides confidence that mitigation capability would be available. The staff concludes that the exclusion of this initiating event is acceptable at the design certification stage.

- Loss of instrument air is not modeled, because there are no significant air-operated components in the U.S. EPR design.

Analysis of Accident Sequences. The applicant used event sequence diagrams (ESDs) to model and document plant response to initiating events, as an input to the core-damage event trees. These initiating events include:

- Loss of main feedwater
- LOCAs (except for large-break LOCAs)
- Steam generator tube ruptures
- Steam line break inside containment
- Steam line break outside containment (SLBO)
- Feed and bleed scenarios

A sequence of events is considered successful if the sequence results in a safe, stable state for 24 hours. Specifically, core damage is defined as uncovering of the core, causing the fuel to heat, oxidize, and become severely damaged. For most transient and LOCA events, the applicant assumed core damage if the peak cladding temperature (PCT) exceeded 1,204.4 °C (2,200 °F). In ATWS scenarios (such as consequences of SLBI initiators), the applicant assumed core damage if RCS pressure exceeded 130 percent of design pressure.

To make these determinations of success or core damage, the applicant used the Modular Accident Analysis Program (MAAP), Version 4.0.7. MAAP was used to analyze success criteria for 155 scenarios representing LOMFW, LOCAs, SGTR, SLBI, SLBO, and feed and bleed. Because certain scenarios (listed in FSAR Tier 2, Section 19.1.4.1.1.7) may challenge the simplified modeling techniques employed by MAAP, benchmarking studies were performed by the staff using S-RELAP5, which has been approved by the NRC for use in safety analyses. MAAP cases resulting in a PCT between 760 °C (1,400 °F) and 982.2 °C (1,800 °F) were examined in detail, often with a corresponding S-RELAP5 calculation. Below 760 °C (1,400 °F), success was assumed; above 982.2 °C (1,800 °F), core damage was assumed directly from the MAAP results. In RAI 133, Question 19-246, the staff requested detailed results of the calculations performed to determine success criteria. In a December 8, 2008, response, the applicant provided detailed information on the seven S-RELAP5 benchmarking scenarios.

Table 19.1-1 of this report (as presented in Table 19-246-1 in the response to RAI 133, Question 19-246) shows the scenarios compared in the benchmark study. The applicant concluded that, overall, the MAAP 4.0.7 results agreed with the S-RELAP results. There were, however, some noteworthy differences, and the applicant recommended further analysis for some scenarios. A comparison of the results is shown in Table 19.1-2 of this report (Table 19-246-2 in the response to Question 19-246), which supports the following acceptance criteria developed by the applicant for MAAP4 use to develop success criteria for the U.S. EPR:

- MAAP4 cases resulting in a PCT of 760 °C (1,400 °F) or less are considered a success.
- MAAP4 cases resulting in a PCT of 982.2 °C (1,800 °F) or greater are considered a failure.
- MAAP4 cases resulting in a PCT greater than 760 °C (1,400 °F) and less than 982.2 °C (1,800 °F) should be examined in greater detail, possibly with a corresponding S-RELAP5 calculation.

- For overpressure events, the reactor coolant system pressure must be less than 130 percent of design pressure. The design pressure is 17.582 MPa (2,550 psia).
- For low power and shutdown events, the core must remain covered (i.e., the two-phase level in the reactor vessel is above the elevation of the top of the core).
- For all events, a 24-hour mission time is required. Therefore, EFWS should be able to inject for this period and all four EFW tanks should not become empty within 24 hours after event initiation.
- The staff finds the applicant's approach prudent, and is confident that it has led to the development of appropriate acceptance criteria for the use of MAAP4 in success criteria determination. The staff further notes that the applicant's acceptance criteria call for further analysis for some scenarios.

Table 19.1-1 Scenarios Compared in the Benchmark Study

Case Trait	3c	4g	12a	13d	16a1	4i	4cc
Initiating Event	LOFW	LOFW	SBLOCA (2 in)	SBLOCA (3 in)	MBLOCA (6 in)	LOFW	LOFW
RCPS	Trip	Run	Trip	Trip	Trip	Run	Run
MSRV	All fail closed	All fail closed	1/4	1/4	Off	All fail Closed	All fail closed
PCD/FCD	NA	NA	PCD	FCD	NA	NA	NA
MSSV	1/8	1/SG	Off	Off	Off	1/SG	1/SG
EFW	1/4	Off	1/4	1/4	Off	Off	Off
MHSI	Off	1/4	1/4	Off	1/4	1 of 4	1 of 4
ACC	Off	1/4	Off	1/4	Off	1 of 4	1 of 4
LHSI	Off	Off	Off	1/4	1/4	Off	Off
Operator	NA	Open PDS valves at 1.1 hr	NA	Open one MSRV at 40 min (FCD)	NA	NA	Open PDS valves at 90 min

Table 19.1-2 Comparison of S-RELAP and MAAP4 Results

Case	Initiating Event	MAAP Peak Region Temp.	S-RELAP Equivalent/Hot Rod PCT (Best Estimate)	S-RELAP5 Equivalent/Hot Rod PCT Sensitivity Study
3c	LOFW	360 °C (680 °F)	354.4 °C/354.4 °C (670 °F/670 °F)	354.4 °C/354.4 °C (670 °F/670 °F)
4g	LOFW	993.3 °C (1,820 °F)	354.4 °C/354.4 °C (670 °F/670 °F)	398.9 °C/371.1 °C (750 °F/700 °F)
4i	LOFW	>1,204.4 °C (>2,200 °F)	>1,204.4 °C (>2,200 °F)	NA
4cc2	LOFW	676.7 °C (1,250 °F)	426.7 °C/454.4 °C 800 °F/850 °F	NA
12a	LOCA	360 °C (680 °F)	354.4 °C/354.4 °C (670 °F/670 °F)	354.4 °C/354.4 °C (670 °F/670 °F)
13d	LOCA	593.3 °C (1,100 °F)	926.7 °C/1,065.6 °C (1,700 °F/1,950 °F)	621.1 °C/704.4 °C 1,150 °F/1,300 °F
16a1	LOCA	654.4 °C (1,210 °F)	704.4 °C/871.1 °C 1,300 °F/1,600 °F	NA

The applicant then proceeded to develop success criteria for the various initiators using the benchmark results and the resulting acceptance criteria; these success criteria are summarized in the December 8, 2008, response to RAI 133, Question 19-246. The staff has reviewed the response to RAI 133, Question 19-246 and finds the acceptance criteria and success criteria appropriate, and that they properly consider the simplified nature of some of the MAAP4 models. The success criteria are also comprehensive, addressing all of the initiating events of interest.

Based on the information compiled from the evaluation of plant response and definition of success criteria, the applicant developed core-damage event trees, which are provided in FSAR Tier 2, Appendix 19A. The applicant states that every safety system and operator action required for each key safety function is explicitly included in the event trees. The three key safety functions that need to be satisfied to ensure a success state are defined by the applicant to be:

- Reactivity Control: A reactor trip is generally needed to reduce heat generation, but failure to trip does not lead directly to core damage, because boron injection can be used. Failure of a reactor trip transfers to the ATWS event analysis.

- Inventory Control: The water inventory needed for heat removal can be challenged by a LOCA or by system failures following another initiating event. Inventory control can also be challenged when secondary systems fail and the operators must initiate feed and bleed. MHSI, LHSI, the accumulators, CVCS, and EBS can all provide inventory makeup to the RCS. In some cases, partial or

fast cooldown via the MSRTs is needed before these makeup sources can be used.

- Heat Removal: Heat must be transferred from the reactor coolant to the environment. In some sequences, the SGs can be used with supply from MFW, EFWS, or SSS and relief to the condenser or the atmosphere. If secondary cooling fails, feed and bleed is initiated with supply from CVCS or safety injection and relief through the PSRVs or SADVs. Heat is then transferred to primary containment, so the IRWST inventory must be cooled by LHSI or SAHRS.

The staff agrees that these safety functions need to be satisfied to avert core damage. Furthermore, the staff's review of FSAR Tier 2, Section 19A confirmed that the success criteria were appropriately used to construct the event trees for the various initiating events.

System Modeling. FSAR Tier 2, Table 19.1-5 lists the systems modeled in the U.S. EPR design-specific PRA. These systems provide the key safety functions needed after an initiating event occurs. Seven systems (MHSI, LHSI, accumulators, IRWST, EBS, CVCS, and SSSS) are used for RCS inventory control. Six systems (MFW, SSS, EFWS, main steam system (MSS), pressurizer relief system, and SAHRS) remove heat from the RCS. Finally, support for these systems is provided by ac and dc electric power, CCWS, ESWS and the ultimate heat sink (UHS), the safeguard building ventilation system (SBVS) and SBVS electrical division (SBVSE), safety chilled water system (SCWS), and I&C systems.

FSAR Tier 2, Table 19.1-5 also lists in the "Comment" column the important attributes of each system as modeled in the PRA. The staff reviewed the comments on each system and verified that these attributes were included in system descriptions elsewhere in the FSAR. The relevant FSAR sections are listed in Table 19.1-3 of this report.

Table 19.1-3 Systems Analyzed in the U.S. EPR PRA (Based on FSAR Tier 2, Table 19.1-5)

System	Attributes	FSAR Sections
MHSI	• Four independent trains, physically separated in different SB • Inventory control for LOCAs, SGTR, and feed-and-bleed cooling	FSAR Tier 1, Section 2.2.3 FSAR Tier 2, Section 6.3
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	FSAR Tier 1, Section 2.2.3 FSAR Tier 2, Section 6.3

System	Attributes	FSAR Sections
Accumulators	• Four separate accumulators (one for each RCS cold leg) • Reflooding of core following LLOCA; additional inventory control for small and medium LOCAs	FSAR Tier 1, Section 2.2.3 FSAR Tier 2, Section 6.3
IRWST	• Single tank, integral to the containment structure • Suction source for CVCS, MHSI,LHSI and SAHRS • 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	FSAR Tier 1, Section 2.2.2 FSAR Tier 2, Section 6.3
EBS	• Two-train system capable of injecting highly borated water into RCS • Manual backup to reactor shutdown systems	FSAR Tier 1, Section 2.2.7 FSAR Tier 2, Section 6.8
CVCS	• Two-train, non-safety system • Inventory control for RCS leaks, avoiding challenges to safety systems	FSAR Tier 1, Section 2.2.6 FSAR Tier 2, Section 9.3.4
SSSS	• Pneumatic seal, backup to normal multi-stage seals • Deployed when RCPs trip on a loss of seal cooling	FSAR Tier 1, Section 2.2.1 FSAR Tier 2, Section 5.4.1
MFW	• Three trains with motor-driven pumps; all normally in service during power operation • Continued secondary heat removal following reactor trip	FSAR Tier 1, Section 2.8.6 FSAR Tier 2, Section 10.4.7
SSS	• Single motor-driven pump • Backup secondary heat removal	FSAR Tier 1, Section 2.8.6 FSAR Tier 2, Section 10.4.7

System	Attributes	FSAR Sections
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 MFW and SSS are unavailable	FSAR Tier 1, Section 2.2.4 FSAR Tier 2, Section 10.4.9
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 fast cooldown accomplished via MSRTs • Isolation following SGTR or secondary line break via closing of MSIV	FSAR Tier 1, Section 2.8.2 FSAR Tier 2, Sections 7.3.1.2.4 (partial cooldown actuation), 10.3 (MSS), and 10.4.4 (turbine bypass)
PDS	• Three PSRVs 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	FSAR Tier 1, Section 2.2.1 FSAR Tier 2, Sections 5.4.13 (PSRV) and 19.2.3.3.4.1 (SADV)
SAHRS	• Single-train system, with heat sink via dedicated trains of CCWS and ESWS • SAHRS takes suction from IRWST • The SAHRS 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	FSAR Tier 1, Section 2.3.3 FSAR Tier 2, Section 19.2.3.3.3.2

System	Attributes	FSAR Sections
ac power	• 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 EDGs in two separate diesel buildings • Two SBODGs separated from and of diverse design with respect to the EDGs • Continued supply of offsite power to plant auxiliaries following reactor trip, without need for fast transfer • Capability for partial trip (runback and supply to house loads from main generator) in the event of a load rejection	FSAR Tier 1, Sections 2.5.1 (Class 1E), 2.5.3 (SBODG), 2.5.4 (EDG), 2.5.5 (offsite), and 2.5.10 (non-1E) FSAR Tier 2, Sections 8.2 (offsite), 8.3.1 (onsite), 8.4 (SBODG), and 14.2.12.12.4 (test of partial trip)
dc power	• 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-hour discharge	FSAR Tier 1, Sections 2.5.2 (Class 1E), 2.5.7 (non-1E), and 2.4.11 (12-hour) FSAR Tier 2, Section 8.3.2
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 SCWS units in Trains 2 and 3 • Dedicated train loads include the MHSI pumps, the RHRS/LHSI heat exchangers in all four trains, and the LHSI pumps in Trains 2 and 3	FSAR Tier 1, Section 2.7.1 FSAR Tier 2, Section 9.2.2
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 support systems)	FSAR Tier 1, Section 2.7.11 FSAR Tier 2, Sections 9.2.1 (ESWS) and 9.2.5 (UHS)

System	Attributes	FSAR Sections
SBVS/SBVSE	• Four independent divisions, one for each SB • Two non-safety divisions serve as backups to the safety divisions of SBVSE for maintenance purposes	FSAR Tier 1, Sections 2.6.6 and 2.6.7 FSAR Tier 2, Sections 9.4.5 and 9.4.6
SCWS	• Four independent divisions, each housed within separate SB • Provides cooling to SB HVAC, which includes cooling to ac and dc switchgear rooms and EFWS pump rooms • Trains 1 and 4 of are air-cooled whereas Trains 2 and 3 are cooled by the CCWS common headers • Trains 1 and 4 provide direct cooling to the LHSI pumps, such that these pumps are supported during a loss of CCWS or ESWS	FSAR Tier 1, Section 2.7.2 FSAR Tier 2, Sections 9.2.8 and 10.4.9.3
I&C	• Digital I&C systems for different functions (reactor protection system (RPS), engineered safety features actuation system (ESFAS), actuation and control of other safety and non-safety systems)	FSAR Tier 1, Section 2.4 FSAR Tier 2, Chapter 7

The applicant provided an extended discussion of digital I&C modeling for the U.S. EPR, since digital I&C is generally not modeled in current plant PRAs. The PS is modeled in detail, because it has the important functions of initiating a reactor trip and actuating engineered safety features (ESFs). The PS has four divisions, each of which consists of two independent subsystems that process primary and backup trip signals and different ESF functions (e.g., EFWS actuation on one subsystem and SIS actuation on the other). Modeling of the PS includes the rack-mounted TELEPERM XS (TXS) modules, which correspond to available failure data (see the section below). The SAS and PAS are currently modeled using simple, high-level models with undeveloped events representing overall failure rates. In addition, the PAS may include backup ESF functions using technology diverse from the PS; however, these functions and the additional diversity they may provide are not yet modeled. These assumptions are included as Item 46 in FSAR Tier 2, Table 19.1-109, "U.S. EPR PRA General Assumptions." As stated in the second note below the table, the PRA assumptions will be re-evaluated as part of the PRA maintenance and update process (discussed above in the evaluation of FSAR Tier 2, Section 19.1.2), and COL Information Item 19.1-9 is provided to confirm that assumptions used in the PRA remain valid for the as-to-be-operated plant.

The treatment of dependencies between the PS and the undeveloped I&C systems was unclear. In RAI 227, Question 19-287, the staff requested additional information on the systems or functions to be actuated by these undeveloped I&C systems and the potential for CCFs between these systems and the PS. **RAI 227, Question 19-287, which is associated with the above request, is being tracked as an open item**.

Several unique or non-intuitive dependencies are also highlighted by the applicant in the discussion of system modeling. These dependencies, as identified below, relate mainly to ventilation and power requirements.

- CCWS Dependencies: Cooling to the RCPs, the water-cooled trains of the SCWS, the charging pumps, and the operational chilled water system (OCWS) chillers comes from two CCWS common headers. (Note that the OCWS, which provides chilled water to the electrical division of the SBVS when the SCWS is unavailable, is not described in the FSAR. In a May 30, 2008, response to RAI 2, Question 19-7, the applicant provided a description and drawing of the system.) Each of the common headers can be supplied by two trains of the CCWS, with an automatic switchover from the running CCWS train to the standby train when needed and automatic isolation of a leaking train or header.

- SCWS Dependencies: SCWS Divisions 1 and 4 are air-cooled, and Divisions 2 and 3 are cooled by CCWS, as mentioned above. The EFWS pumps are modeled as dependent on SCWS for room cooling. SCWS is also credited for cooling to the safety-related electrical rooms in the SBs, as well as motor and seal cooling for the Division 1 and 4 LHSI pumps.

- SB HVAC Dependencies: Because of the dependencies discussed above, complete loss of HVAC to SB 1 (symmetric in SB 4) can significantly affect system availability. Loss of HVAC is assumed to cause a slow heat-up of the electrical and EFWS rooms in the affected SB, with loss of the equipment after 2 hours if operator action is not taken. The running CCWS pump fails, and switchover to the standby pump also fails, meaning that the CCWS common header is inoperable. Therefore, cooling to RCPs 1 and 2 fails, one charging pump fails, and cooling to the Division 2 SCWS chiller via the CCWS common header fails. Because Division 2 SCWS is lost, HVAC to SB 2 fails and Division 2 ac, dc, and EFWS may fail. Thus, if HVAC fails in a SB with a running CCWS train (SB 1 and 4), two electrical and EFWS divisions may eventually fail. Since the Division 2 and 3 CCWS pumps are initially in standby, HVAC failures in SB 2 or 3 would affect only the electrical and EFWS systems in those divisions.

- Primary Depressurization Dependencies: Feed-and-bleed cooling requires all three PSRVs to open. Opening each PSRV requires two solenoids to energize, and the six solenoids are powered from four different 480-volt (V) motor control centers (MCCs) that are backed by two-hour batteries. Therefore, failure of one of these four MCCs disables the use of PSRVs for feed and bleed. If the SADVs are used, two MOVs in series must open. The upstream and downstream valves are supported by two different 480V MCCs that are backed by 12-hour batteries; therefore, both MCCs must be available to use the SADVs.

- MSRIV Dependencies: The MSRTs are used for steam relief and reactor cooldown. Each SG has one MSRIV controlled by four solenoid-operated valves (SOVs) that are powered by four different 480V MCCs backed by two-hour batteries. Because two pilots in series must open to open the MSRIVs, unavailability of certain combinations of two MCCs will cause all four MSRIVs to fail closed.

Relative to the HVAC dependencies described above, the staff noted that the importance of these dependencies is driven in part by the assumption that the CCWS pumps in Divisions 1 and 4 are initially running. Loss of the CCWS common header after HVAC-induced switchover failure results in failure of the CCWS-cooled SCWS equipment in Division 2 or 3. However, if the CCWS pumps in Divisions 2 and 3 were initially running, the air-cooled SCWS divisions could still provide HVAC to SBs 1 and 4 following failure of the CCWS common header, and only one building would be impacted by the initial HVAC failure.

In RAI 138, Question 19-249, the staff requested additional information on the assumption that Divisions 1 and 4 are initially running and an assessment of the reduction in risk if Divisions 2 and 3 were running. In a February 11, 2009, response, the applicant described the rotation of pumps that will realistically occur during operation to provide an equal wear per pump. Although total at-power CDF would be about 40 percent lower if Divisions 2 and 3 were always assumed to be running, the various pump-rotation strategies postulated in sensitivity cases resulted in comparable at-power CDF estimates. Each of these estimates is about 20 percent lower than the CDF estimated with Divisions 1 and 4 always running. Therefore, although certain pump configurations are preferable from a risk perspective, no significant differences in yearly risk were identified in the realistic rotation strategies. In addition, the applicant added the assumption about the running trains to FSAR Tier 2, Table 19.1-109.

However, the HVAC dependencies are also driven by the assumption that the CCWS common header switchover fails following a ventilation failure, leading to failure of CCWS-cooled ventilation in a second SB and thereby failure of that building's equipment. In RAI 227, Question 19-291, the staff requested that the applicant describe any design changes that were considered to eliminate or reduce the likelihood of this scenario. In a July 6, 2009, response, the applicant indicated that potential design changes (e.g., eliminating an interlock or adding an automatic switchover) could introduce additional failure modes that might increase risk. Instead, the applicant stated that "[t]his issue can be addressed through the plant procedures that, on a loss of HVAC for a specific division, instruct operators to make sure that a running CCW pump is not supplied from this division (perform a CCW switchover if necessary)."

In RAI 257, Question 19-318, the staff requested additional information on this procedural action. If the operator succeeds in following this procedure, only one division of equipment (rather than two) would fail following a loss of HVAC to one SB. The applicant was requested to provide further justification for the current treatment.

In an August 17, 2009, response, the applicant clarified that this operator action is not included in the PRA, because it is not yet part of the U.S. EPR documentation and operators may have other means of reducing the risk of a switchover failure (e.g., design change, administrative controls of HVAC maintenance). The applicant performed a sensitivity study crediting an operator action to perform the CCWS common header switchover when HVAC is lost in the building supplying the common header. The results of this study showed approximately a 20 percent decrease in total at-power CDF, dominated by an effect on the internal events model. However, the applicant provided several insights, summarized below, to justify that the operator action would not significantly affect the conclusions gained from the PRA.

- The relative contributions of internal, fire, and flood events would not change significantly. Internal events would dominate with a 48 percent contribution instead of 55 percent.

- The ranking of significant initiating events would not change significantly. LOOP events would dominate with a 39 percent contribution instead of 49 percent.

- The contribution from cutsets including a LOOP and HVAC failures would change significantly, but the overall selection of significant cutsets would not be significantly affected.

- The new CCWS switchover human action would be identified as important, but the remainder of the important operator actions would not change significantly. HVAC recovery would be less significant but still identified as important.

- The ranking of significant equipment failures and parameters would not change significantly.

- No significant changes to fire and flood CDF or risk insights would occur.

The applicant documented multiple insights related to the HVAC dependency in FSAR Tier 2, Section 19.1.4.1.1.3 and FSAR Tier 2, Tables 19.1-108 and 19.1-109. Because this dependency is clearly identified in the FSAR as a significant contributor and the applicant's sensitivity study reveals no significant effect on the PRA results and conclusions if a new operator action were included, the staff concludes that the approach taken by the applicant is acceptable at the design stage. If future COL applicants or holders choose a specific strategy to address the HVAC dependency (e.g., a proceduralized action), then the PRA maintenance process will dictate the changes needed to the PRA.

Assembly of Data. As described in FSAR Tier 2, Section 19.1.4.1.1.4, the U.S. EPR design-specific PRA includes data for several types of unavailability and failures: Initiating event frequencies; component failure rates; test and maintenance unavailability; and CCFs (including software reliability). The sources of initiating event data are described in the initiating events section above.

Component Failure Rates. Component failure data for the U.S. EPR was selected from three major data sources compiled by EG&G Idaho (now a division of URS Corporation), the German organization VGB PowerTech, and the European Industry Reliability Data Bank (EIReDA). In RAI 2, Question 19-04, the staff requested the generic failure probabilities and distribution parameters used for components in the PRA. In an April 30, 2008, response, the applicant provided a table of the data used in the U.S. EPR design-specific PRA, as well as the failure rates suggested in the ALWR URD. The staff compared this failure data to the values tabulated in NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," dated February 2007, and concluded that, as the applicant stated, the failure rates are comparable to other U.S. data sources.

The staff also requested and evaluated additional information on the failure rates as follows:

- In RAI 7, Question 19-73, the staff requested additional information on digital I&C component failures. In a June 16, 2009, response, the applicant provided the failure rates used for TXS digital I&C components and compared them to field failure rates from protection systems in European nuclear power plants, demonstrating that the theoretical failure rates used in the PRA are higher than those observed in the field. The staff considers this approach acceptable when plant-specific data is not available. In RAI 138, Question 19-257, the staff requested further information related to the failure rates. In a December 19,

2008, response, the applicant provided detailed information and proprietary data supporting the I&C failure rates discussed above. The staff compared this information to the failure probabilities presented in the tables of importance measures from the PRA and determined that it was used consistently.

- In RAI 14, Question 19-129, the staff requested a justification for the sump strainer plugging rate of 5E-7 per hour (/hr). In a July 11, 2008, response, the applicant stated that this rate, more than an order of magnitude lower than that cited in NUREG/CR-6928, was justified based on the EG&G strainer plugging failure rate of 5E-6/hr, modified by a 0.1 factor to take credit for advanced design features that make strainer plugging unlikely. These design features and their dispositions are referred to in Item 14 in FSAR Tier 2, Table 19.1-108, "U.S. EPR PRA Based Insights." Given that these design features are evaluated by the staff as part of the review of the strainer design and that future design changes will be evaluated to determine the effect (if any) on the PRA results and insights, the staff concludes that the assumed strainer failure is acceptable.

- In RAI 138, Question 19-256, the staff requested additional information on the modeling of battery failures. In a December 19, 2008, response, the applicant clarified that failures to run are not modeled because of the small hourly failure rate and short operating time. The staff confirmed that, based on the mission time and the failure rates in NUREG/CR-6928, the probability of a failure to run would be about three percent of the demand failure probability assumed in the PRA. The screened failure mode is approximately two orders of magnitude lower than the included failure mode as outlined in the screening criteria, so the staff considers this screening to be acceptable.

- In RAI 138, Question 19-256, the staff requested additional information on the modeling of battery chargers. In a December 19, 2008, response, the applicant provided an hourly battery charger failure rate that is comparable to the failure rates stated in NUREG/CR-6928 and the ALWR URD. Therefore, the staff concludes that the assumed failure rate is acceptable.

- In RAI 138, Question 19-258, the staff requested information on the testing intervals assumed in the PRA. In a December 19, 2008, response, the applicant clarified the assumed test intervals for important PRA components. These test intervals generally correspond to those required by TS and/or the in-service testing (IST) program. In the case of the SIS check valves, the data is based on a one-year test interval. The IST program states that these valves are tested during cold shutdown; since the PRA assumes an 18-month refueling cycle and 5 days forced outage per year, a one-year interval is plausible. In addition, the assumed failure rate is five times that stated in NUREG/CR-6928, and the contribution of single valve failures to overall CDF is low. The staff concludes that any additional failures caused by longer test intervals would not have a significant impact on the PRA results and insights.

- In RAI 138, Question 19-259, the staff requested additional information on the undeveloped I&C failure events modeled in the PRA. In a December 19, 2008, response, the applicant provided the requested information. Undeveloped basic event probabilities were determined by examining fault trees for similar systems, with adjustments for safety- and non-safety-related systems. These undeveloped

events will be modified in accordance with the PRA maintenance and upgrade process described in FSAR Tier 2, Section 19.1.2.4. Uncertainty associated with the digital I&C modeling is described in greater detail below.

- In RAI 227, Question 19-289, the staff requested a detailed discussion of the PRA failure database development process. In a July 6, 2009, response, the applicant clarified that the data sources were selected for consistency with the European EPR PRA model, given that as-built plant-specific data is not yet available. No testing assumptions are postulated to support standby failure data; instead, only demand failure probabilities are used. The applicant verified that risk-important components subject to infrequent testing (e.g., the SIS common injection check valves) have demand failures that account for infrequent testing. The staff concludes that this approach, which includes a comparison of U.S. EPR data to other generic databases, is appropriate at the design stage. When plant-specific data becomes available, PRA maintenance requirements will ensure that the PRA continues to reflect operating experience.

Test and Maintenance Unavailability. The FSAR did not provide the source of test and maintenance unavailabilities in the U.S. EPR design-specific PRA. In RAI 2, Question 19-03, the staff requested a discussion of how these unavailability estimates were derived. In an April 30, 2008, response, the applicant stated that simple assumptions are made during the design certification stage when procedures and plant experience are not available. Generic data are not used, because current plants do not have the four-train redundancy of the U.S. EPR, a configuration that allows more online maintenance. Preventive maintenance (PM) of 7 days per year is assumed for each train. Corrective maintenance (CM) is assumed to occur 3 days per year for operating trains and 9 days per year for standby trains. For comparison, NUREG/CR-6928 provides an EDG unavailability estimate of 1.34E-2, about 5 days per year, and a CCWS pump unavailability estimate of 5.91E-3, about 2 days per year. Therefore, the U.S. EPR estimates reflect longer outage times as a result of online maintenance.

In RAI 14, Question 19-127, and RAI 53, Question 19-127, the staff requested additional information on specific maintenance assumptions. In a July 11, 2008, response, the applicant clarified that EBS was modeled with only CM, because PM was assumed not to be performed at power. Also, the PRA assumes that the PS components do not need PM (based on manufacturer recommendations); CM is treated by using a mean time to repair (MTTR) unavailability model. In a September 22, 2008, response, the applicant further clarified that maintenance of buses, batteries, and inverters is not modeled because of the short TS completion times associated with this equipment. The staff confirmed that the TS completion times cited by the applicant were correct.

The applicant assumes that maintenance will not be performed simultaneously on trains from different divisions. According to FSAR Tier 2, Table 19.1-15, "U.S. EPR Level 1 Internal Events Sensitivity Studies," the internal events CDF would increase by approximately a factor of two if Train 3 were out of service for PM for the entire year.

In FSAR Tier 2, Revision 1, the applicant updated Table 19.1-109, "U.S. EPR PRA General Assumptions," to include these maintenance assumptions as Items 19, 20, and 21. As stated in the second note below the table, the PRA assumptions will be re-evaluated as part of the PRA maintenance and update process (discussed above in the evaluation of FSAR Tier 2, Section 19.1.2), and COL Information Item 19.1-9 is provided to confirm that assumptions used in the PRA remain valid for the as-to-be-operated plant. Therefore, the staff concludes that the

PRA includes estimates of maintenance unavailability that are suitable for the design stage, as well as an appropriate mechanism for updating these estimates as operating experience is gained.

CCF Modeling. CCF modeling in the U.S. EPR design-specific PRA is based on the method presented in NUREG/CR-5485, “Guidelines in Modeling Common-Cause Failures in Probabilistic Risk Assessment,” dated November 1998, with data based on recent NRC parameter estimations. In RAI 138, Questions 19-259 and 19-260, the staff requested additional information on the CCF parameters used. In a December 19, 2008, response, the applicant provided a table of the CCF and uncertainty parameters in the PRA. The staff confirmed that the parameters used were selected appropriately from NUREG/CR-5497, “Common-Cause Failure Parameter Estimations." The applicant also stated in the response that a CCF beta factor for the SAS was assigned using engineering judgment. The staff confirmed the applicant’s statement that this beta factor provides results comparable to the generic MGL parameters in NUREG/CR-5497.

However, the grouping of processor and sensor failures and the exclusion of input and output modules were not appropriately justified in the December 19, 2008, response. In RAI 227, Questions 19-293 to 19-295, the applicant was requested to clarify these topics. **RAI 227, Questions 19-293 to 19-295, which are associated with the above requests, are being tracked as open items.**

In addition, CCF of the AV42 priority actuation control (PAC) modules is not modeled in the PRA. Item 7 in FSAR Tier 2, Table 19.1-108 states that:

> Software CCF is not a concern for the AV42 priority module because the safety-related functions contain neither software nor an operating system. The AV42 uses a programmable logic device; the functions on the module are implemented in solid state logic gate arrays and are non-user programmable. The AV42 is 100 percent testable before installation. The device also undergoes rigorous physical testing and qualification (environmental, electrical, seismic, radiation, electromagnetic interference, and radio frequency interference). The AV42 module is designed with features to ensure independence between the safety-related and non-safety-related circuits.

In RAI 289, Question 19-328, the staff requested additional information on the PAC modules, given that the staff has not reached a conclusion on the testability of the AV42 design as part of the review of FSAR Tier 2, Chapter 7. In addition, Item 7 in FSAR Tier 2, Table 19.1-108, states that "[s]oftware CCF is not a concern" without addressing CCFs that could result from manufacturing, maintenance, or other errors. If a CCF occurred, manual and automatic actuation of components in various systems could be affected. In RAI 289, Question 19-328, the applicant was requested to provide further justification for excluding both software and hardware CCFs of the AV42 modules from the PRA and to revise the assumptions and insights in FSAR Tier 2, Chapter 19 to reflect potential failure modes of the modules. **RAI 289, Question 19-328, which is associated with the above request, is being tracked as an open item.**

In RAI 138, Question 19-261, the staff requested additional information on I&C communication modules. In a December 19, 2008, response, the applicant indicated that individual communication modules are modeled in the PRA, but CCF of these components is not. The applicant described the large number of communication modules, the self-monitoring of all failure modes of the modules, and the fault-tolerant voting logic of the actuation logic units

(ALU). The PRA and I&C staff evaluated the response and determined that undetected CCF resulting in an unsafe state is highly unlikely. Therefore, the staff concludes that the exclusion of communication module CCF is acceptable.

Intra-system CCFs are modeled for similar, non-diverse, active components. In RAI 2, Question 19-40, the staff requested additional details on the evaluation of inter-system common-cause failures. In an April 30, 2008, response, the applicant described a high-level review for inter-system CCFs. Because hardware-based failures depend on the selection of hardware, there is currently no basis to include inter-system CCFs in the design-phase PRA. However, a CCF of the IRWST sump strainers due to debris blockage is modeled; this failure can have a common impact on multiple systems that draw water from the IRWST. The assumptions related to inter-system CCFs are included as Item 16 in FSAR Tier 2, Table 19.1-109, "U.S. EPR PRA General Assumptions." As stated in the second note below the table, the PRA assumptions will be re-evaluated as part of the PRA maintenance and update process (discussed above in the evaluation of FSAR Tier 2, Section 19.1.2), and COL Information Item 19.1-9 is provided to confirm that assumptions used in the PRA remain valid for the as-to-be-operated plant. Because the applicant documented the assumptions related to this evaluation, and because these assumptions will be evaluated by the staff in response to COL Information Item 19.1-9 to ensure they are consistent with plant construction and operation, the staff concludes that the treatment of inter-system CCF at the design stage is acceptable.

Finally, software CCFs were modeled as failure modes of systems actuated by the PS. The PRA includes an operating system failure that disables all actions performed by the TXS software (assigned a 1E-7 failure probability) and an application software failure that disables actions performed by a specific diversity group within the PS (assigned a 1E-5 failure probability). The two diversity groups are assumed to be functionally diverse and independent with different application software; the staff observes that although CCFs between the diversity groups are unlikely, the operating system failure demonstrates the effects of a CCF. In RAI 227, Question 19-284, the staff requested additional information on these failures to conclude that the low postulated failure rates do not result in an overly optimistic estimation of risk. Specifically, the applicant was requested to justify the operating system and software probabilities and associated uncertainty parameters, as well as to perform additional sensitivity studies. **RAI 227, Question 19-284, which is associated with the above request, is being tracked as an open item.**

In addition, in RAI 227, Question 19-292, the staff requested more information on software CCFs that could both cause an initiating event and affect mitigation. **RAI 227, Question 19-292, which is associated with the above request, is being tracked as an open item.**

Additional discussion on software CCF as a source of modeling uncertainty is provided in Section 19.1.4.4.5.1 of this report.

Human Reliability Analysis. FSAR Tier 2, Section 19.1.4.1.1.5 discusses the HRA performed to evaluate the failure probabilities of both pre-initiator and post-initiator operator actions. Pre-initiator actions, which occur during testing or maintenance, could cause a system not to function if they are not performed correctly. Post-initiator actions are steps that operators must take after an initiating event to start or control a system or compensate for a system failure.

Pre-Initiator Actions. The applicant identified pre-initiator operator actions by making test and maintenance assumptions based on engineering judgment and experience with current plants. The HEPs were estimated using the method documented in NUREG/CR-4772, "Accident

Sequence Evaluation Program [ASEP] Human Reliability Analysis Procedure," dated February 1987. Failures to restore equipment after test or maintenance activities are considered negligible if the component (often a valve) has a status indication in the control room.

In performing the ASEP analysis, the applicant used a screening HEP of 0.03 instead of the 0.05 value recommended for cases where no plant visit or interaction is available. In RAI 7, Question 19-69, the applicant was requested to perform a sensitivity study using the recommended value. In a June 16, 2008, response, the applicant concluded that the change would have a four percent impact on the total CDF. Given this small increase and that the PRA will be updated to reflect the as-built, as-operated plant, the staff concludes that the use of the 0.03 screening HEP does not impact the results and insights of the U.S. EPR design-specific PRA at the design stage.

In RAI 2, Question 19-10, and RAI 14, Question 19-128, the staff requested that the applicant justify changing the level of dependence between post-maintenance testing and independent verification from complete to medium. In an April 30, 2008, response, the applicant clarified this statement from the FSAR. The applicant assumed that the two recovery actions are likely to be performed in different time steps with different crews. In a July 11, 2008, response, the applicant provided additional justification for the statement that the change was not significant, based on Fussell-Vesely (FV) importance measures for the failure parameter and a sensitivity study using complete dependence between testing and independent verification. The additional information is sufficient for the staff to conclude that the impact of the change on the overall PRA results was small. The change is also included as Item 26 in FSAR Tier 2, Table 19.1-109, "U.S. EPR PRA General Assumptions." Actions that could lead to calibration errors are not considered in the design-phase PRA, because detail on design and calibration practices is not yet available. This omission is listed as Item 49 in FSAR Tier 2, Table 19.1-109. As stated in the second note below the table, the PRA assumptions will be re-evaluated as part of the PRA maintenance and update process (discussed above in the evaluation of FSAR Tier 2, Section 19.1.2), and COL Information Item 19.1-9 is provided to confirm that assumptions used in the PRA remain valid for the as-to-be-operated plant.

Post-Initiator Actions. Post-initiator human actions generally occur after multiple failures of safety-related equipment (e.g., initiation of feed and bleed or starting the SBODGs in an SBO). Because emergency operating guidelines and procedures are not yet available, the post-initiator actions are identified based on engineering judgment and experience with current plants. The HEPs were estimated using the method documented in NUREG/CR-6883, "The SPAR-H [Standardized Plant Analysis Risk—HRA] Human Reliability Analysis Method," dated August 2005.

The probability estimates stem from a comparison of the time available (estimated from thermal-hydraulic analyses) to the time needed for diagnosis and action, modified by several performance shaping factors (PSFs). The PSFs for stress and complexity are assigned based on engineering judgment and the characteristics of the accident sequence. The PSFs for experience and training, procedures, ergonomics, fitness for duty, and work processes are generally assumed to be one (the value for "insufficient information") until detailed design information is available. Only scenarios that are likely to receive extensive training (such as initiation of feed and bleed or RCS cooldown) have been assigned an "experience and training" PSF of 0.5.

Dependence between operator actions was assigned by considering changes in crew, time and location of the actions, and similarity of cues. NUREG-1792, "Good Practices for Implementing

Human Reliability Analysis (HRA)," dated April 2005, recommends that the total combined probability of all human failures in a core damage cutset should not be less than a defined value, such as 1E-5. In RAI 7, Question 19-70, the applicant was requested to address this recommendation. In a June 16, 2008, response, the applicant stated that only a small number of HEP combinations result in a combined probability of less than 1E-5, and that these combinations apply to situations for which no dependency exists based on the type of task, crew, or time window. A sensitivity case limiting the minimum combined HEP to 1E-5 resulted in a CDF increase of one percent. Based on the minimal increase shown in the sensitivity study, the staff concludes that cutset frequencies have not been inappropriately lowered by combined HEPs, and that the approach is acceptable.

For both types of human errors, the HEP was quantified using the EPRI HRA Calculator, a software tool that guides the PRA analysts through the ASEP and SPAR-H methods.

Model Quantification. The event trees from the accident sequence analysis and the fault trees from the system modeling are quantified together using the RiskSpectrum® computer code. A 1E-20/yr truncation limit and a 1E-6/yr relative truncation limit are used in the quantification, resulting in over 73,000 minimal cutsets.

In RAI 227, Question 19-288, the staff requested that the applicant justify the truncation limits used in the quantification. In a July 6, 2009, response, the applicant provided the results of a sensitivity study demonstrating that the selection of lower truncation limits would not significantly change the results, though it would increase the time required to quantify the model. The results of the LOOP event tree (a significant contributor to the PRA) do not significantly change for absolute truncation limits below 1E-13/yr and relative truncation limits below 1E-7/yr. The increase in CDF caused by reducing the relative truncation limit from 1E-6/yr to 1E-8/yr is approximately four percent, but the quantification time approximately triples. The applicant also clarified that the relative truncation limit is used to generate a cutoff value proportional to the total frequency of the minimal cutsets as they are quantified. Because the internal events CDF estimate is on the order of 1E-7/yr, this relative limit results in an effective truncation limit of approximately 1E-13. Based on this information, the staff concludes that the selected truncation limits do not inappropriately exclude important cutsets and are therefore acceptable.

The applicant performed uncertainty analyses using Monte Carlo simulation within the RiskSpectrum® program, using the probability distributions associated with initiating event frequencies, failure rates, CCF probabilities, and HEPs. Modeling uncertainty was quantified to a limited extent by postulating several possible cases. Sensitivity studies were also performed to address uncertainty in success criteria and assumptions made in the PRA model. These uncertainty and sensitivity studies, performed by the applicant, are discussed below.

19.1.4.4.2.2 *Significant Accident Sequences Leading to Core Damage*

FSAR Tier 2, Table 19.1-6 presents the initiating events whose accident sequences contribute more than one percent to the overall internal events CDF. Accidents initiated by LOOP events contribute the most—nearly 50 percent—to overall risk. The applicant states that this contribution is not surprising, since the U.S. EPR depends on active systems that need electrical power for operation. This 50 percent is divided as follows:

- Thirty percent is contributed by LOOP events that result in neither an RCP seal LOCA nor an SBO.

- Ten percent comes from LOOP events that lead to an SBO.

- Five percent results from LOOP events with a subsequent RCP seal LOCA.

- Five percent represents LOOP events followed by both an SBO and an RCP seal LOCA.

Significant accident sequences are presented by the applicant in two ways. Table 19.1-127 in the applicant's July 24, 2009, response to RAI 227, Question 19-285, lists all sequences contributing more than one percent to the internal events CDF. **Inclusion of this table, as well as Tables 19.1-128, 19.1-129, and 19.1-130, and appropriate references in the FSAR text, is being tracked as Confirmatory Item 19-285.** For each sequence, the table provides the related event tree, sequence number, sequence identifier, total frequency, and description. The top seven sequences, representing about 65 percent of the internal events CDF, are listed below with rounded sequence frequencies.

- LOOP-14 (8.6E-8/yr): LOOP with offsite power not recovered in 2 hrs, followed by failures of EFWS and pressure relief needed for feed and bleed (dominated by HVAC failures), resulting in a loss of all heat removal.

- GT-15 (2.0E-8/yr): Reactor trip that causes a consequential LOOP and failure of MFW and SSS, followed by failures of EFWS and pressure relief needed for feed and bleed (dominated by HVAC failures), resulting in a loss of all heat removal.

- SLOCA-17 (2.0E-8/yr): Small LOCA with failures of SSS and EFWS (dominated by failure of the PCD function), followed by operator failure to initiate feed and bleed, resulting in a loss of all heat removal.

- SLOCA-34 (1.7E-8/yr): Small LOCA with failure of MHSI, followed by operator failure to perform a fast cooldown to enable LHSI, resulting in a loss of the needed injection capability.

- LOOP-45 (1.7E-8/yr): LOOP with offsite power not recovered in 2 hrs, followed by failure of the four EDGs and two SBODGs, resulting in a total loss of ac power and unavailability of all mitigating systems.

- LOOP-44 (1.1E-8/yr): LOOP with offsite power not recovered in 2 hrs, followed by failure of the four EDGs and EFWS, resulting in a total loss of heat removal, because feed and bleed depends on Class 1E power.

- SLBI-40 (1.0E-8/yr): SLBI followed by failure of all steam and feedwater isolation (dominated by CCF of the related PS diversity group), resulting in blowdown of all four SGs and an uncontrolled reactivity event caused by the overcooling.

FSAR Tier 2, Table 19.1-7, "U.S. EPR Important Cutset Groups - Level 1 Internal Events," to which FSAR Tier 2, Table 19.1-127 refers, describes the sequences in more detail by presenting the top 100 cutsets in 24 groups, representing over 50 percent of the total CDF. This treatment provides a slightly different ranking and total frequency, because many lower-frequency cutsets are included in the total sequence frequencies in FSAR Tier 2, Table 19.1-127. The top ten cutset groups are listed below.

- Group 1 (19.3 percent): This group represents a LOOP sequence in which offsite power is not recovered within 2 hrs, and heat removal by both EFWS and feed and bleed fails. In the representative cutset, the SCWS air-cooled chillers in

Divisions 1 and 4 fail to start. Without operator recovery of room cooling, the Division 1 and 4 CCWS pumps fail, switchover to the standby pumps fails, and HVAC is lost to all four SBs.

- Group 9 (3.8 percent): This group represents an SLOCA sequence in which all heat removal (via SSS, EFWS, and feed and bleed) fails. In the representative cutset, the MSRIVs fail to open because of a common cause, disabling the RCS cooldown function, and the operator fails to initiate feed and bleed cooling.

- Group 17 (3.5 percent): This group represents an ATWS when MFW is unavailable; as a result, pressure relief is not credited. In the representative cutset, a total loss of MFW initiator is followed by stuck control rods.

- Group 8 (3.3 percent): This group represents an SLOCA sequence in which inventory control fails—MHSI fails and the operator fails to initiate a fast cooldown to enable LHSI. In the representative cutset, all four MHSI pumps fail to run because of a common cause, and the operator fails to initiate a fast cooldown.

- Group 18 (3.2 percent): This group represents a general transient sequence in which all heat removal (via MFW, SSS, EFWS, and feed and bleed) fails. This sequence and its representative cutset are the same as Group 1, except that there is a consequential LOOP following a plant trip rather than a LOOP initiator.

- Group 16 (3.0 percent): This group represents an SGTR or induced SGTR, followed by failure to isolate the ruptured SG and operator failure to stop the leak by depressurizing the RCS and initiating RHRS. In the representative cutset, the MSIV for the ruptured generator fails to close and the operator fails to initiate RHRS.

- Group 15 (2.5 percent): This group represents a SLBI sequence, followed by failure of both main steam and feedwater isolation. In the representative cutset, the isolation failure is caused by a CCF of the PS diversity group B software.

- Group 11 (2.1 percent): This group represents a SLOCA sequence in which both MHSI and the accumulators fail to restore inventory. In the representative cutset, CCF of the common SIS injection check valves results in a loss of all injection.

- Group 4 (2.1 percent): This group represents a complete SBO. That is, an unrecovered LOOP occurs and all six EDGs and SBODGs fail, resulting in failure of all methods of inventory control and heat removal. In the representative cutset, all four EDGs fail to run because of a common cause, and the two SBODGs fail to run independently.

- Group 3 (1.9 percent): This group represents a LOOP event in which the EDGs and I&C fail. In the representative cutset, CCF of the safety-related batteries prevents starting of the EDGs and causes a loss of all instrumentation, which disables offsite power recovery and SBODG starting.

19.1.4.4.2.3 *Risk-Significant Failures*

The risk-significant equipment failures, human errors, and CCFs modeled in the U.S. EPR design-specific PRA are tabulated in FSAR Tier 2, Tables 19.1-8 through 19.1-11. These

failures are ranked by their risk achievement worth (RAW) and FV importance measures. RAW values show the factor by which overall CDF would increase if an operator action or a particular piece (or set, for CCFs) of equipment were certain to fail. FV values indicate the fraction of CDF that comes from cutsets that include a particular human error, equipment failure, or CCF; if that failure could be made impossible, CDF would decrease by that fraction.

The most risk-significant equipment failures, ranked by FV importance, are failures of a single EDG or a Division 1 or 4 SCWS chiller unit train. EDG failures appear in cutsets that contribute about 20 percent of the CDF. Chiller train failures (which can lead to failure of two divisions' electrical and EFWS systems) appear in cutsets that contribute about 15 percent of the CDF. When the equipment failures are ranked by RAW importance, the most important are failures of a single 250V dc bus. Because the dc bus failure would disable isolation after a break or the entire division after a LOOP, CDF would increase by a factor of about 30 if the bus were always certain to fail. (The EFWS storage tanks were initially identified as important, but their significance is expected to decrease when the design change isolating the four EFWS trains is incorporated in the PRA, as described above in the evaluation of FSAR Tier 2, Section 19.1.2.4. **The revision to the PRA, which is associated with the request in RAI 289, Question 19-329, is being tracked as an open item.**

The most risk-significant human error for both FV and RAW importance is failure of the operator to recover room cooling locally. An unrecovered failure of certain HVAC components can lead to multiple failures, as discussed above. This human error appears in cutsets that contribute about 40 percent of the CDF. Overall CDF would increase by a factor of about 30 if the operator never recovered room cooling when needed. When ranked by RAW importance, operator failures to depressurize and initiate RHRS or to initiate feed and bleed after a transient are also important. If the operator always failed to initiate RHRS, CDF would increase by a factor of about 30. If the operator always failed to initiate feed and bleed, CDF would increase by a factor of about 15.

As expected, CCFs have a much larger effect on overall risk, because they can disable one or more systems. The RAW rankings show that CCFs that disable the safety-related batteries, injection from the IRWST, or the HVAC system are most important. In addition, all CCFs of I&C have high RAW values, because these failures can prevent multiple safety systems from actuating.

The tables provided in the FSAR Tier 2 do not include all failures with importance measures above the thresholds stated on FSAR Tier 2, page 19.1-54 (RAW of 2 or FV of 0.005); instead, components and failure modes are grouped to identify risk-significant components. In RAI 14, Question 19-126, the staff requested additional information on the importance measures. In a July 11, 2008, response, the applicant confirmed that the complete list of equipment failures and operator actions above the thresholds was used as input to other programs (e.g., RAP). In the same response, the applicant submitted 36 tables of specific failures and importance measures for the staff's review. This additional information gave the staff confidence that the most important equipment failures and operator actions were captured in the FSAR and that the appropriate input was provided to other programs.

19.1.4.4.2.4 *Insights from the Uncertainty and Sensitivity Analyses*

Parametric Uncertainty. The applicant quantified parametric uncertainty in the CDF results by propagating uncertainty distributions within the RiskSpectrum® software. For initiating events and equipment failures, the uncertainty parameters were obtained from the same source as the failure data. Initiating events modeled by fault trees were assigned uncertainty parameters by

fitting a lognormal distribution to the distribution obtained when quantifying the fault tree. Common cause uncertainty parameters were obtained from the same source as the CCF probabilities, then fit to a lognormal distribution and applied to the CCF beta parameter. For digital I&C failure rates, a lognormal distribution with an error factor (EF) of five was estimated from confidence intervals in the TXS documentation. Pre-accident HEPs were assigned a lognormal distribution with an EF of 10, as recommended by the ASEP documentation. Post-accident HEPs and various undeveloped events were assigned a constrained non-informative (CNI) prior beta distribution. Finally, time-related parameters such as maintenance unavailability were assigned lognormal distributions with EFs estimated from upper and lower time estimates.

Modeling Uncertainty. The applicant also addressed modeling uncertainty for three cases where design details are incomplete and different success criteria are observed in the global EPR PRAs. Probabilities of conditions within each case were estimated using engineering judgment. Therefore, the RiskSpectrum® uncertainty calculation considers the weighted average of the options for each case. These cases are described below.

EFWS Success Criterion (Case 1). Because the EFWS pump flow curve is not finalized, it is uncertain how many EFWS trains are needed for secondary heat removal when the MSSVs are used for SG relief. In a December 8, 2008, response to RAI 133, Question 19-246 (discussed in Section 19.1.4.4.2.2 of this report), the applicant provided detailed success criteria based on MAAP analyses, showing that the EFWS success criterion depends whether the MSRTs or MSSVs are used for SG relief (one or two trains, respectively).

In RAI 2, Question 19-46, the staff requested additional detail on this modeling uncertainty case. In an April 30, 2008, response, the applicant clarified that one to four EFWS pumps might be needed after a loss of MFW (assigned probabilities of 0.3, 0.5, 0.15, and 0.05, respectively) and one to three EFWS pumps might be needed after a LOOP with RCPs tripped (assigned probabilities of 0.5, 0.3, and 0.2, respectively). Higher CDF estimates would be expected with a more restrictive success criterion than that assumed in the baseline PRA (three or four trains, representing 20 percent of the cases).

PSRV Success Criterion (Case 2). Because conservative assumptions are made about PSRV bleed capability during the design phase, it is not certain how many PSRVs are required for successful feed and bleed. The baseline PRA assumes that all three PSRVs must open to provide an adequate primary bleed path. In RAI 7, Question 19-77, the staff requested that the applicant discuss this success criterion. In a June 16, 2008, response, the applicant stated that a few MAAP cases showed that two PSRVs may lead to success if different timings for feed-and-bleed actuation are selected.

In RAI 2, Question 19-46, the staff requested additional detail on this modeling uncertainty case. In an April 30, 2008, response, the applicant clarified that the sub-case of one PSRV required was assigned a probability of 0.1, two PSRVs required was assigned a probability of 0.4, and three PSRVs required was assigned a probability of 0.5. Lower CDF estimates would be expected with a less restrictive success criterion than that assumed in the baseline PRA (one or two PSRVs, representing 50 percent of the cases).

HVAC Recovery Time (Case 3). Because information on room heat-up rates and equipment survivability is not available, the success criterion for recovery of HVAC to the SBs is uncertain. In FSAR Tier 2, Table 19.1-109, the applicant documented the assumption that a loss of function occurs about 2 hrs after a loss of HVAC and that operator recovery during this time is

possible (OPF-SAC-2H basic event) (operator fails to recover room cooling locally). This modeling will be refined when final building heat loads are known.

In RAI 2, Question 19-46, the staff requested additional detail on this modeling uncertainty case. In an April 30, 2008, response, the applicant clarified the sub-case probabilities. A probability of 0.05 was assigned to the sub-case in which no recovery is required and to the sub-case in which no recovery is possible. A probability of 0.4 was assigned to the sub-case in which recovery is needed in 4 hrs. Finally, a probability of 0.5 was assigned to the sub-case in which recovery is required in 2 hrs. Lower CDF estimates would be expected with a less restrictive success criterion than that assumed in the baseline PRA (4 hrs available or no recovery needed, representing 45 percent of the cases).

The staff observes that, although knowledge about the systems informed the engineering judgment, the relative weights of each case remain uncertain. Although the approach to modeling uncertainty is a somewhat arbitrary investigation of the combined effects of these uncertainties, some important insights can be obtained, as discussed in Section 19.1.4.4.6 of this report.

Uncertainty Results. FSAR Tier 2, Figure 19.1-5, "U.S. EPR Level 1 Internal Events Uncertainty Analysis Results - Cumulative Distributions for Internal Events CDF," shows the results of the uncertainty evaluation for Level 1 internal events at power, which were updated by the applicant following a commitment in the May 30, 2008, response to RAI 2, Question 19-5 (discussed below).

The state-of-knowledge correlation inherent in the model contributes to a mean value higher than the point estimate. In the Monte Carlo sampling approach, the same value is used for each failure probability within a correlated group that uses the same failure data (i.e., the "state of knowledge" about each failure is the same). For cutsets that involve failures of multiple redundant pieces of equipment, the correlation results in a mean value that is larger than the product of the mean values of the event probabilities.

In RAI 2, Question 19-5, the staff requested additional information on this state-of-knowledge correlation. In a May 30, 2008, response, the applicant stated that the impact of redundant equipment is more important in those cases where equipment independent failures are significant contributors to the results, as in the case of the DGs. The applicant changed the DG modeling so that EDG and SBODG failure rates are no longer correlated, because the two types of DGs are assumed to have different vendors, locations, cooling and starting systems, and fuel supplies. The change in this assumption led to a significant reduction in the mean value. In Revision 0 of the FSAR, the mean CDF of 1.8E-6/yr was nearly an order of magnitude higher than the point estimate of 2.9E-7/yr. After the change, the mean value of 4.2E-7/yr is about 45 percent higher than the point estimate of 2.9E-7/yr.

The broken curve of FSAR Tier 2, Figure 19.1-5 shows the effect of the modeling uncertainty cases discussed above; the mean value for this distribution is 2.3E-6/yr, about five times the mean value considering parametric uncertainty.

Insights obtained from these uncertainty analyses are discussed in more detail in Section 19.1.4.4.6 of this report.

Sensitivity Analyses. The applicant also performed more than 25 sensitivity cases to evaluate the impact of modeling assumptions on the internal events CDF. The results of these cases are

tabulated in FSAR Tier 2, Table 19.1-15. Based on these studies, the applicant obtained several insights:

- The results are sensitive to HEP values. CDF more than triples if all HEPs are set to their 95th percentile values. As discussed above, CDF would increase by a factor of about 30 if operators always failed to recover room cooling locally.

- Risk is sensitive to assumptions related to electrical power. CDF nearly triples if offsite power recovery is not credited and nearly quadruples if EDGs and SBODGs are put in the same CCF group.

- If Division 3 equipment is taken out of service for the entire year, CDF approximately doubles. The applicant states that this evaluation is not equivalent to the risk of a three-train plant, because some simplifying assumptions were made for support systems. In RAI 2, Question 19-44, the staff requested a discussion of these simplifying assumptions. In an April 30, 2008, response, the applicant clarified that this statement refers to assumptions that make the model asymmetric, such as where breaks occur (Division 4) and which trains of CCWS are initially running (Divisions 1 and 4).

- In a sensitivity case that combined several assumptions (including all diesel generators in the same CCF group, diesel generator mission time set to 24 hours, consequential LOOP probabilities increased, HEPs set to 95th percentile value, and RCP seal LOCA probability set to 1.0), CDF increased by a factor of about 15 to 4.6E-6/yr.

Sensitivity studies did not identify any cases where a design change would lead to a significant reduction in CDF. If the MSRIVs were realigned such that two electrical divisions were not needed for operation, CDF would decrease by seven percent. In RAI 2, Question 19-45, the applicant was requested to discuss the evaluation of design changes. In an April 30, 2008, response, the applicant described the evaluation of other design changes that were considered but not documented in the FSAR.

In addition to the sensitivity studies documented in the FSAR, the applicant performed numerous sensitivity studies to support RAI responses. Generally, these sensitivity studies demonstrated that a particular modeling assumption or simplification questioned by the staff had no significant impact on the results and insights of the PRA. That is, they do not evaluate key sources of uncertainty for the PRA. These additional sensitivity studies are summarized below.

- In a June 16, 2008, response to RAI 7, Question 19-56, the applicant described a sensitivity study related to the SSSS failure probability. The applicant assumed an SSSS failure probability of 1E-3 based on engineering judgment regarding the simple, passive design. A sensitivity case increasing the SSSS failure probability by one order of magnitude resulted in a 10 percent CDF increase. Given this relatively small impact and the reduction of seal LOCA (and thereby SSSS) importance following the thermal barrier cooling design change described above, the staff concludes that this assumption does not significantly impact the PRA results and insights.

- In a June 16, 2008, response to RAI 7, Question 19-58, the applicant described a sensitivity study related to the total loss of CCWS (LOCCW) initiating event

frequency. If this frequency were increased by an order of magnitude, internal events CDF would increase by about 12 percent. Therefore, even though the frequency is significantly lower than LOCCW frequencies reported for operating plants, the difference can be explained by the four independent trains and the low value does not significantly impact the PRA results and insights.

- In a June 16, 2008, response to RAI 7, Question 19-61, the applicant described a sensitivity study related to ISLOCA. The evaluation of an ISLOCA due to a RCP thermal barrier tube leak does not consider dependence between operator failure to isolate the ISLOCA and operator failure to initiate secondary cooling and align the RHRS in 4 hours. The applicant acknowledged that this dependence should have been considered, but demonstrated that the corresponding increase in internal events CDF would be negligible. Therefore, the exclusion does not significantly impact the PRA results and insights.

- In a June 16, 2008, response to RAI 7, Question 19-68, the applicant described several sensitivity studies performed to illustrate the effect of digital I&C modeling uncertainty. These cases and their results are summarized in Table 19.1-4 of this report. The cases showed that total CDF is moderately sensitive to the assumed low software CCF probability; a 33 percent increase in CDF was estimated when software CCFs were increased by an order of magnitude. In addition, increasing HEPs in cutsets that also include digital I&C CCFs has a significant effect on the overall results (more than 100 percent increase). Given that digital I&C failure probabilities are acknowledged as an area of uncertainty in the PRA (see CCF discussion above), these sensitivity studies provide important insights and illustrations.

- In a June 16, 2008, response to RAI 7, Question 19-69, the applicant described a sensitivity study related to the basic post-accident HEP. In the HRA, the applicant used a screening HEP of 0.03 rather than the value of 0.05 recommended for cases where no plant visit or interaction is possible, as is the case at the design certification stage. In a sensitivity case, the applicant increased the median basic HEP from 0.03 to 0.05, resulting in a two-percent increase in internal events CDF. Given this small increase and the commitment that the PRA will be reviewed by COL holders to ensure it reflects the as-built, as-operated plant, the staff concludes that this assumption does not significantly impact the PRA results and insights.

- In a June 16, 2008, response to RAI 7, Question 19-70, the applicant described a sensitivity study related to sequences containing multiple operator actions. The applicant did not set an absolute lower bound for combinations of HEPs within the same sequence. In a sensitivity case using a value of 1E-5 for combinations of human errors identified as having a lower combined probability, the applicant estimated an increase of 1 percent in total at-power CDF. Therefore, this assumption does not significantly impact the PRA results and insights.

- In a July 11, 2008, response to RAI 14, Question 19-128, the applicant described a sensitivity study related to dependence in the HRA. The applicant used medium (rather than complete) dependence for the relationship between post-maintenance testing and independent verification in the HRA. The results of a sensitivity study in which complete dependence was assumed showed an

increase of three percent in the at-power CDF. Therefore, this assumption (for which additional justification was provided) does not significantly impact the PRA results and insights.

- In an August 15, 2008, response to RAI 26, Question 19-163, the applicant described a sensitivity study related to CCF of the operators' control interface. The applicant assumed that the process information and control system (PICS) and SICS are implemented on diverse I&C platforms and are not vulnerable to the same CCF. The applicant defined a sensitivity case in which a CCF could occur, disabling all operator actions; in this case, total CDF increased by 0.2 percent. Even if the systems were susceptible to an unlikely CCF, this assumption does not significantly impact the PRA results and insights.

- In an August 15, 2008, response to RAI 26, Question 19-165, the applicant described a sensitivity study related to circular logic in the PRA. The applicant used zero-probability undeveloped basic events to represent power supplies for the HVAC, CCWS, and ESWS systems. In a sensitivity case, the applicant increased the failure probabilities to values calculated from fault trees for these power supplies. Because total CDF increased by one percent, the staff determines that this assumption does not significantly impact the PRA results and insights.

- In an August 15, 2008, response to RAI 26, Question 19-170, the applicant described a sensitivity study related to the alternate feed configuration. An alternate feed connection is included in the U.S. EPR design to provide a normal and standby source of power when certain electrical components, including an EDG, are out of service. This connection is not modeled in the PRA for the scenario when an EDG is out of service for maintenance. If the EDG were in maintenance all year, the applicant estimated a four percent reduction in total CDF by modeling the alternate feed connection. However, since the PRA assumes about two weeks of maintenance per year, the realistic effect would be even smaller. Therefore, this exclusion does not significantly impact the PRA results and insights.

- In a September 22, 2008, response to RAI 53, Question 19-200, the applicant described a sensitivity study related to early operator actions. The U.S. EPR design philosophy includes the expectation that operator actions are not required within the first 30 minutes for control room actions or the first 60 minutes for local actions. The applicant identified several control room actions credited in the PRA that occur within 30 minutes after an initiating event, but no local actions that occur within 60 minutes. The applicant evaluated failure probabilities of these actions based on PSFs including the amount of time available relative to the time needed. If these operator actions were not credited, total at-power CDF would increase by 12 percent. Therefore, including these actions has a slight effect on the PRA results, but makes the PRA more realistic. The staff concludes that it is acceptable to model a small number of operator actions that must be performed in the control room in less than 30 minutes.

- In a December 19, 2008, response to RAI 138, Question 19-247, the applicant described a sensitivity study related to the thermal barrier cooling design change described above. Internal events CDF decreased by three percent; the reduction

of the fire and flood CDF was more significant. As described above, the applicant clarified that the reduction was driven by a smaller seal LOCA contribution. The numerical results of this sensitivity study were updated in a September 1, 2009, response to RAI 257, Question 19-316(l), but the general conclusions were not affected. **Incorporation of these changes in the PRA, which is associated with the request in RAI 289, Question 19-329, is being tracked as an open item.**

- In a December 19, 2008, response to RAI 138, Question 19-248, the applicant described a sensitivity study related to hot leg injection. For simplicity, the PRA does not model switchover to hot leg injection to prevent boron precipitation following a large LOCA. In the sensitivity study, the applicant modeled this operator action and estimated a 0.02 percent increase in total CDF (five percent increase in large LOCA CDF). The applicant concluded that this simplification does not significantly impact the PRA results and insights. Based on this small impact, the staff concludes that excluding the switchover action is acceptable.

- In a February 11, 2009, response to RAI 138, Question 19-249, the applicant described a sensitivity study related to running and standby CCWS pumps. As discussed above, the applicant evaluated several CCWS pump rotation strategies to determine their impact on overall risk. Although operation of Divisions 2 and 3 all year would result in about 40 percent lower risk than operating Divisions 1 and 4 all year, the realistic rotation strategies all resulted in similar CDF estimates (about 20 percent less than the baseline CDF). The applicant concluded that the overall risk is low, and no design changes or procedural guidance related to risk-important strategies is needed. The staff's conclusion on this study is discussed above in Section 19.1.4.4.2.1, subsection entitled, "System Modeling," of this report.

- In an April 10, 2009, response to RAI 197, Question 19-274, the applicant described a sensitivity study related to the EFWS design change described above. Internal events CDF increased by six percent as a result of the additional operator actions required. **Incorporation of these changes in the PRA, which is associated with the request in RAI 289, Question 19-329, is being tracked as an open item.**

- In an August 17, 2009, response to RAI 257, Question 19-318, the applicant described a sensitivity study crediting an operator action to perform a CCWS common header switchover when HVAC is lost in the building supplying the common header. As discussed above, total at-power CDF decreased by 20 percent as a result of the new mitigation action, but the overall PRA results and conclusions did not change significantly.

Table 19.1-4 Digital I&C Sensitivity Study Results (Response to RAI 7, Question 19-68)

Case	Model Changes	CDF	Percent Increase in CDF
1	Increase both operating system and application software CCF probabilities by one order of magnitude (10X). Remove 0.5 software CCF recovery probability (a conservative estimate for operator recovery that also bounds the reliability of possible automated backups).	7.0E-7	33
2	Same as case 1, but without credit for the backup reactor trip performed by DAS.	7.3E-7	39
3	Same as case 1, plus increase the CCF beta factors for digital components by one order of magnitude (10X).	7.0E-7	33
4	Same as case 3, plus increase all HEPs appearing in cutsets with digital I&C CCFs by one order of magnitude.	1.1E-6	102

In summary, 10 CFR 52.47(a)(23) requires that the applicant describe the design-specific PRA and its results. The discussion above provides the staff's evaluation of the applicant's description of the Level 1 PRA for operation at power and its results, as well as of related issues raised in RAIs. The staff reviewed detailed results including data, sequence, and importance measures and requested justification of specific aspects of the PRA described in the FSAR. This review was sufficient to determine that the Level 1 PRA for internal events occurring at power appropriately reflects the U.S. EPR design. Additional discussion related to the scope, level of detail, and technical adequacy of the PRA in general was discussed in the staff's evaluation of FSAR Tier 2, Section 19.1.2 above. Therefore, the staff concludes, based on the detailed information described above, that the applicant has provided an adequate description of the design-specific internal events PRA, as well as its results, sufficient for the staff to obtain risk insights about the U.S. EPR design.

19.1.4.4.3 Use of PRA to Establish Specifications and Objectives

SRP 19.0 states that the staff should ensure that the applicant has used the PRA results and insights in an integrated fashion to identify and establish specifications and performance objectives for the design, construction, testing, inspection, and operation of the plant. The staff evaluates this acceptance criterion by reviewing PRA input to the design process (FSAR Tier 2, Section 19.1.3.4), PRA input to other programs (FSAR Tier 2, Section 19.1.7), and the applicant's list of COL information items. The staff also reviews the applicant's development of PRA-based insights. In RG 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)," the staff defined the "PRA-based insights" that should be included in applications (see note 8 on page C.I.19.A-5 of RG 1.206):

> PRA-based insights" are those insights identified during the [design certification] process that ensure that assumptions made in the PRA will remain valid in the as-to-be-built, as-to-be-operated plant and include assumptions regarding SSCs and operator performance and reliability, ITAAC, interface requirements, plant features, design and operational programs, and others. The usage of this phrase

is intended to be consistent with its use in referring to the information provided in Table 19.59-29 in the [Westinghouse] AP600 design control document [DCD].

In the AP600 DCD, each insight receives a disposition such as a reference to another portion of the DCD, an ITAAC, or a COL information item. FSAR Tier 2, Revision 0, Table 19.1-102, "Summary of Insights from the PRA of the U.S. EPR," did not include a similar disposition for each insight to ensure that the table reflects all important assumptions and insights that must remain valid for future plants. In RAI 2, Question 19-02, the staff addressed this information need. In a May 30, 2008, response, the applicant provided an update to FSAR Tier 2, Table 19.1-102.

However, in RAI 26, Questions 19-166 and 19-167, the staff identified that the disposition of insights could be tied to portions of the FSAR that provide stronger assurance that the insight will remain valid (e.g., Tier 1, ITAAC, and COL information items) and that multiple assumptions that should be communicated to COL applicants were not included in the table. In an October 31, 2008, response, the applicant committed to revise the FSAR. The staff confirmed that Revision 1 of the U.S. EPR FSAR, dated May 29, 2009, contains the changes committed to in the RAI response. This change divides the original Table 19.1-102 into three separate 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 Modeling Assumptions

FSAR Tier 2, Table 19.1-102 relates to the reduction of risk in the U.S. EPR design and is discussed in the section below. The other two tables document two categories of "risk insights."

FSAR Tier 2, Table 19.1-108 lists insights about the design that were developed as a result of the PRA process (e.g., importance of ac power and mid-loop level control). Each of these insights is linked to an FSAR section or COL information item that provides additional details. Several of the insights relate to portions of the design that are not yet developed, such as procedures (especially shutdown and fire protection). FSAR Tier 2, Section 18.6.2, "Human Reliability Analysis – Methodology," describes the identification of risk-significant operator actions in the context of the human factors engineering (HFE) program. The tabulation of insights provides a ready reference to U.S. EPR designers to ensure that PRA insights are considered in future design development. Throughout the review process, NRC staff also shared these insights with staff from other technical branches (e.g., the branches responsible for the HRA and minimum inventory described in FSAR Chapter 18) to ensure that the underlying assumptions were appropriate and that issues were identified.

In contrast, FSAR Tier 2, Table 19.1-109, "U.S. EPR PRA General Assumptions," lists important modeling assumptions. In an October 31, 2008, response to RAI 26, Question 19-167, the applicant reviewed over 1,200 assumptions and grouped them according to commonality, importance, and the need to update the PRA model. The resulting list consists primarily of those that need to be reviewed for applicability in a future plant-specific PRA update. Information for these assumptions will come from the plant operating procedures or from an "as-built-as-operated" plant. Each assumption is assigned a category corresponding to the element of PRA development. Note 2, following the table, ties the content of the table to the PRA update process:

> The PRA assumptions will be re-evaluated as part of the PRA maintenance and update process. The PRA maintenance and upgrade process is described in U.S. EPR FSAR Tier 2, Section 19.1.2.4. COL Information Item 19.1-9 listed in FSAR Tier 2, Table 1.8-2 − U.S. EPR Combined License Information Items is provided to confirm that assumptions used in the PRA remain valid for the as-to-be-operated plant.

The staff expects that COL holders will perform this task as part of the PRA development required by 10 CFR 50.71(h)(1):

> No later than the scheduled date for initial loading of fuel, each holder of a combined license under subpart C of 10 CFR part 52 shall develop a level 1 and a level 2 probabilistic risk assessment (PRA). The PRA must cover those initiating events and modes for which NRC-endorsed consensus standards on PRA exist one year prior to the scheduled date for initial loading of fuel.

The staff expects to use FSAR Tier 2, Table 19.1-109, in its confirmation that both the COL information item (which is documented as a license condition in COL applications referencing the U.S. EPR design that have been submitted to the NRC) and the regulation have been met. Therefore, based on the information provided in the FSAR, the staff concludes that the applicant has appropriately identified and documented insights and assumptions from the shutdown PRA.

In RAI 257, Question 19-316, the staff requested that the applicant address several inconsistencies and areas needing clarification in FSAR Tier 2, Tables 19.1 2, 19.1-5, 19.1-102, 19.1-108, and 19.1-109. In two responses dated August 17, 2009, and September 1, 2009, the applicant proposed multiple revisions to these tables, as well as to several other FSAR sections that the tables reference. The staff reviewed the response and determined that these tables now link to appropriate sections of the FSAR where the relevant design features are described. These proposed revisions will be included in FSAR Tier 2, Revision 2. **RAI 257, Question 19-316 is being tracked as Confirmatory Item 19-316.**

19.1.4.4.4 Reduction of Risk Compared to Operating Plants

19.1.4.4.4.1 *Qualitative Improvements*

For designs that have evolved from the technology of currently operating plants, the results of the PRA should indicate that the design represents a reduction in risk compared to operating plants. The evaluation of FSAR Tier 2, Section 19.1.3 above provides a qualitative assessment of the ways that the U.S. EPR design has achieved this risk reduction, as presented in FSAR Tier 2, Table 19.1-2, “Features for U.S. EPR that Address Challenges for Current PWRs.”

In addition, FSAR Tier 2, Table 19.1-102, introduced in the section above, lists the design features (such as redundant trains of safety systems, physical separation, and RCP seal improvements) that contribute most to the low risk estimated for the U.S. EPR design. These features were also described above in the evaluation of FSAR Tier 2, Section 19.1.3. Because these features are critical to achieving the stated risk reduction, each table entry includes references to Tier 1, Tier 2, and COL information items where the feature is described in more detail, providing assurance that the as-built plant will match the as-designed plant.

19.1.4.4.4.2 *Quantitative Improvements*

The risk metrics discussed above in Section 19.1.4.4.2.4 of this report, also demonstrate a quantitative reduction in risk compared to current operating plants. The highest estimate of Level 1 internal events CDF for operations at power provided by the applicant is a mean value of 2.3E-6/yr, including parametric and modeling uncertainty. In comparison, the IPE program results showed that PWR internal events CDF ranged from about 4E-6/yr to 5E-4/yr, with most plants clustered in the 2E-5/yr to 2E-4/yr range. These results include the internal flooding contribution, which is quantified separately for the U.S. EPR (see the evaluation of FSAR Tier 2, Section 19.1.5.2 in Section 19.1.4.7 of this report). The internal flooding contributions are presented in Table 19.1-5 of this report. The U.S. EPR design, even when parameter and modeling uncertainties are considered, represents a quantitative reduction in risk compared to current operating plants.

Table 19.1-5 Comparison of U.S. EPR Risk to IPE Results

Initiating Event	CDF (/yr)					
	B&W	**CE**	**W 2-Loop**	**W 3-Loop**	**W 4-Loop**	**U.S. EPR**
Total	1E-5 to 8E-5	1E-5 to 3E-4	4E-5 to 2E-4	5E-5 to 5E-4	4E-6 to 2E-4	3E-7
SBO	1E-6 to 2E-5	3E-7 to 3E-5	8E-7 to 3E-5	4E-6 to 7E-5	4E-7 to 4E-5	3E-8
ATWS	1E-8 to 1E-6	1E-8 to 3E-5	6E-8 to 4E-7	6E-8 to 5E-5	1E-8 to 1E-5	1E-8
Transient	7E-7 to 7E-5	2E-6 to 2E-4	1E-5 to 5E-5	1E-5 to 4E-4	5E-7 to 1E-4	3E-8
SGTR	7E-8 to 1E-6	8E-8 to 5E-6	4E-6 to 3E-5	2E-7 to 1E-5	1E-8 to 9E-6	1E-8
LOCA	3E-6 to 2E-5	9E-7 to 6E-5	1E-5 to 4E-5	2E-5 to 9E-5	1E-6 to 7E-5	5E-8
ISLOCA	1E-8 to 1E-6	1E-8 to 3E-6	6E-8 to 8E-6	1E-7 to 9E-6	1E-8 to 4E-6	<1E-9
Internal Flooding	8E-7 to 6E-6	1E-8 to 2E-5	2E-7 to 1E-5	1E-8 to 9E-5	1E-8 to 2E-5	See Section 19.1.5.2

In addition, SRP Chapter 19.0 directs the staff to compare U.S. EPR risk to current operating plants' risk by initiating event category. FSAR Tier 2, Table 19.1-3 lists the IPE CDF point estimates for Babcock & Wilcox (B&W), Combustion Engineering (CE), and Westinghouse (W) operating plants, taken from figures in NUREG-1560, "Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance," and the results for the U.S. EPR. In all cases, the U.S. EPR contributions for the selected initiating events are equal to or lower than

those for operating plants. The absolute contribution of SBO, transient, and LOCA events, while still important for the U.S. EPR, has been significantly reduced. Specific improvements related to these initiating events are discussed above in the evaluation of FSAR Tier 2, Section 19.1.3. For SGTR and ATWS events, the U.S. EPR CDF estimate is comparable to the lowest IPE estimate. However, improved SGTR mitigation capability has been incorporated in the U.S. EPR design (see the evaluation of FSAR Tier 2, Section 19.1.3 in Section 19.1.4.3 of this report). In addition, the ATWS modeling includes an assumption that pressure relief always fails if feedwater is unavailable. Therefore, given the reliable reactor trip system, it is likely that ATWS contribution to CDF is smaller for the U.S. EPR than for operating reactors. Finally, the U.S. EPR initiating events listed above do not reveal any major contributors that were not considered for operating plants.

Based on the information presented above, the staff concludes that the U.S. EPR internal events PRA reflects a qualitative and quantitative reduction of risk compared to operating plants.

19.1.4.4.5 Uncertainty, Importance, and Sensitivity Studies

According to SRP Chapter 19.0, the staff should consider the impact of data uncertainties on the risk estimates. In addition, the staff should review the applicant's risk importance studies to obtain insights about the systems, components, and human actions that contribute the most to the assessed risk, as well as the failures that contribute the most in achieving the low risk level assessed in the PRA. The staff should also review the applicant's sensitivity studies performed to determine (1) the sensitivity of the estimated risk to potential biases in numerical values, (2) the impact of the lack of detail, and (3) the sensitivity of the estimated risk to previously raised issues.

19.1.4.4.5.1 *Impact of Uncertainty*

As discussed above, FSAR Tier 2, Figure 19.1-5 shows the results of the uncertainty evaluation for Level 1 internal events at power. The two curves show the effects of parametric and modeling uncertainty on the CDF estimate.

Parameter Uncertainty. Because of the state-of-knowledge correlation defined previously, the mean CDF (the risk metric requested in NRC guidance, as well as the ASME PRA standard) is higher than the point estimate CDF reported throughout the FSAR. As identified in a 1981 paper (G. Apostolakis and S. Kaplan, "Pitfalls in Risk Calculations," *Reliability Engineering*, 2:135-145), state-of-knowledge dependencies must be handled correctly because of the potential understatement of both the mean and variance of a probability distribution. The worst-case underestimation among the simple examples presented in the paper is a system with four redundant components, where the mean is underestimated by a factor of 300 and the 95th percentile by a factor of 25. The high mean for a probability distribution that includes redundant equipment failures is therefore an important insight.

In addition, inclusion of modeling uncertainty—three cases discussed above—increases the mean CDF by about five times, from 4.2E-7/yr to 2.3E-6/yr. As detailed information on EFWS pump flow, PSRV capacity, and HVAC recovery becomes available, realistic conditions can be modeled in the PRA.

Modeling Uncertainty. Modeling uncertainty is a significant issue at the design stage. The applicant made numerous assumptions when developing the internal events PRA, both for convenience (e.g., assuming that certain trains are running) and because of lack of knowledge

(e.g., assuming that 2 hrs are available for HVAC recovery). Section 19.1.4.4.7 of this report, describes the approach taken by the applicant to ensure that this modeling uncertainty is appropriately documented so that it can be addressed in the future. Modeling uncertainty is discussed below as it was investigated by the applicant (via uncertainty cases) and the staff (via a screening approach). Detailed discussions are also provided for two important sources of uncertainty: Generator diversity and digital I&C.

Uncertainty Cases In three cases, the applicant explicitly explored the effect of modeling uncertainty on the internal events PRA results. FSAR Tier 2, Figure 19.1-5 compares the cumulative distributions for CDF both with and without modeling uncertainty, showing that inclusion of modeling uncertainty increases the mean CDF by about five times. Even with this consideration, the mean CDF is nearly two orders of magnitude below the Commission's goal for CDF. Therefore, the postulated modeling uncertainty cases (which depend on the applicant's judgment of the relative weights within each case) do not significantly affect the internal events CDF at power.

The staff examined the apparent source of this five-fold increase to understand any associated risk insights. As described above, the PSRV success criterion case explores criteria the same as or less restrictive than the base case (three PSRVs required). However, the impact of less restrictive success criteria is not expected to be significant. The PSRVs are used for feed and bleed, needed only when secondary cooling fails. The individual valves are not included in the lists of important equipment, but insights into their importance can be derived from the importance measures of the operator action required to initiate feed and bleed. FSAR Tier 2, Tables 19.1-10 and 19.1-11 show FV values for the operator actions after small LOCAs and transients, respectively, of 0.082 and 0.008. Therefore, even if the PSRVs could be designed such that they never fail, the risk reduction is expected to be less than 10 percent.

The HVAC recovery case does include a more restrictive scenario in which no recovery is possible, but weights it only with a 0.05 factor; the other cases are less restrictive or the same as the base case (2 hrs available). The RAW value of the HVAC-recovery operator action indicates that not crediting HVAC recovery would increase CDF by a factor of about 30. A five percent weight to this case might increase CDF by a factor of about two. The FV value of the operator action indicates that, if recovery of HVAC were not needed, about 40 percent of the internal events CDF could be removed. A five percent weight to this case might decrease CDF by about two percent, which is not a significant change. A longer time available for recovery would simply reduce the HEP and result in a CDF somewhere between the baseline and the case with no recovery needed.

Only the EFWS case gives significant weight (20 percent) to a more restrictive success criterion. If three or four trains of EFWS are needed when the MSSVs are used for SG relief (rather than the two trains that appear to be required in the baseline model), a higher CDF would result. FSAR Tier 2, Table 19.1-12 lists a RAW value of 302 for failure all four EFWS pumps. Therefore, even if EFWS were never available, the baseline CDF would increase to about 9E-5/yr. A 20 percent weight to this dramatic scenario would result in a CDF of about 6E-6/yr.

Therefore, the modeling uncertainty distribution provided in FSAR Tier 2, Figure 19.1-5 appears to be dominated by two cases: (1) Inability to recover HVAC and (2) more restrictive EFWS success criterion. COL Information Item 19.1-9 directs COL holders referencing the U.S. EPR design certification will review as-designed and as-built information to confirm that the assumptions in the PRA remain valid. This COL information item gives the staff confidence that as-built plant information (i.e., room heatup information and EFWS pump flow curves) will be

used to update the PRA as necessary such that the CDF estimate reflects the plant design. The staff also observes that the significance of HVAC recovery is tied to the conservative CCWS switchover assumption described above, so the effect of this uncertainty (even if less time is found to be available for recovery) is expected to be overestimated.

Failure Probabilities as Key Sources of Uncertainty. The staff also investigated which elements of the internal events at-power PRA could be considered key sources of uncertainty. Given that the CDF[2] is about 3E-7/yr, this value would need to increase by a factor of more than 300 to challenge the 1E-4/yr CDF goal. Therefore, any potential modeling uncertainties related to the failure probabilities of equipment and operator actions could be key sources of uncertainty if the RAW value of the related basic event is above approximately 300.

The staff reviewed FSAR Tier 2, Tables 19.1-9 and 19.1-11 to 19.1-13 to determine which basic events exceed this RAW threshold. No single equipment failure or operator action has a RAW value higher than approximately 30. Even if the reliability of a single piece of equipment decreased or if an operator never performed one of these actions, CDF is not likely to increase above the 1E-4/yr goal. Therefore, potential modeling uncertainties related to individual failure probabilities or HEPs do not represent key sources of uncertainty for internal events CDF (at power).

CCFs, however, can disable multiple trains of mitigating systems, so dramatically increased CCF probabilities have the potential to increase CDF above the 1E-4/yr goal. FSAR Tier 2, Tables 19.1-12 and 19.1-13 show that CCFs of more than 20 types of equipment have RAW values greater than 300. Therefore, these failure probabilities could potentially be key sources of uncertainty, because CDF would exceed the 1E-4/yr goal if one of them were guaranteed to occur.

The staff explored how high each CCF probability could increase before CDF would reach the 1E-4/yr threshold. For each of these high-RAW CCFs, the staff reviewed the top 200 cutsets from the internal events model (provided by the applicant in a July 16, 2009, response to RAI 227, Question 19-285) to determine if the basic event appears in any of these cutsets. If not, the staff concluded that the CCF would be unlikely to be a significant contributor to risk even if the failure probability were increased. If the CCF is included in one or more of the top 200 cutsets, the staff calculated approximately how large the failure probability would have to be for total internal events CDF to increase to 1E-4/yr. If the higher failure probability is unreasonable, the CCF probability is judged not to be a key source of uncertainty. If the failure probability is plausible, then the CCF probability should be preserved as a potential key source of uncertainty.

In no case did the staff consider that the higher CCF probability was a plausible value for CCF of the equipment. Most of the CCF probabilities would have to be greater than 0.1 for internal events CDF to exceed 1E-4/yr. However, in seven cases, the increased probabilities were too large to be realistic but small enough to warrant discussion. A list of these failures follows:

- CCF of IRWST sump strainers (JNK10AT001SPG_P-ALL): If all six of the IRWST strainers plug for a common cause (such as foreign materials left in containment or post-LOCA debris), no injection source drawing from the IRWST

[2] The point estimate CDF is cited here, because importance measures are calculated with respect to it, rather than with respect to the mean CDF. The difference between the two − a factor of about 1.5 − would not affect the conclusions of this section.

will succeed and a LOCA will lead to core damage. However, the CCF probability would have to increase to about 0.07 for internal events CDF to exceed 1E-4/yr. Given that NUREG/CR-6928 lists a single-strainer plugging failure rate equivalent to a 1.7E-4 probability over 24 hours, the staff concludes that a CCF probability of 0.07 is too high to be reasonable. In addition, Item 14 in FSAR Tier 2, Table 19.1-109 indicates that IRWST design elements and plant procedures ensure that strainer plugging is unlikely, with reference to the relevant part of FSAR Chapter 6. Item 2 of Table 19.1-108 also provides the insight that these CCFs cause small LOCAs to be significant to the overall PRA results. Therefore, the staff concludes that modeling uncertainty associated with the IRWST strainer CCF probability is unlikely to be a key source of uncertainty for the internal events PRA.

- CCF of the LHSI and MHSI common injection check valves (JNG12AA004CFO_D-ALL): Similar to the IRWST strainers, if all four of the check valves that admit injection from LHSI and MHSI to the RCS fail to open, injection fails and a LOCA will lead to core damage. Again, the CCF probability would have to be about 0.07 for internal events CDF to exceed 1E-4/yr. NUREG/CR-6928 estimates a failure probability of 1.3E-5 for a single check valve to open. Even if infrequent testing of these valves means that standby failures are more likely than estimated in NUREG/CR-6928, a CCF probability for all four valves of 0.07 is too high to be reasonable. In addition, Item 2 of Table 19.1-108 also provides the insight that these CCFs cause small LOCAs to be a significant contributor to the overall PRA results. Therefore, the staff concludes that modeling uncertainty associated with the common injection check valve CCF probability is unlikely to be a key source of uncertainty for the internal events PRA.

- CCF of the normal air supply or exhaust fans (SAC01AN001EFR_D-ALL and SAC31AN001EFR_D-ALL): The ventilation assumptions in the PRA mean that failures of all four of either type of fan lead to failure of other mitigating systems. However, the CCF probability would have to be about 0.06 for internal events CDF to exceed 1E-4/yr. NUREG/CR-6928 estimates higher failure probabilities for standby fans than for running fans, and the combined probability of a single standby fan failing to start and run for 24 hours is about 7E-3. Therefore, the staff concludes that a CCF probability of 0.06 is unreasonably high and that modeling uncertainty associated with these fans is unlikely to be a key source of uncertainty for the internal events PRA.

- CCF of computer processors for the PS (ALU-B CCF NS-ALL and APU-4 CCF NS ALL): Failures of these processors could lead to failure of multiple mitigating systems to actuate. Specifically, failures of ALU-B and acquisition and processing unit (APU) 4 prevent isolation of a steam line break; without isolation, uncontrolled blowdown and core damage are assumed to result. The PRA currently includes separate CCF groups for processors in seven different ALUs and APUs. Even if these processors perform different functions, they could be of the same type with common manufacturing, maintenance, or installation errors. In RAI 227, Question 19-293, the staff requested additional information on this assumption. **RAI 227, Question 19-293, which is associated with the above request, is being tracked as an open item.** With the current treatment of ALUs and APUs, the individual CCF probabilities would have to increase to about 0.05

for internal events CDF to exceed 1E-4/yr. The highest failure probability for "process logic" listed in NUREG/CR-6928 is approximately 5E-3. As discussed previously, the failure rates in the PRA are theoretical rates that are higher than the observed failure rate of the TXS components. Therefore, it is unlikely that a CCF probability that is orders of magnitude higher than the historical failure rates for these components would be reasonable. Digital I&C is discussed below as a separate source of uncertainty in the PRA.

- CCF of the safety-related batteries (BTD01_BAT__ST_D-ALL): If all four of the safety-related batteries fail after a LOOP, the PRA assumes that core damage results, because no instrumentation will be available to the operators. Because LOOP events are more frequent than most other initiating events, increases in this failure probability can affect the PRA results more easily than the other failures discussed. For internal events CDF to exceed 1E-4/yr, the battery CCF probability must increase from 2.9E-7 to about 5E-3. Given that the failure probability for a single battery is estimated as 5E-4 in the ALWR URD and 6.6E-4 in the PRA, a CCF probability of 5E-3 is likely to be unreasonable. In addition, FSAR Tier 2, Table 19.1-109 calls out the importance of this failure in Item 18, the assumption of minimal maintenance in Item 21, and the assumption of frequent monitoring in Item 27. Therefore, the staff concludes that modeling uncertainty associated with these batteries is not likely to be a key source of uncertainty for the internal events PRA. However, any changes in the reliability of the batteries in the as-built, as-operated plant or in the assumptions listed in FSAR Tier 2, Table 19.1-109 must be evaluated in the future to determine their effect on the PRA.

- CCF of the TXS application software (CL-PS-B-SWCCF): As discussed previously, the PRA includes an application software failure that disables actions performed by a specific "diversity group" within the PS (assigned a 1E-5 failure probability, reduced by a factor of 0.5 to account for possible operator recovery or diverse functions not yet modeled). Only the failure of diversity group B appears in the top 200 cutsets, and the failure probability would have to increase to 0.07 for internal events CDF to exceed 1E-4/yr. This probability appears to be unreasonably high, but increases in the failure probability could be coupled with increased operating system failures, meaning that the CDF impact could be larger. In RAI 227, Question 19-284, the staff requested additional information on these failures. **RAI 227, Question 19-284, which is associated with the above request, is being tracked as an open item.** Digital I&C is discussed below as a separate source of uncertainty in the PRA.

- CCF of the TXS operating system (CL-TXS-OSCCF): As discussed previously, the PRA includes an operating system failure that disables all actions performed by the TXS software (assigned a 1E-7 failure probability). The failure probability would have to increase to 0.02 for internal events CDF to exceed 1E-4/yr. This probability appears to be unreasonably high, but increases in the failure probability could be coupled with increased application software failures, meaning that the CDF impact could be larger. In RAI 227, Question 19-284, the staff requested additional information on these failures. **RAI 227, Question 19-284, which is associated with the above request, is being tracked as an open item.** Digital I&C is discussed below as a separate source of uncertainty in the PRA.

Diversity of EDGs and SBODGs. In the PRA, the applicant has assumed that no hardware CCF can fail all four EDGs and both SBODGs simultaneously[3]. This assumption significantly reduces total internal events CDF, because two independent failures are required to disable both the EDGs and SBODGs. As stated previously, the applicant performed a sensitivity study to investigate the effect of a CCF of all six generators; the resulting CDF was nearly a factor of four higher than the baseline.

In addition, the applicant chose not to correlate the two groups of equipment (i.e., allowed independent sampling from the EDG and SBODG failure probability distributions during the uncertainty analysis) because of the design differences assumed when excluding CCF. In FSAR Tier 2, Revision 0, the two groups were correlated, and the mean CDF was approximately six times higher than the point-estimate CDF, largely because of the state-of-knowledge correlation associated with the six-generator cutset. In FSAR Tier 2, Revision 1, the correlation was removed and the resulting mean CDF is about 1.5 times higher than the point-estimate CDF.

Although the applicant did not provide the mean value of the six-generator-CCF sensitivity case, the staff expects that it would have a similar relationship to the point estimate as in the correlated case documented in Revision 1 of the FSAR. Therefore, the mean CDF with CCF of all six generators postulated could be as high as about 7E-6/yr[4]. Significant margin exists between estimated CDF and the Commission's goal of 1E-4/yr, even with consideration of this uncertainty. Both the EDGs and the SBODGs are identified as important equipment, so no change to programs that receive input from the PRA would be expected even if CCFs of all six generators were modeled. Based on this information, the staff concludes that the applicant's modeling approach is acceptable.

However, it is important to ensure that the basis for the applicant's assumption remains valid in the as-built, as-operated plant. The staff issued several RAIs to obtain additional justification for the assumption that the EDGs and SBODGs are diverse. In RAI 26, Question 19-162, the staff requested additional information on CCF limitation between the two types of generators. In addition, the staff observed in the question that the diversity assumption was stated differently in various sections of the FSAR.

In an August 15, 2008, response, the applicant provided the following additional discussion.

> As discussed in the response to NRC RAI No. 11, Question 08.04-3, due to the large difference in nominal size between the SBODG and the EDG, the two types of diesel generator will be different models. As noted in FSAR Tier 2, Section 8.4.1.1, the two types of diesel generators are located in separate areas, and do not share control power, HVAC, engine cooling, or fuel systems. For example, the cooling system for the emergency diesel generators, transfers heat through a water-to-water heat exchanger, while the corresponding system for the station

---

[3] In contrast, some support system failures that affect both types of generators are explicitly modeled in the PRA. For example, a CCF of the safety-related batteries is assumed to prevent starting of the EDGs and to disable all instrumentation, without which the SBODGs cannot be started. Also, failure of the TXS operating system disables all mitigating functions.

[4] Although total CDF is not discussed in this section, the applicant did provide similar information for total Level 1 CDF. The relationships between mean and point estimate and between CCF cases are similar, and total CDF is not significantly higher than internal events CDF. Therefore, this discussion applies to total CDF as well.

blackout diesel generators transfers heat by a water-to-air radiator. There are no single active failures that can simultaneously disable the station blackout and emergency diesel generators.

Specific diesel generator models have not yet been selected; therefore, comparing specific engines, generators, or support system components is not currently possible. However, the differences in size, location, and support systems minimize the probability of common mode failures.

The applicant also committed to revise the FSAR to include the same diversity description in FSAR Tier 2, Chapters 8 and 19: "different model, control power, HVAC, engine cooling, fuel system, location." The staff confirmed that Revision 1 of the U.S. EPR FSAR, dated May 29, 2009, contains the changes committed to in the RAI response.

In RAI 197, Question 19-278, the staff requested additional information on the diversity assumption. In an April 10, 2009, response, the applicant provided additional information about the ITAAC that will ensure the as-built plant remains consistent with this description.

- FSAR Tier 1, Section 2.5.4, Item 5.1 provides assurance that different dc power sources are provided for the EDGs and SBODGs (Class 1E and 12-hour uninterruptible power supply (UPS), respectively).

- FSAR Tier 1, Section 2.5.3, Items 3.1 and 4.5 verify that the SBODG air start system is independent from the EDG air start systems.

- FSAR Tier 1, Section 2.5.3, Items 3.2 and 3.3 verify that each SBODG has an independent fuel oil storage tank and day tank. FSAR Tier 2, Section 2.5.4, Items 3.9 and 3.10 verify that each EDG has a fuel oil storage tank and day tank.

- FSAR Tier 1, Section 2.5.4, Item 2.2 and Section 2.5.3, Item 4.1 provide assurance that the SBODGs and EDGs are physically separated and that the SBODGs are separated from the EPSS.

The conclusion in Section 8.4 of this report is that, based on this information, the EDGs and SBODGs are sufficiently diverse. In addition, the PRA treatment of the generators is included in FSAR Tier 2, Table 19.1-108 with a disposition pointing to FSAR Tier 2, Section 8.4.1. If the design of the two types of generators change, the PRA would be revised. The impact is expected to be similar to that predicted in the discussion above. Therefore, the staff concludes that it is appropriate to place the EDGs and SBODGs in different CCF and correlation groups in the PRA.

Digital I&C. As discussed previously, the PRA includes an operating system failure that disables all actions performed by the TXS software (assigned a 1E-7 failure probability) and an application software failure that disables actions performed by a specific "diversity group" within the PS (assigned a 1E-5 failure probability). Many other failure modes of the digital I&C system, such as processor or communication module failures, are modeled in detail as well.

It generally is accepted that high reliability can be achieved for digital I&C systems by following formal and disciplined methods during the system development process. FSAR Tier 2, Table 19.1-102 states that software CCFs are minimized by measures such as high quality software design tools, a deterministic operating system, built-in monitoring and testing, and built-in functional diversity. These measures are evaluated as part of the staff's review of FSAR

Tier 2, Section 7.1.1. However, there is uncertainty as to the actual CCF rate in these digital I&C systems, and the staff considers it prudent to be cautious, as it is extremely difficult to either accurately predict or verify such failure rates.

As presented above, the applicant performed several sensitivity studies in a June 16, 2008, response to RAI 7, Question 19-68. These sensitivity studies illustrate the effect of digital I&C modeling uncertainty. These cases and their results are summarized in Table 19.1-4 of this report. The cases showed that total CDF is moderately sensitive to the assumed low software CCF probability: A 33 percent increase in CDF was estimated when software CCFs were increased by one order of magnitude. In addition, increasing HEPs in cutsets that also include digital I&C CCFs has a significant effect on the overall results (more than 100 percent increase).

In RAI 227, Question 19-284, the staff requested that the applicant expand on these sensitivity studies in two ways:

- CDF and LRF results from the fourth sensitivity case for both at-power and shutdown modes

- CDF and LRF results from a sensitivity study in which the software failure probabilities are increased to demonstrably conservative values

RAI 227, Question 19-284, which is associated with the above request, is being tracked as an open item.

Clearly, CDF increases as the probability of digital I&C CCFs increases. Digital I&C CCFs can, in some cases, disable all mitigation (e.g., an operating system failure). In other cases, multiple failures are needed because of diversity built into the system (e.g., diverse reactor trip, independent PICS and SICS in the control room, application diversity groups in the PS). Individual equipment failures (e.g., a single processor) are not significant contributors to risk because of the redundancy built into the design.

Therefore, the assumed low CCF rates, both of equipment and software, contribute significantly to achieving the low risk of the U.S. EPR design. As indicated in a June 3, 2008, response to RAI 5, Question 17.04-1, and an August 8, 2008, response to RAI 21, Question 17.04-3, all of the digital I&C equipment for which important CCFs are identified in the FSAR is included in the RAP. Both self-monitored and non-self-monitored failure modes are identified in the RAP. In addition, multiple I&C systems were included in the RAP based on an expert panel review, as documented in an August 8, 2008, response to RAI 21, Question 17.04-7. The staff's evaluation of the RAP is documented in Section 17.4 of this report. Finally, important insights and assumptions related to the digital I&C model are identified in FSAR Tier 2, Tables 19.1-102, 19.1-108, and 19.1-109.

The identification of risk insights and assumptions related to digital I&C, the performance of sensitivity studies to characterize the uncertainty, and the inclusion of digital I&C components in the RAP are sufficient for the staff to conclude that U.S. EPR digital I&C PRA model is appropriate for deriving results and insights.

19.1.4.4.5.2 *Risk Importance Studies*

Risk importance studies address the following two general objectives: Risk reduction and reliability assurance. The goal of risk reduction is to identify design and/or operational changes that could lower overall risk. Reliability assurance means maintaining the "built-in" risk level −

ensuring that risk does not increase and is as low as the PRA indicates it is. To meet these two objectives, the applicant evaluated the risk importance of failures in the PRA and provided lists of failure events with FV values greater than 0.005 or RAW values greater than 2 in FSAR Tier 2, Tables 19.1-8 through 19.1-14, as supplemented by a July 11, 2008, response to RAI 14, Question 19-126.

Risk Reduction. FV importance is the fraction of the total risk that is associated with an SSC or operator action. The value also indicates the existing margin for improvement. For example, if an SSC has an FV importance of 0.10, it means that the SSC appears in minimal cutsets contributing 10 percent of the total CDF, and that CDF would decrease by 10 percent if the SSC could be made perfectly reliable. FV importance measures are useful in identifying areas where there is margin for improvement through design and operational changes. In particular, FV importance can be used to identify SSCs that would benefit the most from improved testing and maintenance to minimize equipment unavailability and failures.

A selection of the risk-significant failures presented by the applicant (only those with an FV importance of more than five percent) follows:

- Failure of the operator to recover room cooling locally. An unrecovered failure of certain HVAC components can lead to multiple failures, as discussed above. This human error appears in cutsets that contribute about 40 percent of the CDF.

- Failure of a single EDG. LOOP is a significant initiating event for the U.S. EPR, and EDG failures appear in cutsets that contribute about 20 percent of the CDF.

- Failure of a single Division 1 or 4 SCWS chiller unit train. Chiller train failures (which can lead to failure of two divisions' electrical and EFWS systems) appear in cutsets that contribute about 20 percent of the CDF.

- Failure of the operator to initiate feed and bleed cooling after an SLOCA. SLOCA is a significant initiating event for the U.S. EPR, and this human error appears in cutsets that contribute about 10 percent of the CDF.

- Failure of the operator to start a fast cooldown after an SLOCA. SLOCA is a significant initiating event for the U.S. EPR, and this human error appears in cutsets that contribute less than 10 percent of the CDF.

- Failure of a single SBODG. LOOP is a significant initiating event for the U.S. EPR, and SBODG failures appear in cutsets that contribute about five percent of the CDF.

- Failure of the operator to crosstie Division 1 to Division 2 or Division 4 to Division 3 after a LOOP when there is no SBO. LOOP is a significant initiating event for the U.S. EPR, and this human error appears in cutsets that contribute about five percent of the CDF.

- Failure of a single 2-hour 250V dc battery train. LOOP is a significant initiating event for the U.S. EPR, and battery failures appear in cutsets that contribute about five percent of the CDF.

This list of failures suggests that risk could be reduced by implementing design or operational changes related to electrical equipment (EDGs, SBODGs, and batteries) and the SCWS

chillers. In addition, improvements to procedures, training, cues, or other human factors contributors that would reduce the likelihood of the human errors listed could have an impact on overall risk. Particularly, the recovery of room cooling is an operator action that should be re-examined at a later stage in the design, since the maximum ambient temperatures, heat-up rates, and equipment survivability are uncertain (see the modeling uncertainty discussion above). However, given the low CDF reported above, even when uncertainty is included, it is likely that design changes would need to be cost-effective and justified based on deterministic as well as probabilistic considerations.

Reliability Assurance. RAW is the factor by which CDF increases when an SSC or operator action is assumed not to be there or to be failed (event probability is assumed to be one). This value shows the importance of maintaining the existing reliability. For example, if an SSC has a RAW value of 100, it means that the plant CDF would increase 100 times should the plant be operated with that SSC unavailable. RAW values help to identify important design features and assumptions that contribute to the "low risk" of the design. These features and assumptions should be captured in requirements to ensure that the risk remains low when such a plant is built and operated. In addition, the RAW importance measure is useful in identifying areas that need particularly good maintenance and training, since poor reliability of this equipment or frequent human errors would significantly increase the CDF estimate.

A selection of the risk-significant failures presented by the applicant (only those with a RAW value of more than 20) follows:

- All 37 CCFs listed in FSAR Tier 2, Tables 19.1-12 and 19.1-13. Common-cause failures remove the benefits of four-train redundancy by failing multiple trains at once. If they are certain to occur, as the RAW value reflects, an entire safety function may be lost. In addition, much of this equipment is assigned an extremely low CCF probability. For example, the CCF probability of the safety-related batteries is about 3E-7 (calculated from cutset Group 3 of FSAR Tier 2, Table 19.1-7). Therefore, when this probability is set to 1.0, the relative change in CDF is much higher than that for a lower-reliability set of equipment.

- Failure of an EFWS storage tank. Since a significant leak in one EFWS tank could disable all four trains if the supply headers were interconnected, CDF would increase by a factor of about 40 if one EFWS tank were always certain to fail. However, as stated in the evaluation of FSAR Tier 2, Section 19.1.2.4, the design has changed to maintain the interconnection valves closed. Failure of a single storage tank is no longer expected to be as significant to total risk. **Incorporation of this change in the PRA, which is associated with the request in RAI 289, Question 19-329, is being tracked as an open item.**

- Failure of the operator to recover room cooling locally. An unrecovered failure of certain HVAC components can lead to multiple failures. Overall CDF would increase by a factor of about 30 if the operator never recovered room cooling when needed.

- Failure of a single 250V dc bus. Because the dc bus failure would disable isolation after a break or the entire division after a LOOP, CDF would increase by a factor of about 30 if the bus were always certain to fail.

- Failure of the operator to depressurize and initiate RHRS. This action is needed to mitigate an SGTR, ISLOCA, or steam line break. If the operator always failed to take this action, CDF would increase by a factor of about 30.

- Failure of a single two-hour 250V dc battery train. CDF would increase by a factor of about 20 if the battery were always certain to fail.

- Failure of a single 6.9kV switchgear. CDF would increase by a factor of about 20 if the switchgear were always certain to fail.

- The list of failures suggests that—as expected—special attention should be paid to any activities or design changes that could increase the likelihood of a CCF, because the low risk of the plant depends strongly on redundant equipment and low CCF probabilities. In addition, inspection and maintenance on the dc batteries and buses and the 6.9kV switchgear should be of high quality to ensure that failure probabilities do not increase above those assumed in the PRA. Finally, operator training should appropriately emphasize recovery of room cooling and the sequence of depressurization and initiation of RHRS, such that HEPs will remain as low as assumed in the PRA. FSAR Tier 2, Table 19.1-102 states that the HRA was performed under assumptions that the operating procedures and guidelines, as well as training, will be well written and complete. As discussed above, FSAR Tier 2, Section 18.6.2 describes the methodology for HRA and PRA insights with the various HFE programs.

19.1.4.4.5.3 *Sensitivity Studies*

As outlined above, the applicant performed multiple sensitivity cases to evaluate the impact of modeling assumptions on the internal events CDF. Based on these studies, the applicant concluded that the results are sensitive to both HEP values and electrical power assumptions. The results are not sensitive to the mission time assumed for long term cooling or the assumptions about isolation of the EFWS tanks. To assess the impact of the lack of detail, the applicant included several alternative cases in the uncertainty analysis discussed above. Previously raised issues, such as the probability of RCP seal failure following a loss of cooling, were also studied with sensitivity cases.

Only two sensitivity cases resulted in a CDF point estimate more than an order of magnitude higher than the baseline estimate. When no credit was given to operator recovery of HVAC (an important operator action discussed in several sections above), CDF increased by a multiple of about 30 times. In a sensitivity case that combined several assumptions (including all diesel generators in the same CCF group, diesel generator mission time set to 24 hours, consequential LOOP probabilities increased, HEPs set to 95th percentile value, and RCP seal LOCA probability set to 1.0), CDF increased by a factor of about 15. In both of these extreme cases, even if the mean value were an order of magnitude higher because of the state-of-knowledge correlation, the CDF estimate is still expected to be below 1E-4/yr. The staff concludes that the Commission's CDF goal is met, even with the consideration of uncertainty.

Based on the information presented above, the staff concludes that the applicant has sufficiently evaluated uncertainties in the shutdown PRA, in part by performing sensitivity studies, and identified important equipment and operator actions.

19.1.4.4.6 Assumptions During Design Certification

The staff must ensure that the assumptions made in the applicant's PRA during design certification are identified such that they can be addressed by COL applicants. COL Information Item 19.1-9 listed in Table 19.1-20, "Combined License Information Items," of this report, addresses this topic:

> 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 SAMDA [severe accident mitigation design alternatives]) remain valid with respect to internal events, internal flood and fire events (routings and locations of pipe, cable and conduit), and HRA analyses (development of operating procedures, emergency operating procedures and severe accident management guidelines and training), external events including PRA-based seismic margins HCLPF fragilities, and LPSD procedures.

FSAR Tier 2, Section 19.1.4.1.2.5 lists seven key assumptions, summarized as follows:

- EDGs and SBODGs are diverse (different model, control power, HVAC, engine cooling, fuel system, location), justifying their assignment to different common-cause groups.
- Operating procedures, guidelines, and training are well written and complete.
- Different HEPs are estimated for SBO conditions than for LOOP events that do not result in an SBO, because operators will have better direction to perform crossties in SBO scenarios.
- CVCS is credited only for RCP seal injection, with supply available from the volume control tank (VCT) 90 percent of the time.
- RCP seal LOCAs occur with a probability of 0.2 given a total loss of seal cooling and an RCP trip.
- The software CCF probability is assumed to equal 1E-5. Recovery is credited with a failure probability of 0.5. (Additional justification for this assumption, based on the defense-in-depth features not yet included in the PRA, as indicated in Item 46 of FSAR Tier 2, Table 19.1-109, was provided by the applicant in a June 16, 2008, response to RAI 7, Question 19-67.)
- Initiating event frequencies are based on operating at power all year. Adjusting for an average of 18 days shut down per year would reduce the initiating event frequencies by five percent.

Other areas for which modeling is not complete or for which assumptions have been made (such as HVAC recovery times, I&C details, calibration errors, and cooldown operator actions) are in different locations in FSAR Tier 2, Chapter 19. As discussed above, the applicant added Table 19.1-109, a list of the most important PRA assumptions, to the FSAR in response to RAI 26, Questions 19-166 and 19-167. In RAI 2, Question 19-38, the staff requested additional information on the strategy for communicating these assumptions to COL applicants and holders. In a May 30, 2008, response, the applicant stated that the applicant (AREVA NP) will

be responsible for maintaining and updating the U.S. EPR PRA during the design and construction phases until ownership is transferred to the COL holder, no later than the time of the first fuel load, when the PRA must be updated in compliance with 10 CFR 50.71(h)(1). The documentation that is supplied to the COL holder at that time, in addition to the content in the FSAR, is the principal means of communicating all assumptions in the PRA. Before then, assumptions will be communicated as they relate to other efforts, such as the development of emergency procedures. The applicant states that PRA staff will be involved with procedure development to ensure PRA insights and assumptions are considered.

The staff concludes that the documentation of assumptions in the FSAR is sufficient to ensure that they will remain valid for the as-built, as-operated plant. Any changes to these assumptions will be incorporated in the PRA as part of the PRA maintenance process described above in the evaluation of FSAR Tier 2, Section 19.1.2. Addressing COL Information Item 19.1-9, to which FSAR Tier 2, Table 19.1 109 refers, is the responsibility of the COL holder.

19.1.4.5 *FSAR Tier 2, Section 19.1.4.2: Level 2 Internal Events PRA for Operations at Power*

The following sections present results and insights from the Level 2 portion of the U.S. EPR full-power internal events PRA. These sections address the methodology, evaluation of severe accident phenomena, frequency of the various accident classes considered in the Level 2 analysis, the frequency and conditional containment failure probability, a breakdown of containment failure frequency in terms of important containment failure/release modes, and a summary of the risk-significant insights from the Level 2 PRA and the supporting sensitivity analyses.

In summary, the results of the Level 2 PRA for U.S. EPR, as discussed below, show that the U.S. EPR containment design is sufficiently robust to effectively mitigate the consequences of severe accidents with a low attendant CCFP.

19.1.4.5.1 Level 2 PRA Methodology

The U.S. EPR design-specific Level 2 PRA stated objective is to assess, using a combination of deterministic and probabilistic analyses, the response of the containment and its related systems and the radioactive releases during severe core damage accidents. The containment response has been evaluated for a 24-hour period following the onset of core damage.

The Level 2 assessment model is characterized in the FSAR descriptions primarily in terms of a traditional plant damage state binning-type of linking of the Level 1 accident sequences to the Level 2 containment event trees (CETs). The CETs indicate the basic chronological progression of the accidents. They characterize the assessment of the outcome of the physical effects of the various severe accident phenomena and of the mitigation actions of the systems and the containment design features. CET analyses provide the necessary input conditions to model and assess fission product transport through the containment; calculate radiological release fractions associated with containment release paths, and determine large release frequency associated with each fission product release category.

Functionally, for quantification purposes, the U.S. EPR Level 1 and Level 2 PRA models are contained in a single linked large fault tree that effectively includes the various bins and CETs. Operationally, this linked model allows more integration and completeness in the treatment of dependencies and interactions at the cost of some loss of scrutability.

The discussion of the Level 2 PRA in the following sections will be in terms of the core damage end state CET paradigm, consistent with the descriptions in the FSAR.

There are two types of interfaces between the Level 1 and Level 2 PRA models: The core damage end states (CDESs), and the systems credited in the event trees. The core damage accident sequences identified in the Level 1 analysis are binned into 30 distinct CDESs. Each CDES is characterized by a set of attributes that defines similar Level 1 core damage sequences. FSAR Tier 2, Table 19.1-16, "Core Damage End States and their Treatment in the CETs," describes each CDES used in the Level 1 to Level 2 interface. Prior to transfer to a Level 2 CET, each individual end state in the CDES is transferred through an intermediate "CDES link" event tree that allows some technical aspects of the linked model to be implemented, and that also allows assignment of limited core damage sequences to a simple CET for release categorization. The systems interface is handled via direct linking of the Level 1 and Level 2 portions of the model. These include the PSRVs and SADVs, SAHRS, and SIS. The inputs to the CETs preserve the Level 1 accident sequence information (the status of Level 1 event tree top events), directly accounting for dependent top events between the Level 1 and Level 2 analyses. In addition to needed support systems, the above frontline systems are also credited in the Level 1 PRA model.

Once the incoming sequences from the Level 1 have passed through the CDES link trees, they are then transferred to the appropriate CET model. 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 except for the case of the first stage high pressure CET. The release category assignments are marked on the end of each CET sequence.

The quantification of CETs is largely based on the results of plant-specific MAAP (Version 4.07) analyses. In areas where phenomenological uncertainties fall outside of the MAAP framework (e.g., steam explosions, direct containment heating, etc.), supplementary codes and calculations that are sometimes supported by experimental data have been used for the quantification process.

The U.S. EPR Level 2 PRA uses eight CETs. These are described in Section 19.1.4.5.4 of this report.

19.1.4.5.2 Computer Codes Used In Level 2 Analysis

MAAP Version 4.07 (MAAP4) 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 reactor pressure vessel (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 provides further information on MAAP 4.07.

MAAP4 is used to perform deterministic severe accident analyses (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 release category bins

The computer codes MELTSPREAD-1 and WALTER were used to model certain aspects of the decomposition and subsequent solidification of the corium-concrete mixture. Inputs required for both of these codes were derived from MAAP4 uncertainty analysis bounding values.

The acceptance evaluation of the use of the above listed computer codes is presented in the final safety evaluation report (SER) for the U.S. EPR Severe Accident Evaluation Topical Report.

19.1.4.5.3 Phenomenological Evaluations

Evaluations of severe accident phenomena have been performed to develop plant-specific phenomenological information to quantify the CET. Each phenomenological evaluation (PE) examined the current state of knowledge concerning the phenomenon, and incorporated the available information from experiments, industry studies, and plant-specific accident progression analyses to develop probability values and uncertainty distribution for use in Level 2 analyses. The phenomenological probabilities were in the case of some phenomena developed using small decomposition event trees (DET).

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

The U.S. EPR design-specific PRA treatment of each of these physical phenomena by the applicant is described below.

19.1.4.5.3.1 *Induced Rupture of the RCS Pressure Boundary*

This PE investigates induced ruptures of the reactor system during high-pressure severe accidents for the U.S. EPR. In RAI 6, Question 19-79, the staff requested that the applicant provide additional information regarding the rupture evaluation of the reactor system pressure boundary during severe accidents. In addition to the information in the FSAR, the August 8, 2008, response to RAI 6, Question 19-79, details existing evaluations and experimental supporting evidence. The important phenomena are investigated and a design-specific analysis was presented to support the development of split fractions for the containment event tree. In

addition, key uncertainty parameters are identified and sensitivity studies showing the importance of these parameters are presented. It shows how the results of these analyses are used to develop the probabilities of rupture of the hot legs and/or SG tubes for relevant accident sequences for the U.S. EPR design. These values are then available for use in containment event tree quantification. The results of this study apply only to sequences proceeding at high pressure.

This PE considers two important and mutually exclusive failure modes:

- Failure of the SG tubes
- Failure of the hot leg close to the RPV (hot leg nozzle), or surge line nozzle prior to reactor vessel failure

The applicant used MAAP 4.0.7 to investigate various high-pressure accident sequences and to evaluate the sensitivity of the induced rupture phenomena. A probabilistic evaluation was then performed by developing uncertainty distributions for the key parameters, and performing Monte Carlo simulations to determine the predicted times to hot leg, SG tube, and vessel failure. Sensitivity calculations were performed to assess the potential impact of core blockages, the results of which showed that the probability of induced rupture of the RCS would not increase significantly. The results of an EPRI study of Diablo Canyon were cited by the applicant, to conclude that full-loop natural circulation would be unlikely even for a large LOCA scenario and, in any event, would not lead to significantly higher RCS structural temperatures.

For cases with no primary depressurization, the strongest sensitivity observed is to the secondary side pressure. If SGs were to remain pressurized, the analyses indicated no risk of tube failure for any case analyzed. Hot leg rupture was, however, assessed to be highly likely (>0.9). The location of hot leg rupture was predicted to be at the weld of the nozzle to the hot leg pipe. For cases where the SGs are fully depressurized, SG tube failure is predicted to occur with a probability of up to 0.84 for sequences involving RCP seal failure or small LOCAs, and with a probability of about 0.0004 for transients.

The staff issued follow-up RAI 133, Question 19-240, requesting that the applicant provide additional information on the temperature-induced SGTR, and additional clarifications on system-related top events in the containment event trees. In December 8, 2008, and February 11, 2009 responses, the applicant performed a MAAP simulation of an accident scenario with a depressurized secondary side and an assumed 50 percent wall thinning of the steam generator tubes. The applicant concluded that RCS hot leg rupture would occur prior to SGTR.

The staff's confirmatory MELCOR calculations also predicted that the SGTR conditions would not be reached, assuming thinning of the steam generator tubes by 50 percent. The expected RCS failure location was also assumed to be the hot leg nozzles. Accordingly, the staff finds that the applicant has adequately addressed this issue and, therefore, the staff considers RAI 133, Question 19-240 resolved.

To further evaluate the potential for induced SG tube failures, the staff issued RAI 22, Question 19-148, requesting that the applicant provide information relating to the consequences of an instrument tube failure. While lowering the probability for induced SG tube ruptures, instrument tube failure could result in the release of steam, hydrogen, and fission products to the containment building. In an October 1, 2008, response, the applicant described the results of an analysis using MAAP analyses, from which it was determined that the consequences of a single instrumentation nozzle [4.57 cm (1.8 in.) diameter] failure for relevant severe accident

scenarios LOOP_PL and LBOP_TR (loss of balance of plant), are insignificant. For the LOOP_TR and LOOP_SS, there would be several potential consequences of an instrumentation tube failure. The first consequence is an approximately 1.5-percent increase in the hydrogen concentration in containment. However, the hydrogen concentration remains below the 10 percent limit set in 10 CFR 50.44, "Combustible Gas Control for Nuclear Power Reactors." The second consequence is an increase in the CsI+RbI, SrO, and CsOH+RbOH masses in containment. Lastly, the containment pressure increases in both the LOOP_PL and LBOP_SS scenarios. The maximum containment pressure is approximately 448.2 kPa (65 psia), which is below the 921.8 kPa (133.7 psia) ultimate capacity pressure for the U.S. EPR. The applicant did not consider a change to the FSAR to be necessary based on these analyses. However, the applicant had not considered multiple instrument tube failures, so the staff needed additional information.

Some of the needed information was supplied by recent analyses performed for the NRC Office of Research for TMI-2 and PWRs with inverted U-tube SGs. This information is reported in "Analysis of the Impact of Instrumentation Tube Failure on Natural Circulation during Severe Accidents," ERI/NRC 08-211, October 2008, and shows that, the failure of in-core instrumentation tubes can significantly reduce the core to upper plenum natural circulation, thereby reducing the likelihood of temperature/creep-induced SGTR. Based on this information, the staff issued RAI 133, Question 19-244, requesting that the applicant provide an analysis of the consequences of failing all of the Aeroball Measuring System (AMS) probes in the region of the core where the Zircaloy oxidation takes place, for each of the relevant scenarios. In addition, the staff requested that the applicant discuss the flow of hydrogen, steam, and fission products through the AMS probes and into the instrumentation rooms. In a March 6, 2009, response, the applicant showed the results of MAAP simulations considering the impact of AMS probe failure on accident progression, and concluded that both the trends and the magnitudes of the calculated results in the single and multiple AMS probe failure simulations are similar in each of the relevant scenarios. The consequences of these failure conditions were shown to be minor relative to the hydrogen transport phenomena as governed by the pressurizer relief/safety, and primary depressurization system valves.

Confirmatory calculations for the U.S. EPR were then performed using MELCOR 1.8.6, which included a relatively detailed modeling of the AMS probes. The results show that, due to the small cross-sectional area of these probes, their failure can only result in a slight increase in the in-vessel hydrogen production, with a correspondingly higher hydrogen concentration inside the instrumentation compartment of the primary containment. These results are similar to those reported by the applicant in response to RAI 133, Question 19-244. Accordingly, the staff finds that the applicant has adequately addressed this issue and, therefore, the staff considers RAI 133, Question 19-244 resolved.

Analysis of MELCOR-predicted RCS temperature evolution for a high-pressure scenario (i.e., station blackout) showed that creep-induced failure in the vicinity of the hot-leg nozzles dominated RCS failure. This is consistent with the AREVA MAAP predictions. Furthermore, modeling of the failure of the in-core instrumentation tubes did not appear to alter this behavior, even though some impact on hydrogen release into the containment was noted.

19.1.4.5.3.2 *Fuel-Coolant Interactions*

The fuel-coolant interaction PE prepared by the applicant evaluates the potential for steam explosions, in both the in-vessel and ex-vessel phases of an accident. The probabilistic evaluations, using Monte Carlo simulations, compare mechanical energy generated to a

threshold sufficient to cause failure. The loads and the failure threshold are treated as uncertain parameters with distributions drawn from published expert opinions.

For the in-vessel scenario, the PE focuses 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 upper head failure. Both the load and the threshold are treated as uncertain parameters. It was conservatively assumed that any load sufficient to fail the upper head would fail containment. The following probabilities for in-vessel steam explosion leading to containment failure were assessed:

- A value of 2.3E-5 for a high-pressure core melt scenario
- A value of 5.6E-6 for a low-pressure core melt scenario

In this evaluation, the probability of an in-vessel steam explosion leading to containment failure or structural damage is higher in a high-pressure scenario than in a low-pressure scenario. The key parameter in reaching this position is the conversion ratio of thermal to mechanical energy. The distribution for the conversion ratio in the high-pressure scenario has a long upper tail, representing increased weight given to the possibility (with low assigned probability) of large conversion ratios. When the assigned distributions are combined to generate overall probabilities of vessel head failure, the distribution's longer upper tail outweighs the reduced relative occurrence frequency of an initial steam explosion at high pressure.

Failure of the lower head as a consequence of an in-vessel steam explosion was similarly investigated by the applicant, except in this case 100 percent of the mechanical energy was assumed to impact the lower head. Lower head failure was assumed to lead to unspecified reactor pit damage. The CET modeling assumes further that this pit damage would result in early release of melt from the pit into the spreading area and, because this is not the design pathway for melt stabilization, molten core-concrete interaction (MCCI) would occur. The results of the probabilistic evaluation of a steam explosion causing failure of the lower head are reported as:

- A value of 8.4E-4 for a high-pressure core melt scenario
- A value of 2.5E-5 for a low-pressure core melt scenario

Ex-vessel steam explosions were similarly probabilistically evaluated for a bounding scenario in which molten corium could be released from the vessel into a cavity pit that is filled to a depth of 4 m (13.1 ft) with saturated water following hot leg creep rupture. The failure probability was evaluated by comparing a distribution of impulse loads to a distribution of reactor cavity pit structure strengths.

Specifically, the applicant evaluated the mechanical energy release by multiplying the total mass of corium in premixing, the thermal energy stored in the core materials per unit mass of core, and the conversion ratio for thermal to mechanical energy. The total load was evaluated probabilistically using Monte Carlo simulations for these three items. To evaluate the impulse loading a correlation relating energy release to peak overpressure and duration was used.

The staff notes that the reactor cavity pit in the U.S. EPR is a large concrete structure. The weakest point is considered to be the melt plug, as there are no manway or equipment doors to the reactor cavity pit. The applicant assigned a probability distribution for the capacity of the reactor cavity pit to withstand dynamic loads, for the purpose of representing the state of

knowledge about the structural capability of the reactor cavity pit. Table 19-147-1, "Probability Distribution for Dynamic Load Withstand Capacity of the Reactor Pit in the U.S. EPR," included in the applicant's September 5, 2008, response to RAI 22, Question 19-147, provides a summary of the specific probability distribution assigned for the capacity of the reactor cavity pit to withstand dynamic loads, and the supporting rationale. Using this approach, the applicant estimated the probability of structural damage due to an ex-vessel steam explosion to be 2.6E-5. As presented, there is no specific linkage of the geometries considered in that report to the U.S. EPR cavity. Further, no supporting direct computation of the dynamic load capacity of this structure is reported by the applicant.

The staff questioned this analytical approach, based on previous NRC-sponsored analyses for other plants under similar conditions (see NUREG/CR-6849, "Analysis of In-Vessel Retention and Ex-Vessel Fuel Coolant Interaction for AP1000," August 2004). Accordingly, RAI 133, Question 19-230 was issued, requesting the applicant to:

- perform a mechanistic analysis that supports the assigned uncertainty distribution
- discuss the implication of the NUREG/CR-6849 results for U.S. EPR in light of the assumed reactor pit capacity
- provide the technical justification for arriving at ex-vessel fuel-coolant interaction (FCI) loads that are much lower than has been estimated for other plants under similar conditions (e.g., AP 1000)
- provide the range of expected loads on the RPV, and if there is any potential for RPV uplift impacting containment penetrations
- provide an analysis of the impact of the reactor pit failure on severe accident progression for U.S. EPR

In a July 2, 2009, response, the applicant stated that, due to the limitations of the initial structural analyses, a new structural analysis of the U.S. EPR reactor pit was performed to evaluate its capacity to withstand steam explosion dynamic pressure loads. The structural analysis considered the effects of pressure loads on reactor cavity pit wall and melt plug. The applicant estimated a revised probability of 5.0×10^{-3} for the combined failure probability of the reactor pit.

The staff identified several issues in this response that require further clarification by the applicant, including the impact of uncertainties associated with the estimation of pre-mixing and explosion loads, and the technical basis for the newly developed "static pressure" capacity as a measure for assessment of dynamic pressure loads including those resulting from steam explosions inside the reactor pit. Accordingly, the staff issued RAI 349, Question 19-334, requesting that the applicant provide additional information on the impacts of uncertainties associated with the dynamic load capacity of the reactor cavity pit. **RAI 349, Question 19-334, which is associated with the above request, is being tracked as an open item.**

19.1.4.5.3.3 *In-Vessel Core Recovery*

To estimate the impact of the safety injection on U.S. EPR severe accidents, the applicant divided a generic severe accident scenario for the U.S. EPR into different phases, and determined the impact of the safety injection recovery for each phase. In RAI 6, Question 19-87, the staff requested the applicant to provide details on the potential for recovery during each

phase. In an August 8, 2008, response, the applicant provided the requested details, which have subsequently been examined by the staff.

The CDES with a high primary system pressure and a potential for later depressurization are important for in-vessel recovery, and were used by the applicant in this PE. If depressurization reduces the primary pressure below the shutoff head of the LHSI pump before vessel failure, the injected flow may be sufficient to recover the core, the melt progression may be arrested, and the degraded core quenched. The (limited) accumulator flows are ignored.

The probability of successfully arresting core damage in-vessel was estimated by the applicant as the product of the probability that sufficient water is present to potentially quench the degraded core, and the conditional probability to succeed in the quenching given that sufficient water is present (i.e., a favorable geometry pertains). The quenching starts at a time when primary depressurization is initiated using the severe accident depressurization valves.

The evaluations considered three phases:

- Phase 1 − core heat-up to core melt onset. During this phase the core is in a coolable geometry and safety injection (SI) restores core cooling in most cases.

- Phase 2 − core melt onset to relocation into the RPV lower head. The core is above the support plate and core recovery depends on SI recovery. The probability of arresting core damage is evaluated as a function of the quenching probability and the volume of quenching water available.

- Phase 3 − relocation into the RPV lower head to vessel failure. The corium falls into the water in the lower head which experiences a boiling-off phase, depending on the amount of water present. If the corium subsequently re-melts, the same evaluation as for Phase 2 is performed.

The applicant carried out a study for sequences representing the various core damage end states (CDES) to determine the probabilities of successful in-vessel core recovery following depressurization that would enable the low head safety injection pump to be turned on, for cases where recovery of SI is assumed to occur. Using a set of MAAP calculations for the various sequences, the applicant provided Tables 19-87-4 through 19-87-6, showing the probability of successful quenching as a function of the time after recovery of SI. The results show that quenching is very likely to occur during Phase 1, somewhat likely during Phase 2, but highly unlikely during Phase 3.

The staff considers the applicant's approach reasonable, and considers this issue resolved. The staff also believes that it is prudent to assign a very low probability of quenching if SI recovery does not occur until Phase 3. As a result, it is very important to be able to arrest core melt progression after vessel breach.

19.1.4.5.3.4 *Phenomena at Vessel Failure*

The following reactor vessel failure modes were considered:

- An off-center tear of the lower head due to corium jet impingement and ablation of the wall (i.e., side tear)

- A rupture of lower head at its base due to fully mixed static corium pool (i.e., base tear)
- An ablation failure of lower head due to jet impingement (i.e., small base or base/side tear)
- A complete circumferential failure of lower head (i.e., complete vessel breach (CVB))

The probabilities of vessel failure modes were performed by developing a DET containing the following headers:

- Location of crust breach (side or base)
- Prompt vessel failure by jet impingement
- Corium pool state, (phase separation, fully mixed convective, and fully mixed static)
- Vessel failure mode

By assigning the probabilities to various states, the probabilistic evaluation of the vessel failure mode results in the overall outcomes listed in Table 19.1-6, “Results of Vessel Failure Mode Probabilistic Evaluation,” of this report.

Table 19.1-6 Results of Vessel Failure Mode Probabilistic Evaluation

Failure Diameter (m)	Failure Mode	Probability
0.1	small base or base/side	0.04
0.1-0.5	Base	0.048
0.5-1.0	side tear	0.902
4.87	CVB	0.010

The PE considered the following phenomena at vessel failure:

- Rocketing of the vessel, due to reaction forces on the vessel when it fails at high RCS pressure
- Over-pressurization of the reactor cavity due to release of gases from the vessel at vessel failure (high RCS pressure)
- 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

Rocketing of the vessel was assessed by evaluating 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 (vessel and corium mass), rocketing was discounted except for the complete circumferential rupture of the vessel (CVB case), where rocketing is expected as the restraining forces are exceeded by nearly an order of magnitude. The CET models assume containment failure in this case.

Over-pressurization of the reactor cavity may occur when the blowdown rate of the vessel exceeds the venting capability of the cavity for a range of vessel failure sizes with the structural capacity of the cavity. The over-pressure loads were estimated using a series of MAAP runs for the vessel failure sizes evaluated in the vessel failure modes. Peak pressures ranged from 0.6 MPa (87 psi) for a 0.1 m (3.3 ft) breach up to 2.0 MPa (290 psi) for a complete circumferential breach.

The reactor pit circumferential pit sacrificial layers and plug are designed for 2 MPa (290 psi) over-pressure. A structural study was performed to show that the cavity would withstand the pressure loads, impact of the detached lower head, and various thermal loadings. A typical best estimate value would be 1.5 times the design value. A median failure pressure of 3 MPa (435 psi) with a log-standard deviation of 0.2 is assigned. The expected point of rupture is the melt plug (gate).

For a complete circumferential vessel rupture (probability 0.01, structural failure probability 0.2), the pit overpressure probability is 2E-4. An overpressure probability for the largest assessed side tear of 1 m (3.3 ft) diameter is conservatively set at 2.3E-6.

The applicant addressed the DCH pressure rise probabilistically. The 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. 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 probabilistic evaluation concluded that, following a DCH event with the vessel failing at high pressure, the probability of containment failure is 5.5E-4; whereas, the conditional probability of cavity failure due to DCH would be bounded by 2.3E-6 (for breach sizes of 1 m (3.3 ft) or less, for which vessel rocketing is not the limiting failure mechanism).

In the paper, “Direct containment heating integral effects tests in geometries of European nuclear power plants,” Nuclear Engineering and Design 239 (2009), pp 2070-2084, Leonhard Meyer et al, reported the results of recent research on the effects of DCH in European reactor geometries. In particular, it was found that vessel breaches greater than 0.5 m (1.6 ft) in diameter can lead to significant melt dispersal and containment peak pressure, even if the pressure in the vessel was low (between 1 and 2 MPa) at the time of lower head failure. Moreover, it was observed that, for the EPR geometry, there would be significant dispersal of debris into the pump and steam generator rooms, even at such pressures. The staff believes that the impacts of the presence of core debris in pump and steam generator rooms need to be taken into account in preparing severe accident management guidelines. Staff review of the applicant’s Operational Strategy for Severe Accidents (OSSA) Methodology is still ongoing (see the discussion of Open Item 19-243 in Section 19.2.4.5 of this report).

19.1.4.5.3.5 *Hydrogen Phenomena*

This PE considered containment loads generated from hydrogen combustion. The evaluation considered potential 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)). Containment loading from hydrogen deflagration was estimated considering an adiabatic isochoric complete combustion (AICC) process. This calculation would lead to a conservative containment condition, since combustion is neither adiabatic (no heat loss), nor isochoric (constant volume).

Consumption of hydrogen and oxygen by recombiners was accounted for by varied assumptions regarding PAR efficiency in 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-6.

- 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-4.

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, and the observation based on MAAP results that the containment atmosphere would likely become steam-inerted in the absence of SAHRS sprays or active cooling.

For the evaluation of destructive combustion, 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. Carbon monoxide was conservatively treated as equivalent to hydrogen for these analyses. 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 Organisation for Economic Co-Operation and Development (OECD) Nuclear Energy Agency (NEA) state-of-the-art report on hydrogen combustion.

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 scenarios (cases), with the probabilities of flame acceleration causing local or global containment damage assessed as the product of several conditional probabilities, including that of no burning of hydrogen in smaller amounts at the point of release (0.01 to 0.5); of ignition occurring at the point of release during a period of high hydrogen concentration (0.01 to 1); of flame acceleration occurring (0.01 to 0.5); of an enhanced load being experienced

at the containment boundary, given flame acceleration (0.5 to 1); and of containment failure or damage occurring, given an enhanced load (assumed to be 1).

The highest net probability of containment failure out of the cases that were assessed was found to be 0.016, for the case of transients at high pressure, in-vessel phase period of discharge from RCS via pressurizer valves. Where a destructive combustion mode was assessed to occur without leading to containment failure, the possibility of localized damage to recombiners was considered, with an assessed probability as high as 1.6E-2 for some cases.

19.1.4.5.3.6 *Long-term Containment Challenges*

The evaluation of long-term containment challenges starts at the time of core debris transfer from the reactor cavity to the melt spreading area. Additional details on core melt stabilization system are provided in the evaluation of FSAR Tier 2, Section 19.2.3. This evaluation identifies and decomposes the treated phenomena, which relies on the results of the analyses performed using MAAP 4.07. MAAP 4.07 was used to model 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 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.

The applicant considered eight distinct containment challenge mechanisms organized into a DET that provides the framework for performing the probabilistic evaluation of long-term challenges consisting of a quantification of the failure probability expected due to the failure mechanisms. The containment challenge mechanisms (i.e., DET headings) considered were:

- Success/failure of passive flooding
- SAHRS sprays availability
- Active cooling availability
- No containment overpressure failure (during quench): Containment pressure rise was estimated based on a probabilistic analysis including the impact of uncertainties associated with both the fraction of debris quenched (between 0.08 and 1) and in the flat-plate CHF Kutateladze number MAAP 4.07 input parameter (best estimate of 0.1 with an upper bound of 1). This was evaluated by a million sample Monte Carlo analysis in a spreadsheet model. The results, as detailed in a July 7, 2008, response to RAI 6, Question 19-107, show a conditional probability of containment failure of 0.0 for CDES PL, SL, ML, SS, LL, and 3E-06 for CDES TP/TR.
- No significant MCCI: Given the success of passive flooding, sustained MCCI was viewed as unlikely, and a conditional probability of 1×10^{-3} was assigned to this node.
- No containment overpressure failure (before basemat penetration): Extrapolation of MAAP4.07 results indicated that, in a scenario with sustained MCCI, containment overpressure would require approximately 17 days, while basemat penetration would occur in about 9.5 days. Therefore, containment overpressure occurring first was determined to be unlikely, and a conditional probability of 0.01 was assigned.

- No basemat penetration: Because of the debris temperature during sustained MCCI and the resultant ablation rate, there is no significant probability that MCCI will arrest before penetration of the 4.4 m (14.4 ft) thick basemat below the spreading area, a conditional probability of 0.99 was assigned.

- Containment overpressure failure (incomplete melt transfer): Conditional probabilities of containment overpressure were assigned between the values of 0.01 without hot leg rupture (i.e., judged to be unlikely) and 0.5 with hot leg rupture (i.e., judged to be uncertain but cannot be ruled out, due to the likelihood of water from the RCS flooding the reactor pit).

The results of the long-term challenge evaluation are summarized in FSAR Tier 2, Table 19.1-17, "Summary of Long Term Challenges Probabilistic Evaluation."

19.1.4.5.3.7 *Evaluation of Phenomena Modeling and Analysis*

The discrete probabilities and uncertainty distributions for the approximately 50 phenomenological basic events quantified through the PEs described above are tabulated in the July 7, 2008, response to RAI 6, Question 81, Tables 19-81-1 and 19-81-2. The basis for the mean values has been described in the above discussions of the appropriate PE. RAI responses provided the staff with additional information for assessment of the evaluation methodology, coverage, and analysis. Induced ruptures of the reactor system pressure boundary, vessel rocketing, steam explosions, reactor pit pressurization, high pressure melt ejection (HPME)-induced DCH, basemat penetration and hydrogen combustion have been provided in the applicant's responses to RAI 6, Questions 19-79, -81, -88, -89, -90, -91, -92, -93, and -95, respectively.

In general, the applicant extensively examined known severe accident phenomenological uncertainties using computer codes (e.g., MAAP, MELTSPREAD, etc.), reviewing experimental data from the literature, and referencing competent expert judgment.

19.1.4.5.4 Containment Event Tree

Containment event trees were used to evaluate the complete spectrum of potential challenges to containment integrity. The top events included in the CETs address the phenomenological events, the systems, and the human actions credited to mitigate severe accidents. The top events included are those that are expected to have a significant impact on severe accident progression, meaning that they can affect, directly or indirectly, either the likelihood of containment failure or bypass or the magnitude of radiological releases.

The set of 91 MAAP accident progression analyses performed to support development of the containment event trees and supporting fault trees for branch probabilities, each targeted to investigate particular aspects of the phenomena examined, are characterized in the July 7, 2008, response to RAI 6, Question 19-82, Table 19-82-1. A second set of 25 MAAP analyses performed to support the source term analysis are characterized in the response to RAI 6, Question 19-82, Table 19-82-2.

The event tree includes top events, dependent on the entering core damage end-state from the CDES link trees:

Phenomena:

- Direct containment heating
- Steam explosion
- Core debris cooling
- Systems functions
- Severe accident depressurization valves
- Core melt stabilization system
- Containment isolation system
- Severe accident heat removal system

For conditions leading to containment failure, the CETs are grouped into three different time frames:

- Timeframe 1 (TF1), which considers the period from the onset of core damage up to the time of vessel failure (if this occurs). Relevant events considered in this timeframe include containment isolation, induced RCS failures, depressurization of RCS by the operators, and hydrogen combustion. Containment failures in this timeframe may be a loss of isolation or a rupture, including alpha-mode failures.

- Timeframe 2 (TF2), which considers the period from the time of vessel failure to the start of melt transfer to the spreading area. Relevant events in this timeframe 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 combustion or vessel rocketing). Only such containment rupture failures could occur in this timeframe.

- Timeframe 3 (TF3), which considers long-term events from the time of melt transfer to the spreading area. Relevant events considered in this timeframe include melt transfer to the spreading area, initial stabilization of melt ex-vessel, steam overpressurization during quenching leading to containment failure, hydrogen combustion, steam over-pressurization in the long term, long-term overpressure or basemat failure due to core concrete interaction, and sprays for source term mitigation. Containment failures in this timeframe may be a rupture or a basemat melt through.

There are eight CETs, seven of which receive a direct transfer from the CDES link event trees. The eighth CET, the second stage CET for high-pressure sequences, only receives transfers from the first stage CET for high-pressure sequences. A summary description of each CET is provided in FSAR Tier 2, Table 19.1-18. These summary descriptions are supplemented by FSAR Tier 2, Tables 19.1.C-1 through 19.1.C-8. The trees themselves are depicted in FSAR Tier 2, Appendix 19C, Figures 19.1.C-1 through 19.1.C-8. The following briefly characterize these trees:

- The CET for CDES with guaranteed containment failure is a "straight line" with no mitigating or recovery actions. These are ATWS sequences with an uncontrolled reactivity transient following a Steam Line Break Inside Containment.

- The ISLOCA CET only determines whether or not there is water available to cover break outside containment and scrub the fission products released from the leak.

- The CET for limited core damage CDES only questions the containment isolation status.

- The CET for low pressure CDES has 12 top events (not counting entry and labeling) and 81 end points. Five of the top events are for TF1, two are in TF2, and five are in TF3. High-pressure sequences which depressurize in TF1 transfer to this tree.

- The CETs for unscrubbed and scrubbed SGTR sequences are straight lines.

- The first stage CET for high pressure CDES sorts out sequences with induced steam generator tube rupture (ISGTR) failures and those sequences depressurized in TF1.

- The second stage CET for high pressure CDES is for all high pressure sequences not sorted out in the first stage high pressure CET.

- The complex trees are the low and high pressure CETs. The others are either pass-through or ask only one question.

The containment isolation (CI) status is only questioned in the low pressure CET, the second stage high pressure CET, and the limited core damage CD. The CI status is characterized as no failure, a small release failure for lines with less than 7.62 cm (3 in.), or a large release failure for lines with greater than 7.62 cm (3 in.) diameter. A failure of two or more lines of greater than 5.08 cm (2 in.) diameter is considered a large failure. It is noted that MCCI is assumed to take place for large CI failures.

The steam line breaks were explicitly dispositioned for the purpose of the FSAR Tier 2, Section 19.2 analyses, and were not explicitly analyzed. The main assumption that leads to the severe consequences for steam line breaks is a coincident severe ATWS, which is considered as an additional failure that moves the events out from the suite of relevant scenarios. Without this assumption, the steam line breaks leading to core damage are treated as events in which core damage results from loss of secondary heat sink. It is noted that the steam line break contributions are assigned to LBOP TR category.

The CET-supporting fault trees incorporating the phenomenological basic events, operator action events, selective flag events, and system performance have been provided by the applicant in the July 7, 2008, response to RAI 6, Question 19-81, Figures 19-81-1, Sheets 1 to 19. These supporting fault trees are the essential quantifying mechanism for the top event branch fractions and, therefore, for the containment portion of the severe accident sequences. The staff reviewed these fault trees and find them reasonable and comprehensive.

19.1.4.5.4.1 *Accident Release Categories*

The containment response to a severe accident is depicted by the end-state of containment event trees. These end-states are binned into the "release categories" that are used to characterize potential source terms. The release categories are defined based on the following attributes:

- Containment bypass
- Time and mode of containment failure
- Melt retention in-vessel
- MCCI
- Melt flooding status (ex-vessel)
- Other source term mitigation (i.e., containment sprays, SG pool scrubbing, or reactor building retention)

Twenty-five release categories are defined. Figure 19-83-1 in the July 7, 2008, response to RAI 6, Question 19-83, illustrates how the various significant attributes of the accident sequences have been grouped into the release categories. The release categories and their descriptions are provided in Table 19.1-7, based on FSAR Tier 2, Table 19.1-19.

Table 19.1-7 Release Category Definitions

Release Category	Description
RC101	No containment failure
RC201	Containment failure before vessel breach due to isolation failure, melt retained in-vessel
RC202	Containment failure before vessel breach due to isolation failure, melt released from the vessel, with MCCI, melt not flooded, with containment spray
RC203	Containment failure before vessel breach due to isolation failure, melt released from vessel, with MCCI, melt not flooded, without containment spray
RC204	Containment failure before vessel breach due to isolation failure, melt released from the vessel, without MCCI, melt flooded, with containment spray
RC205	Containment failure before vessel breach due to isolation failure, melt released from vessel, without MCCI, melt flooded, without containment spray
RC206	Small containment failure due to failure to isolate 2-inch or smaller line
RC301	Containment failure before vessel breach due to containment rupture, melt released from the vessel, with MCCI, melt not flooded, with containment spray

Release Category	Description
RC302	Containment failure before vessel breach due to containment rupture, melt released from vessel, with MCCI, melt not flooded, without containment spray
RC303	Containment failure before vessel breach due to containment rupture, melt released from the vessel, without MCCI, melt flooded, with containment spray
RC304	Containment failure before vessel breach due to containment rupture, melt released from vessel, without MCCI, melt flooded, without containment spray
RC401	Containment failure after vessel breach and up through debris quench due to containment rupture, melt released from the vessel, with MCCI, without debris flooding, with containment spray
RC402	Containment failure after vessel breach and up through debris quench due to containment rupture, melt released from vessel, with MCCI, without debris flooding, without containment spray
RC403	Containment failure after vessel breach and up through debris quench due to containment rupture, melt released from the vessel, without MCCI, without debris flooding, with containment spray
RC404	Containment failure after vessel breach and up through debris quench due to containment rupture, melt released from vessel, without MCCI, without debris flooding, without containment spray
RC501	Long term containment failure after debris quench due to rupture, with MCCI, without debris flooding, with containment spray
RC502	Long term containment failure after debris quench due to rupture, with MCCI, without debris flooding, without containment spray
RC503	Long term containment failure after debris quench due to rupture, without MCCI, without debris flooding, with containment spray
RC504	Long term containment failure after debris quench due to rupture, without MCCI, without debris flooding, without containment spray
RC601	Long term containment due to basemat failure, without debris flooding, with containment spray
RC602	Long term containment due to basemat failure, without debris flooding, without containment spray
RC701	Steam generator tube rupture with fission product scrubbing
RC702	Steam generator tube rupture without fission product scrubbing

Release Category	Description
RC801	Interfacing system LOCA with fission product scrubbing
RC802	Interfacing system LOCA without fission product scrubbing, but with building deposition/depletion

19.1.4.5.4.2 *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 MAAP 4.0.7 code, which includes U.S. EPR-specific models. The source term is the result of the MAAP analysis and represents the fraction of the initial core inventory that is released to the environment as a function of time for each of 12 fission product classes defined on the basis of physical and chemical similarity. The source terms for each RC listed in FSAR Tier 2, Table 19.1-20, are the MAAP results regrouped into nine chemical element groups suitable as input to offsite release calculation models.

To characterize the source term associated with each release category, a single representative sequence was chosen for each release category, which had a non-zero frequency, associated with the CET quantification. Sensitivity analyses were also performed to determine the sensitivity of source terms to a number of key variables such as isolation failure break sizes, operation of SAHRS, and retention potential for interfacing system LOCAs.

The highest release fraction (represented by Cs) is for RC201, a containment isolation failure. The chosen representative sequence involved a hot leg rupture which led to a significantly increased release to the environment, even though there was recovery in-vessel. For the characterization of the scrubbed SGTR source term (RC701), a decontamination factor (DF) of 20 has been applied to the unscrubbed SGTR source term (RC702) from MAAP4.0.7. A scrubbing evaluation was performed using the MAAP pool scrubbing models to confirm this assumption. This value is found to be conservative for most aerosols, and overall adequate to model source term scrubbing in the SGs. In estimating the RC702 (SGTR without scrubbing) release category, the rupture of one tube was assumed, though a case could be made for more concomitant tube ruptures. In a December 10, 2008, response to RAI 6, Question 19-84e, the applicant stated that a sensitivity analysis has been performed assuming two and five tube ruptures, and the results showed that there would not be a rapid depressurization of the RCS following a single tube rupture, and the calculated radiological releases would increase for the case involving multiple tube rupture. The staff issued RAI 133, Question 19-233, requesting the applicant to address the likelihood of multiple SGTRs, and to provide the associated source term.

In a February 11, 2009 response to RAI 133, Question 19-233, the applicant's calculated the likelihood of multiple SGTRs using a Poisson distribution due to random flaws in the tubes under creep-induced conditions. However, a review of this response identified an issue in the applicant's analyses regarding the potential implications of failure propagation due to the continued heat-up of the steam generator tubes, after the initial tube failure. Natural circulation and steam generator tube heat-up is expected to continue well beyond the failure of a single tube. Therefore, the analysis of the calculated failure likelihoods by the applicant is incomplete.

Furthermore, the applicant's calculated fission product releases to the environment for the single and multiple tube rupture cases based on MAAP results are also judged to be low, especially, in comparison to the results of recent NRC confirmatory calculations using MELCOR for a single double-ended induced-SGTR scenario. The MAAP source term results cited in the applicant's response are about 50 percent too low, at 24 hours into the accident, and about a factor of 3 low at 48 hours into the accident, when compared to the MELCOR calculations (see Table 19.1-8 of this report). One reason for these differences is the termination of MAAP calculations after 24 hours, thus limiting the releases due to revaporization. The use of the MELCOR source terms would make release category 702 a major (if not the most) risk significant category. These differences are significant and need to be reconciled by the applicant.

Therefore, the staff issued RAI 349, Question 19-335, requesting that the applicant:

- Revise the SGTR analyses to reflect the potential impact of continued heat-up of the steam generator tubes, in order to determine at what level of failure (number of tubes) RCS depressurization can occur, to terminate additional tube failures

- Extend the present MAAP-based source term calculations to at least 48 hours, and report the impact on fission product releases and severe accident risk for U.S. EPR, including comparisons to the NRC early and latent fatality safety goals

RAI 349, Question 19-335, which is associated with the above request, is being tracked as an open item.

Table 19.1-8 Comparison of the MELCOR- and MAAP-Predicted Source Terms for a 5.08Cm (2-in.) Cold-Leg Break with an Induced SGTR [Table 3.5b of Ref. 19-15]

Radionuclide Group	MAAP	MELCOR	
	24 hours into the accident	24 hours into the accident	48 hours into the accident
Xe	1.1E-01	2.31E-01	2.74E-01
I	8.4E-02	1.71E-01	2.68E-01
Cs	8.7E-02	1.34E-01	1.71E-01
Te	1.4E-01	1.76E-01	2.45E-01
Mo	9.6E-02*	6.03E-03	6.59E-03
Ba	5.4E-02	1.56E-03	2.11E-03
Ru	9.6E-02*	2.23E-03	2.25E-03
Ce	2.2E-03	6.76E-06	7.41E-06
La	4.5E-04	1.10E-06	1.28E-06

* In MAAP releases for Mo group are also assigned to Ru group

19.1.4.5.4.3 *Large Release Definition*

The Level 2 PRA quantifies the frequency and source term of each RC, and provides a comprehensive prediction of release risk. However, for reporting purposes, and to allow comparison with various targets and criteria, the applicant calculated the LRF as the fraction of CDF predicted to fall into release categories that it classified as “Large.”

Following guidance from Appendix A of NUREG/CR-6595 the applicant defined the release associated with a given release category to be “Large” if any predicted Cs, Te, or I release is above approximately 2 ½ to 3 percent. In addition, 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 were classified as “large release”: RC201 through RC205, RC301 through RC304, RC702, and RC802. All other categories have release fractions less than the guideline. These release categories comprise large isolation failures, early containment failures, and bypass events.

19.1.4.5.4.4 *Containment Fragility*

The containment structural 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 static or dynamic pressure load p, as a function of containment failure probability. The values obtained for the U.S. EPR containment structure are shown in FSAR Tier 2, Table 19.1-21, "Probability Distributions (Lognormal) for the Six Dominant Containment Failure Modes." Only static over-pressure loads have been examined. The response of the affected containment structures (i.e., reactor pit) to local dynamic loads has not been assessed on a plant-specific basis; however, information from literature is cited and used in a qualitative manner to arrive at the conditional probability of failure, given a range of dynamic loads.

The composite fragility curve combines the results from each of the individual failure modes into a single distribution representing the capacity. The composite curve shown in FSAR Tier 2, Figure 19.1-8, “Composite Containment Fragility Curve at 170 °C (338 °F),” was revised as a result of RAI 234, Question 19-307. The response presented the new composite fragility curve at 154 °C (309 °F).

19.1.4.5.4.5 *Equipment Survivability*

In a review of the equipment credited in the CET with respect to equipment qualification for severe accidents, the applicant 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. Consequential damage to the recombiners due to accelerated flame phenomena is considered in the CET model. Further details on severe accident equipment qualifications are provided in the evaluation of FSAR Tier 2, Section 19.2.3.3.

19.1.4.5.5 Results from the Level 2 PRA for Operations at Power

The total LRF from internal events is 2.2E-8/yr (point estimate). The corresponding CDF is 2.9E-7/yr. The CCFP for internal events, which is the probability that a given core damage sequence will result in a large radiological release to the environment, is calculated to be 0.076, which is within the NRC containment performance goal of no more than 0.1.

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. Scenarios with containment failure prior to vessel breach are due primarily to containment overpressure resulting from an SLBI, with failure to isolate multiple SGs. Continued blowdown of multiple SGs with failure to isolate feedwater or failure to inject extra boration for reactivity control is expected to over-pressurize the 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, which accounts for 21 percent of LRF. RC702 encompasses containment bypasses from SGTR without fission product scrubbing, including both SGTR core damage sequences from the Level 1 analysis and induced SGTR sequences deriving from the Level 2 analysis. An additional four percent of LRF is attributed to sequences with failure to isolate the containment prior to core damage, and one percent of LRF is the result of containment bypass due to core damage sequences initiated by breaks outside containment.

The residual challenge to the containment (i.e., approximately eight percent of LRF), other than those listed in the previous paragraph, is primarily phenomenological and is mainly due to short-term localized hydrogen concentrations leading to conditions with the potential for flame acceleration.

19.1.4.5.5.1 *Leading Contributors to Containment Failure for Internal Events*

The significant cutsets for the internal events Level 2 PRA are illustrated in FSAR Tier 2, Table 19.1-25. This table provides all of the cutsets contributing more than one percent to LRF. Cutsets that contribute one percent or more to large release for internal events are described below.

Release Category RC304: Cutsets 1 through 8. These cutsets contribute approximately 39 percent to the internal events large release frequency. They involve an SLBI with CCFs of I&C that lead to failure of the signals for MSIV and MFW isolation to multiple SGs. These failures are assumed to lead to an uncontrolled reactivity event due to overcooling and a condition where the steam line break continues to supply steam to the containment as long as feedwater is supplied to the SGs. 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.

In a November 4, 2008, response to RAI 22, Question 19-160, regarding the most likely SLBI scenario involving failure of I&C signals for MSIV and MFW isolation for at least three SGs, the applicant provided a deterministic analysis. The applicant stated that this analysis had determined that the assumptions in the FSAR of core damage from an uncontrolled reactivity event during overcooling and subsequent containment failure because of overpressure are conservative. The applicant performed a sensitivity analysis on the PRA to quantify the impact of this conservatism.

For the analysis, the RELAP 5 code was used to determine that there is no return to power, because the total reactivity remained negative. Moreover, a MAAP 4.0.7 calculation was performed to verify that the containment would remain intact. Removal of the conservatism in the SLBI sequence involving blowdown of four SGs changes the LRF for internal events from 2.2E-8/yr to 9.5E-9/yr. This represents a 57 percent reduction in LRF if the conservatism associated with this scenario is eliminated. Release Category RC304 no longer has significant cutsets associated with the SLBI initiating event, and the LRF from RC304 drops from 8.5E-9/yr

to 2.6E-9/yr. Core damage frequency is not significantly affected. The staff agrees that the analyses and consequent reductions in the LRF are reasonable. Although these results have been reported in the response to RAI 22, Question 19-160, Revision 1 of the FSAR does not yet include the changes. **Inclusion of the above assumption, which is associated with RAI 22, Question 19-160, is being tracked as Confirmatory Item 19-160.**

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 SGTR (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 SG tube without scrubbing (feedwater not available).

19.1.4.5.5.2 *Significant Core Damage End-States, Initiating Events, Phenomena and Basic Events*

Core Damage End-States. About 57 percent of the LRF results from the ATI CDES (core damage from ATWS sequences with no operator initiated SG depressurization). This contribution arises because of the steam line break inside containment. Of the remaining contribution, 10 percent of the LRF comes from CDES involving SGTR, and eight percent from core damage sequences involving loss of offsite power with the primary system at high pressure. Additional information is provided in FSAR Tier 2, Table 19.1-26.

The key assumption with regards to SLBI is that failure of three main steam lines to isolate necessitates additional reactivity control (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 puts these sequences directly in a release category indicating early, large containment failure.

Initiating Events. FSAR Tier 2, Table 19.1-27 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. The second largest contributing initiating event is SGTR (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 SGTR (IE Induced SGTR, 8 percent); note that this induced SGTR is 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.

The staff issued RAI 22, Question 19-160, requesting that the applicant perform a deterministic analysis of the most likely steam line break inside containment (SLBI) scenario with failure of I&C signals for MSIV and MFW isolation of at least three steam generators, leading to an uncontrolled reactivity event during overcooling. In a November 4, 2008. response, the applicant provided information showing that it used an EPR-specific RELAP5 point kinetics calculation with the corresponding containment pressure calculated by MAAP4, and presented for about 3 hours after accident initiation. These results showed that after 2.8 hours, the

containment pressure is within approximately 310.3 kPa (45 psi) of the median failure pressure of the containment. Subsequently, the staff issued RAI 236, Question 19-309, requesting the applicant to provide the results of the analyses that extend to 24 hours.

In a July 13, 2009, response, the applicant extended the calculation time and showed that the SBLI does not result in a recritical condition and the RELAP5/MAAP4-predicted containment pressure remains below the containment failure threshold. The staff finds the applicant's calculation of containment pressurization identified the potential for errors. Independent MELCOR calculations using a point kinetics model and the AREVA-supplied reactor feedback coefficient showed that the reactor remains subcritical due to the large shutdown margin provided by the control rods, and subsequently, the rate of containment pressurization is low, and containment failure was not predicted to occur for at least 2 days. Accordingly, the staff finds that the applicant has adequately addressed the SLBI issue and, therefore, the staff considers RAI 236, Question 19-309 resolved.

Physical Phenomena. FSAR Tier 2, Tables 19.1-28, and 19.1-29 show the risk-significant containment phenomena based on FV and RAW importance. The insights from RAW importance are discussed in the sensitivity analysis section below.

The most risk-significant phenomenological event based on FV and RAW is the L2PH VECF-FA(H) (Level 2 phenomena, very early containment failure, flame acceleration [high RCS pressure]) event. This event 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 through the PSRVs. 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 next event is the L2PH VECF-FA (HL) event, 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 include: induced hot leg rupture (L2PH CPIHLR-TR, TP=Y), small LOCA with no depressurization (L2PH LOCA-DEPRESS=N), and in-vessel recovery (L2PH INVREC (NR) =N). These events do not represent direct containment failure events. Rather, these represent phenomenological occurrences during the sequences that have an indirect impact on containment performance. 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).

Basic Events. FSAR Tier 2, Table 19.1-30 shows the top risk-significant equipment based on FV importance. This table shows a strong consistency with the results of the Level 1 analysis, 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.

FSAR Tier 2, Table 19.1-31 shows the top risk-significant equipment based on RAW importance. This table shows consistency with the results of the 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 containment isolation function.

FSAR Tier 2, Tables 19.1-32 and 19.1-33 show the risk-significant human actions based on FV and RAW importance. These tables indicate a few operator actions (less than 10) 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 that represent a severe challenge or bypass of the containment, and (2) the automation of severe accident measures, which reduces reliance on operator actions to prevent large release. With regards to the latter, the main actions considered in timeframes that are relevant for LRF are (1) backup actions for containment isolation, (2) operator entry to the OSSA, and (3) 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.

FSAR Tier 2, Tables 19.1-34 and 19.1-35 show the risk-significant common cause events based on RAW importance. These tables show strong consistency with the results of the Level 1 analysis. 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. In addition, 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 played by the I&C system in the initiation of protective signals and the control of active components throughout the plant.

19.1.4.5.6 Insights from Sensitivity and Uncertainty Analyses

19.1.4.5.6.1 *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 where 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 mentioned previously, 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 (the increase is estimated based on RAW importance, FSAR Tier 2, Table 19.1-29):

- 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]). If assumed to always occur, these events would lead to a 9 to 11 times increase in LRF.

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

The FSAR notes that hydrogen deflagration causing failure of the containment is close to being a physically unreasonable event. Its base probability of 1.38E-4 in the 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 quantities of hydrogen present in the containment rather than on performing a detailed Monte Carlo simulation as was done for some other events, and no credit was taken for consumption of hydrogen due to random ignition at low concentrations (i.e., benign burning).

The U.S. EPR Level 2 PRA assessed containment failure due to steam explosion as a very low probability event; but with an assessed probability greater than 1.0E-6, 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.

The applicant concluded that thermally-induced SGTR sequences are not significant contributors to the LRF for internal events. However, given that sequences with a depressurized secondary side contribute nine percent of CDF, the applicant carried out sensitivity studies to address 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 (i.e., factor of 2) change in LRF for internal events.

19.1.4.5.6.2 *Uncertainty Analysis*

An integrated uncertainty analysis was performed for the U.S. EPR Level 1 and Level 2 PRAs. The basis for the input uncertainty distributions for systems-related basic events and operator actions is discussed in FSAR Tier 2, 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). These are presented by the applicant as 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.

The calculated CDF, LRF, and CCFP values for internal events at power are listed in Table 19.1-9 of this report.

Table 19.1-9 Risk Metric Results for Level 2 Internal Events

Risk Metric	Point Estimate	Quantile		
		Mean	5th percentile	95th percentile
CDF	--	4.2E-7/yr	--	--
LRF	2.2E-8/yr	3.1E-8/yr	1.5E-9/yr	1E-7/yr
CCFP	0.076	0.074	--	--

19.1.4.5.6.3 *Key Insights from the Level 2 PRA for Internal Events*

The LRF is dominated by sequences entering from the Level 1 PRA, which represent a severe challenge to the containment or in which the containment function is already defeated (bypassed). These sequences are largely made up of (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) SGTR core damage sequences from the Level 1 PRA, including induced ruptures occurring before core damage.

The CCFP of large release due to internal events at power is about eight percent, below the NRC objective of 10 percent. If the two types of sequences identified above (SLBI and SGTR) 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.

19.1.4.6 *FSAR Tier 2, Section 19.1.5: Safety Insights from the External Events PRA for Operations at Power*

19.1.4.6.1 FSAR Tier 2, Section 19.1.5.1: Seismic Risk Evaluation

The applicant evaluated the risk resulting from seismic events using a PRA-based seismic margins approach, which is described in SECY 93-087 and ANSI/ANS-58.21. A PRA-based

margin analysis differs from traditional seismic margin assessments (SMA) such as EPRI-type SMA or NRC-type SMA in that the PRA-based margin approach would expand the system analysis scope to include all of the SSCs normally included in a seismic PRA, but it does not estimate the core damage frequency from seismic events. Instead, a sequence-level high confidence of low failure probability (HCLPF) capacity is estimated for all sequences that have the potential to lead to core damage or containment failure. The lowest sequence-level HCLPF capacity represents the design-specific plant HCLPF capacity. The PRA-based seismic margin assessment allows potential vulnerabilities in the design to be identified so that measures can be taken to reduce the risk associated with seismic events.

The U.S. EPR design-specific PRA model developed for internal initiating events was used as a framework for addressing potential failures induced by seismic events. The internal events PRA model also provides the primary basis for establishing the seismic equipment list (SEL), which identifies equipment and structures for seismic fragility analysis.

The U.S. EPR PRA-based seismic margins assessment involves the following primary steps:

- Determine the seismic input
- Evaluate the seismic fragility to obtain HCLPF capacities for SSCs on SEL
- 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 SSCs that are limiting with respect to the potential for core damage.

The following subsections provide summary descriptions of these steps provided in the application and the staff's evaluation.

19.1.4.6.1.1 *Seismic Input*

Since the U.S. EPR standard design uses the certified seismic design response spectra (CSDRS) for seismic design of Category I SSCs, the seismic input to the seismic fragility analysis of SSCs in the SEL should be consistent with the CSDRS. For the seismic design of the U.S. EPR, the CSDRS is based on the European Utility Requirements (EUR) spectral shapes for ground motion, anchored to peak ground acceleration (PGA) of 0.3g. This PGA applies to both horizontal and vertical motions.

The CSDRS for the U.S. EPR are shown in FSAR Tier 2, Figure 3.7.1-1. These are ground response spectra for EUR Control Motions—hard (EURH), medium (EURM), and soft (EURS) soils. The staff reviewed the PRA-based seismic margin assessment against the guidance in SECY 93-087 to determine if there is a minimum seismic margin of 1.67 times the CSDRS.

The applicant used the NUREG/CR-0098 median spectral shapes anchored to the average peak spectral acceleration (PSA) in the 2 to 10 Hz frequency range to define the seismic input to the seismic fragility analysis. This resulted in a 1.17g average spectral acceleration for rock sites and 1.45g for the envelope of the soil sites. The applicant made comparisons of the NUREG/CR-0098 spectra with CSDRS raised by a factor of 1.67 for PGA which showed that the NUREG/CR-0098 spectra anchoring to the average PGA practically envelopes 1.67 times CSDRS for soil sites, while for rock sites it resulted in a spectral exceedance in the frequency range of 8 – 30 Hz. This means that the use of NUREG/CR-0098 spectral shape anchoring to

the average PSA between 2 – 10 Hz for rock sites results in a seismic margin less than 1.67 times CSDRS in this frequency range.

In the first part of RAI No. 234, Question 19-304, the staff requested that the applicant address the effect of the spectral exceedances for rock sites as discussed above. Specifically, the staff requested that for rock sites, the applicant identify those SSCs on the seismic accident sequences with fundamental frequencies falling within 8 – 30 Hz, and demonstrate that these SSCs possess adequate seismic margins to meet 1.67 times CSDRS based on the spectral acceleration; alternatively, the applicant can use the CSDRS as the seismic input to reconstitute the sequence level HCLPFs for the US EPR design. The applicant responded to this RAI on November 5, 2009. This response is currently being reviewed by the Staff. **RAI 234, Question 19-304, which is associated with the above request, is being tracked as an open item.**

19.1.4.6.1.2 *Seismic Fragility Evaluation*

The fragility evaluation characterizes the capacities of SSCs to withstand the ground motion due to an earthquake. Fragility is expressed as the conditional probability of failure of a SSC as a function of earthquake size. The capacity of a component to maintain its safety 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 which represents a 95 percent confidence that the failure probability is less than five percent.

For the U.S. EPR design certification, some details of the design, including specification of anchorage and detailed stress calculations, are not yet available. Therefore, for most SSCs generic estimates for these design margins were obtained from EPRI TR-103959 [Reed, J.W. and Kennedy, R.P., "Methodology for Developing Seismic Fragilities," EPRI TR-103959, Electric Power Research Institute, Palo Alto, California, 1994].

Since the U.S. EPR design uses the concept of a nuclear island (NI) which provides foundation support to most Category I Structures including containment, it is important that the NI has adequate seismic capacity. The staff noted that the fragility analysis by the applicant did not address the stability of the NI against seismic sliding and overturning. Therefore, in the second part of RAI No. 234, Question 19-304, the staff requested that the applicant demonstrate the seismic margin of 1.67 times CSDRS for the NI against seismic induced sliding and overturning. The applicant responded to this RAI on November 5, 2009. This response is currently being reviewed by the Staff. **RAI 234, Question 19-304, which is associated with the above request, is being tracked as an open item.**

19.1.4.6.1.3 *Systems and Accident Sequence Analysis*

The U.S EPR PRA-based seismic-margins used event trees and fault trees that comprise the model for internal initiating events so that potentially important accident sequences were identified, and so that the relationships among seismic failures and other failure modes could be captured.

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

The applicant identified the following consequential initiating events and included in the U.S. EPR seismic model:

1. Seismic loss of offsite power (S LOOP) – 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 were removed, as were events that reflected the use of systems that are not seismically qualified. 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.
2. Seismic small LOCA (S SLOCA) – 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.

Structures and other passive components not typically included in the internal events PRA were added to the SEL. Fault trees developed in the internal events PRA were used 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 SSCs for which fragility evaluations were performed have been added at appropriate points in the fault trees.
- Seismic failures were treated as common events for all 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.
- No credit is given for recovery of offsite power.
- Human failure events were retained in the fault-tree models, but were set to failure with a probability of 1.0.

The applicant identified loss of offsite power as the most important seismically induced initiating event because equipment needed for offsite power to function has low seismic capacity (e.g., ceramic insulators) 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.

For purposes of the seismic margins assessment, the U.S. EPR SMA assumed that a seismic event would lead to leakage from the RCS equivalent to an SLOCA. This assumption was made although 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 was included so that a broader set of equipment would be considered in the SEL and associated fragility evaluations. 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. 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 were also considered as initiating events that were assumed to result in core damage. The applicant evaluated these structures and assigned HCLPF capacities larger than the RLE based on its performed calculations and generic information.

The U.S. EPR seismic cutsets reflect the following contributions:

- Seismic failure of ac power cabinets, I&C cabinets, EDGs, batteries, ESWS or room cooling represent single element cutsets that limit the plant level HCLPF.
- Seismic failure of EFWS and failure of the operators to initiate feed-and-bleed cooling constitute the first two-element cutset.
- Seismic failure of CCWS and a consequential RCP 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 to permit injection by LHSI following a seal LOCA and MHSI failure, and the other is to initiate feed-and-bleed cooling.
- The last three cutsets include seismic failure of EFWS and non-seismic failures of equipment and failure of operator action. The seismic SLOCA results are similar to the seismic LOOP sequences. These cutsets also include two types of single-element cutsets that reflect seismic failures (i.e., failure of CCWS and failure of LHSI). Either failure would result in a loss of IRWST cooling, which is required in the long term following a LOCA.

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.

The staff noted that the applicant did not address the effects of seismically induced fires and the impacts of inadvertent actuation of fire protection systems on other safety systems and the effects of seismically induced external flooding and internal flooding on plant safety during plant walkdowns. Thus, in RAI 97, Question 19-220, the staff requested that the applicant provide a COL Action Item for performing the above assessments.

In an October 17, 2008, response, the applicant stated that the following assumption will be added to FSAR Tier 2, Table 19.1-109, "U.S. EPR PRA General Assumptions." It should be noted that, FSAR Tier 2, Section 19.1.2.2, COL Information Item 19.1-9 requires a COL applicant to review of as-designed and as-built information in order to confirm that the assumptions used in the PRA remain valid.

> The PRA-based seismic margin assessment assumes that equipment will be installed as designed and that there are no potential spatial interaction concerns in the as-built configuration (e.g., adjacent cabinets are bolted together, collapse of non-seismically designed equipment or masonry wall onto safety-related equipment is precluded, and no likelihood of seismically induced fire or flood impacting safety-related equipment).

Inclusion of the above assumption and appropriate references in the FSAR text is being tracked as Confirmatory Item 19-220.

The staff finds that the U.S EPR seismic-margins model is consistent with SR SM-B4 of ANSI/ANS-58.21-2007 by analyzing seismically initiated transient events (SLOOP) and small seismically induced primary coolant leakage events (S SLOCA). The SLOOP and S SLOCA event trees shown in FSAR Tier 2, Figures 19.1-10 and 19.1-11 logically identified the top events in consistent with the U.S. EPR design. The staff finds the accident sequences

generated by these events trees to be consistent with the event tree logics. Therefore, the staff concludes that the U.S. EPR seismic-margins modeling approach is appropriate and is detailed enough to establish the SEL.

19.1.4.6.1.4 *High Confidence of Low Failure Probability Sequence Assessment*

The seismic margin assessment evaluates the impact of seismic initiators by determining whether there is adequate margin. The applicant used the "MIN-MAX" method of evaluating accident sequences at the cut-set level 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 were also considered in the evaluation. The result of this evaluation is identification of the structures and components that arise in the core damage cutsets and that limit the plant-level HCLPF.

The staff reviewed Table 19-215-1 "Summary of Seismic Capacity of Structures of U.S. EPR" and Table 19-215-2 "Summary of Seismic Capacity of Equipment of U.S. EPR" provided in the applicant's October 17, 2008, response to RAI 95, Question 19-215, and finds that there are no SSCs with HCLPF values less than 0.5g PGA. Therefore, the staff determines that the U.S. EPR level HCLPF is at least 0.5g PGA and is in accordance with SECY-93-087.

In RAI 349, Question 19-330, the staff requested that the applicant provide additional information regarding the results of the HCLPF Sequence Assessment (i.e., identification of the structures and components that may limit the plant-level HCLPF capacity, the potential seismic vulnerabilities relative to the RLE, and the proposed measures to reduce risk impact). **RAI 349, Question 19-330, which is associated with the above request, is being tracked as an open item.**

The staff recognizes that the PRA-based seismic margin analysis is based on the design information provided in the DCD and its results may be affected by site-specific seismic characteristics of a particular site. Therefore, in the third part of RAI No. 234, Question 19-304, the staff requested that the applicant provide a COLA Information Item for meeting Part 52.79(a)(46) to update the system model (seismic accident sequences) developed in the DCD to incorporate site-specific capacity reductions due to site-specific effects (soil liquefaction, slope failure, etc.) and site-specific structures (safety related site-specific intake structure, intake tunnel heat sink,) if any appears on the seismic accident sequences used for the PRA-based HCLPF assessments of the DC, and demonstrate the seismic margins of the applicable site-specific SSCs; the HCLPFs for respective site-specific SSCs will be estimated based on the site-specific GMRS. The applicant responded to this RAI on November 5, 2009. This response is currently being reviewed by the staff. **RAI 234, Question 19-304, which is associated with the above request, is being tracked as an open item.**

19.1.4.6.1.5 *Sensitivities and Uncertainties*

The applicant stated that, because the seismic margin assessment is primarily qualitative, no sensitivity and uncertainty studies are conducted. The staff agrees that, because the applicant performed PRA-based SMA, it is not necessary to perform the sensitivity and uncertainty studies.

19.1.4.6.2 FSAR Tier 2, Section 19.1.5.2: Internal Flooding Risk Evaluation

19.1.4.6.2.1 *Internal Flooding Methodology*

The applicant performed a bounding internal flooding PRA to evaluate risk from flooding events and to obtain related risk insights. Floods were analyzed for the entire building, the worst PRA scenario resulting from the failure of all SSCs in the building was modeled, and the total building flooding frequency was applied to that scenario. For each building containing SSCs credited in the internal events PRA, the internal flooding evaluation was performed in the following steps:

- Calculate flooding frequency based on the flooding sources and piping segments
- Analyze possible flooding scenarios for each location and select the worst scenario
- Apply the total building flooding frequency to the worst scenario, and calculate the corresponding CDF and LRF

The applicant identified and selected the following eight U.S. EPR buildings that contain SSCs credited in the internal events PRA for the flooding analysis:

- Four Safeguard Buildings
- Fuel Building
- Reactor Building Annulus
- Essential Service Water System Building
- Turbine Building

The Switchgear (SWGR) Building and Emergency Power Generation Buildings (EPGBs) that also contain SSCs credited in the internal events PRA, were screened out from the flooding assessment because the SWGR Building does not contain significant flooding sources, and a flood in an EPGB would not cause an initiating event but would only disable the corresponding EDG.

The principal flooding protective measure for these eight buildings is physical separation. Below elevation +0 m (+0 ft), 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 m (+0 ft), a combination of watertight doors and openings for water flow to the lower building levels prevents water ingress into adjacent divisions. In SBs, only the ESWS system contains enough water to rise to the +0 m (+0 ft) elevation, and potentially propagates to the adjacent SB. Safety sensors in the sumps are installed to ensure a prompt trip of the effected ESWS pump. Propagation between buildings through a backflow from the drain collection headers is not considered, 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 (i.e., door) are analyzed together, such as, FB and SB 1 and SB 4, and between RB annulus and SB 2 and SB 3.

Based on the evaluation of the information summarized above, the staff determines that the applicant's modeling approach for U.S. EPR internal flooding events is conservative because it defined/analyzed flood areas at the level of buildings and/or portions thereof from which there would be no propagation to other modeled buildings and applied the total building flooding frequency to the worst scenario. The staff reviewed the conceptual configuration and layout of U.S. EPR buildings in FSAR Tier 2, Chapter 1, and finds that the applicant properly identified and selected the flood areas for the flooding assessment. The staff finds that the U.S. EPR internal flooding modeling approach is consistent with ASME-RA-Sc-2007 PRA Standard, and is therefore acceptable.

19.1.4.6.2.2 *Flooding Frequencies for the Selected Locations*

In developing flooding frequencies, the applicant considered all plant systems that transport fluid through a selected flood areas as potential flood sources. Specifically, for each selected location, the following flooding sources were considered in the flooding analysis:

- equipment (e.g., piping, valves, pumps, tanks or pools) in the location
- external sources of water (i.e., UHS reservoirs), that are connected to the location through some systems or structures

The applicant chose Topical Report EPRI TR-102266, ("Pipe Failure Study Update," Electric Power Research Institute,1993), to derive internal flooding frequencies for the selected locations/buildings. EPRI TR-102266 gives a pipe break frequency based on the number of pipe segments for different sizes of pipes and for different systems. For each selected building, the flooding frequency was calculated based on the number of pipe segments as determined by the piping and instrumentation diagrams (P&IDs). Both operating systems and standby systems (including the fire water system) were considered in the calculation. The systems were chosen based on their potential to cause a significant flooding event. 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. For the TB, a generic flooding event frequency from NUREG/CR-2300 is used because no P&IDs are available yet for the systems located in the building.

The staff review found that the flooding sources of valves, pumps, tanks, and pools have not been included in the flooding analysis. Thus, the staff issued RAI 4, Question 19-50 and RAI 142, Question 19-262 to request justification for the exclusion of these potential flooding sources. The applicant responded to these questions on May 9, 2008, and March 6, 2009, respectively, and stated that EPRI TR-102266 does not explicitly state whether non-piping components, such as pumps, valves or heat exchangers are included in the pipe segment rupture frequencies. Thus, to assess the potential impact of non-piping components, the applicant performed a sensitivity study comparing U.S. EPR internal flooding frequencies against the frequencies obtained using a data source that explicitly includes non-piping components (i.e., EPRI Report 1013141, "Pipe Rupture Frequencies for Internal Flooding PRAs, Revision 1").

The sensitivity study showed that using EPRI Report 1013141 flooding frequencies results in a small (one percent) decrease in overall flooding CDF. The resulting flooding CDF from the sensitivity study was calculated to be 6.3E-8/yr. This value is slightly lower than the total flooding CDF of 6.4E-8/yr as shown in FSAR Tier 2, Table 19.1-40 and slightly higher than the U.S. EPR flooding CDF of 6.1E-8/yr due to the lower relative truncation for individual scenarios.

The staff examined the applicant's sensitivity study and concludes that, because of the conservatism embedded in the U.S. EPR flooding frequency estimate and the low contribution of valves, pumps, tanks, and pool to the frequency, the exclusion of non-piping components is acceptable.

The staff review also noted the exclusion of human-induced flooding events from the flooding frequency estimate. Thus, in RAI 120, Question 19-228c, the staff requested a sensitivity study specifying the impacts of these events on the internal flooding CDF. In a November 26, 2008, response, the applicant evaluated the effects by performing an assessment which identified the following types of events as potential human-induced floods:

- Maintenance on a system that is not isolated
- Spurious valve operation or valve rupture while system is open for maintenance
- System vent valve or other valve left open during system restoration
- Inadvertent tank overflow during tank fill
- Inadvertent actuation of a fire water system

The applicant stated in the response that, based on the industry flooding data, the historical frequency of significant (greater than 2000 gallons released) human induced flooding at-power is low. There have been only four events of this type, three of which were in the Turbine Building. The operational experience covered by this data includes over 9000 reactor-years, giving human-induced flooding at-power a point estimate frequency of:

- 3.3E-04/yr in the Turbine Building
- 1.1E-04/yr in the Safeguard Buildings
- 4.4E-04/yr the total flooding frequency for all areas

Based on this additional information and the demonstrated small effect on the estimated internal flooding frequency, the staff finds that the contribution from the human-induced floods is not likely to change the U.S. EPR flooding frequency of 4.3E-02/yr significantly (less than 1.5 percent) and is not expected to have a significant impact on the results.

Based on the information provided in the FSAR and in the applicant's responses to RAIs, the staff concludes that, at the design stage, the applicant practically estimated the U.S. EPR flooding frequency based on the available design information. To ensure that the estimated flooding frequency will remain valid for the as-built, as-operated plant, the applicant stated in the COL Information Item 19.1-9 that "[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 remain valid with respect to internal events, internal flooding, internal fire, human reliability analyses, PRA-based seismic margins, and other external events."

19.1.4.6.2.3 *Flooding Scenarios*

For each location/building selected for the flooding analysis, the applicant defined the worst flooding scenario by assuming all mitigating equipment at the location was lost. Other effects of

pipe breaks, like jet impingement, spray, pipe whip, or humidity, were not specifically evaluated because all equipment at a location was considered to be failed.

Due to the complexity of the RB annulus flooding scenario, the applicant developed a simple event tree to calculate the flooding frequency. In this scenario, an operator action was credited to isolate a pipe break before a significant flood level to occur. 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. The operator action and these two propagation paths resulted in five possible outcomes as follows:

- Operator successfully isolates flooding before any undesirable consequences can occur
- Flooding propagates to both SBs 2 and 3
- Flooding propagates to SB 2 only
- Flooding propagates to SB 3 only
- Unisolated flooding is contained inside the RB annulus and reaches the level of the electrical penetrations to the containment.

If propagation occurs, the safety systems in the adjacent building are assumed to be failed. If the flood is not isolated and contained in the annulus, the water level is assumed to reach containment penetrations. Control and power cables are designed to pass through the annulus in air-tight conduits and enter the containment through the connection boxes. The applicant estimated that, if flooded, the connection boxes would fail with a probability of 0.5. If the connection boxes fail, the applicant assumed that connection with the containment, including all instrumentation, is lost and, therefore, core damage is assumed to result.

The staff review noted that, for the analyzed RB annulus flooding scenario, the treatment of door failure and potential impacts of barrier failure may not have been adequately credited and assessed in the flooding model. Thus, in RAI 4, Question 19-52 and RAI 120, Question 19-228e, the staff requested that the applicant provide the potential impacts of these findings on the flooding results. The applicant responded to these questions on May 9, 2008, and November 26, 2008, respectively, and described that if failure of the doors between the annulus and the SBs is not to be modeled, which would also imply that barrier structural failure is not to be considered, the approach to modeling this scenario would be changed to the following.

Without the concern for door opening, the operators would have more time to isolate, because the new height of concern becomes the elevation of the lowest electrical penetration (Elevation +4.88 m (+16 ft)) and not the elevation of the doors (Elevation +0 m (+0.0 ft)). The operator action was re-evaluated based on the time that it would take for the water column to reach elevation +4.88 m (+16 ft) (calculated to be 73 minutes). The HEP was recalculated to be 2.0E-4 based on 73 minutes timing, assuming nominal stress for diagnosis and action. The CDF resulting from this scenario would become 3.2E-8/yr.

Currently, as reported in the FSAR, the U.S. EPR CDF for all annulus floods was calculated to be 3.2E-8/yr. Thus, the two approaches are found to yield similar results.

Although the approach currently described in the FSAR to modeling RB annulus flooding is not quite practical, the staff concludes that crediting door failures would not significantly change the CDF and CRF from the U.S. EPR internal flooding analysis. Thus, the RB annulus flooding CDF of 3.2E-8/yr is acceptable based on the evaluation provided in the response to RAI 120, Question 19-228e.

To calculate the corresponding CDF, the flooding scenarios were quantified using the same fault tree and event tree logics developed in the Level 1 internal events PRA. The unavailable mitigating systems assumed in a flooding scenario were disabled in the quantification for each scenario. FSAR, Tier 2 , page 19.1-117, last paragraph, indicates that flooding scenarios are quantified using the same event tree logic used in the Level 1 internal events evaluation; however, it does not specifically indicate the event trees. The staff issued RAI 142, Question 19-264, and requested that for each analyzed scenario, the applicant identify the conditional event tree used to quantify the internal flooding CDF and provide the basis for selection. In a January 8, 2009, response, the applicant identified the event tree used to quantify each flooding scenario, as well as the mitigating systems assumed to be disabled by these flooding scenarios.

The staff finds the U.S. EPR flooding analysis does not include main control room (MCR) flooding. Thus, in RAI 4, Question 19-54, the staff requested that the applicant provide clarification for the exclusion. In a May 9, 2008, response, the applicant described that the MCR was not included in the internal flooding PRA, because no flood scenario was identified that could affect the MCR. The fluid-carrying systems at or above MCR elevation of 16.15 m (53 feet), were identified as follows:

- Fire water distribution system (FWDS)
- Safety chilled water system (SCWS)
- Potable and sanitary water system (PSWS)
- Demineralized water system (DWS)
- Component cooling water system (CCWS)

The floors at and above Elevation +16.15 m (+53 ft) are designed to direct water releases from FWDS, SCWS, DWS, CCWS, via openings and pipe shafts, to the lower elevations of the building. Therefore, the control room would not be affected by a break in any of these systems. There are parts of the PSWS that are located within the control room (piping to the operator's toilets). A pipe break or a system malfunction in this area could result in a flooding event. The occurrence of a significant flooding event from this system was judged to be unlikely based on the following:

- The PSWS is fitted with two automatic isolation valves upstream of the connection to SB 2. These isolation valves would close when the water height reaches the actuation level of the local measurements in the operator's toilet rooms.
- If the automatic isolation fails, it is very likely that the operators would notice the flood and manually isolate it. The flow rate for a potable and sanitary water pipe break is expected to be low [2.54 cm (1 in.) pipe], giving operators ample time to terminate the flood.

Based on the above additional information and the applicant's demonstration that no flood scenario is capable of significantly impacting the MCR, the staff determines that the MCR can be screened out from the flooding PRA.

The staff also noted that the potential electrical equipment failures in other divisions or at other locations due to water contact or pipe whip on cables/conduits/cabinets are not clearly addressed in the U.S. EPR flooding PRA. Thus, the staff issued RAI 4, Question 19-51, requesting additional information on this issue. In a May 30, 2008, response, the applicant stated that the internal flooding PRA did not identify any potential electrical equipment failures in multiple divisions or locations. In general, divisional separation in the U.S. EPR is such that flood events affecting one building would have effects restricted to that particular division. Because of a possibility to cross connect safety buses between different divisions (alternative feed), there could be places where two different electrical divisions are connected. However, the SB switchgear rooms where cables would be routed together were not included in the internal flooding PRA, because no flood scenario was identified that could affect them.

The U.S. EPR flooding analysis for the SBs showed that the floors at and above Elevation +4.57 m (+15 ft) are specifically designed so that water released by the FWDS, SCWS/OCWS, DWDS, and CCWS would be directed via openings and pipe shafts to the lower elevations of the building. There is enough free volume between Elevation -9.45 m (-31 ft) and Elevation +0 m (+0 ft) to contain the largest postulated flooding event; therefore, elevations above ground level would not be affected.

Furthermore, there are four locations within the SBs where cables from more than one division are routed together. These locations were assessed as follows:

- MFW/ main steam (MS) valve rooms located on the top elevations of SBs 1 and 4 – MFW/MS valve room flooding sources are steam/feed line breaks. The flooding effects associated with these breaks are studied in the High Energy Line Break analysis. This analysis concluded that the high energy line breaks effects would not adversely challenge the plant functions credited to respond to this event. The MFW and main steam components in this area are designed for harsh environments.

- Control room in SB 2 – The control room was not included in the internal flooding PRA, because no flooding hazard was identified that would affect this area.

- Cable spreading area in SB 2 – The cable spreading area was not included in the internal flooding PRA, because no flooding hazard was identified that would affect this area.

- Remote shutdown station (RSS) floor in SB 3 – The remote shutdown station was not included in the internal flooding PRA, because no flooding hazard was identified that would affect this area.

The staff reviewed the plant description described in FSAR Tier 2, Chapter 1, the design of SSCs in FSAR Tier 2, Chapter 5, and the applicant's response to the RAI, and the staff finds that the potential for equipment failures in multiple divisions or locations due to a flooding event can be negligible.

Based on the information provided in the FSAR and additional information provided in the applicant's responses to the RAIs, the staff concludes that the applicant has appropriately

identified the U.S. EPR flooding scenarios, consistent with the ASME PRA Standard and RG 1.200.

19.1.4.6.2.4 *Results of Internal Flooding*

As currently documented in the FSAR Tier 2, Section 19.1.5.2.2.1, the total point estimate CDF from internal flooding events was estimated to be 6.1E-8/yr (mean CDF = 8.8E-8/yr). All flooding initiating events modeled and their contribution to the internal flooding CDF are summarized in Table 19.1-10, "Internal Flooding CDF," of this report. However, in an April 10, 2009, response to RAI 197, Question 19-274, regarding the design change to maintain the EFWS supply header isolation valves closed during operation, the applicant recalculated the U.S. EPR flooding CDF to include the design change to 6.7E-8/yr. In either case, the staff finds that the U.S. EPR internal flooding CDF is well below the NRC goal of 1.0E-4/yr.

Table 19.1-10 Internal Flooding CDF

Location ID	Description	Frequency (/yr)	CDF (/yr)	CDF (%)
IE FLD-ANN ALL	Flood in the RB Annulus (contained)	6.4E-08	3.2E-08	50.0%
IE FLD-SAB14	FB Flood in SB 1 or 4 (Pump Room) including Fuel Building, excluding EFWS-caused floods	5.8E-03	2.1E-08	32.3%
IE FLD-EFW	EFW-caused flood in SB 1 or 4 propagating to the Fuel Building	1.4E-03	7.2E-09	11.3%
IE FLD-TB	Flood in the TB	3.3E-02	4.0E-09	6.3%
IE FLD-SAB23	Flood in SB 2 or 3 (Pump Room), excluding EFWS-caused floods	1.9E-03	3.3E-11	0.1%
IE FLD-ESW	Flood in the ESWS Building	7.2E-04	4.0E-11	0.1%
IE FLD-ANN SAB23	Flood in the RB Annulus, propagating to the Safeguard Building 2 and 3 (Pump Room)	5.8E-07	8.9E-13	0.0%
IE FLD-ANN SAB2	Flood in the RB Annulus, propagating to the Safeguard Building 2 (Pump Room)	5.8E-06	1.3E-12	0.0%
		Total	6.1E-08	100%

As can be seen from Table 19.1-10 of this report, the flood contained in the annulus dominates the internal flooding CDF, which contributes about 50 percent. The next biggest contributor to the flooding risk is a flood in SB 1 or SB 4. The third largest contributor is the TB flood. The important contribution of these specific buildings could be attributed to the PRA modeling assumption on the initially running CCWS trains, and on the location of the CCWS switchover

valve, so that a flood in SB 1 or SB 4 would disable one CCWS common header. The relatively high contribution of the TB flood was mainly caused by the high flood frequency and a loss of both main feedwater and startup and shutdown systems as a result of a flood. All other flooding scenarios contribute less than one percent to the total internal flooding CDF.

The staff finds that the low estimated internal flooding CDF and leading contributors identified above are the results of the decent spatial separation of the safety SSCs.

Significant Cutsets and Sequences

The key sequence related to the flooding scenarios is a flood in SB 1 which could result in a failure of the CCWS CH 1. In the following sequence of this event, the flood disables the Division 1 running CCWS train and the corresponding switchover valves (assumed to fail open), thereby disabling a switchover to the CCWS 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 FSAR Tier 2, 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 same is true for SB 4, which hosts another running CCWS train.

According to the top 100 cutsets, one cutset dominates the flooding CDF, with a contribution slightly above 50 percent. This cutset relates to a flood contained in the annulus as previously discussed. Apart from this outlier, cutset contributions to the internal flooding CDF are relatively evenly distributed, and mostly less than one percent contribution each. The number of cutsets that contribute to 95 percent of the flooding CDF is larger than 12,500.

FSAR Tier 2, Table 19.1-41 shows the important cutsets of Level 1 internal flooding.

The staff finds that the cutsets provided in FSAR Tier 2, Table 19.1-41 are consistent with the flooding scenarios discussed in the previous section.

Significant SSCs, Operator Actions, and Common Cause Events

According to the U.S. EPR internal flooding PRA, the applicant identified the important SSCs, operator actions, and common cause events as follows:

- MHSI pump trains have the highest FV. This was caused by an overall high contribution of the consequential RCP seal LOCA sequences that follow a flood in a SB and a need of safety injection.

- RCP seal isolation MOVs (i.e., nitrogen and leakoff valves) and SSSS are the two most important components. This was caused by the importance of those components in preventing an RCP seal LOCA following a flood in SB 1 or SB 4. Since the floods are assumed to propagate to the FB, they could simultaneously fail one CCWS common header and the CVCS, thereby disabling thermal barrier cooling and the seal injection to two RCPs. In addition, a single failure of RCP seal isolation MOV or the SSSS could result in a seal LOCA.

- Failure to recover room cooling locally following a loss of ventilation is the most important operator action based on the FV. This reflects the importance of ventilation dependencies in the plant risk in general.

- Operator failure to initiate a feed and bleed for transient events is the most important operator action based on the RAW value. Its importance was caused by multiple flooding sequences leading to a total loss of feedwater.

- Operator failure to isolate a FWDS break in the annulus is also important; however, because it is modeled as part of the initiating event frequency, it is not shown in either FV or RAW list.

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

- CCF of the TXS operating system is the most important common-cause I&C failure. 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 flooding event.

19.1.4.6.2.5 *Key Assumptions*

The key PRA assumptions related to the modeling of internal flooding events were identified as follows:

- Due to incomplete information on equipment and piping locations, it was assumed that a flood in any building would fail all equipment in this building.

- It was 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 was assumed that any flood would cause it to fail.

- A flood in an SB was assumed to affect the CCWS switchover valves. This is believed to be 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) were assumed to be contained below ground level of the affected buildings (SB or FB). This is believed to be a reasonable assumption, since those systems are automatically isolated if the building sump detects a large flooding event. Moreover, if automatic isolation failed, operators would have a higher chance to isolate the break, since expansive time is needed to flood a building up to ground level.

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

The staff concludes that the documentation of assumptions in the FSAR is sufficient to ensure that they will remain valid for the as-built, as-operated plant. Any changes to these assumptions will be incorporated in the PRA as part of the PRA maintenance process described above in the evaluation of FSAR Tier 2, Section 19.1.2. Addressing COL Information Item 19.1-9, to which FSAR Tier 2, Table 19.1-109 refers, is the responsibility of the COL holder.

19.1.4.6.2.6 *Sensitivity Analysis*

The applicant performed 26 sensitivity case studies to evaluate the impact of a series of the PRA modeling assumptions and HEP values on the flooding CDF. FSAR Tier 2, Table 19.1-49 provides the results from the Level 1 flooding events sensitivity studies. The applicant has drawn several insights from the analyzed sensitivity cases as summarized below.

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 was explained by the fact that the flooding CDF is dominated by one scenario of annulus flooding.

The flooding CDF is sensitive to the assumption on seal LOCA probability this assumption. This is consistent with the high importance of components and assumptions related to the mitigation of seal LOCAs. 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 CCWS CH 1 or 2 and the CVCS directly leading to a loss of seal cooling.

The impact on the CDF of the assumptions specific for the flooding events modeling was also studied. The assumption on the isolation of an EFWS tank leak 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.

Besides the sensitivity studies documented in the FSAR, the applicant performed additional sensitivity studies to support RAI responses. These studies are described in the text above as appropriate. Generally, these sensitivity studies demonstrated that a particular modeling assumption or simplification questioned by the staff had no significant impact on the results and insights of the PRA.

Based on the information presented above, the staff concludes that the applicant has sufficiently evaluated uncertainties in the internal flooding PRA, in part by performing sensitivity studies, and identified important equipment. Generally, these sensitivity studies demonstrated that the modeling assumptions or modifications questioned by the staff had no significant impact on the results and insights of the internal flooding PRA.

19.1.4.6.2.7 *Uncertainty Analysis*

The applicant performed an uncertainty analysis on the Level 1 internal flooding PRA results using a process similar to that described for the internal events PRA by propagating uncertainty distributions within the RiskSpectrum® software. Parametric uncertainty was represented by selecting an uncertainty distribution for each parameter type.

FSAR Tier 2, Figure 19.1-13 shows the results of the uncertainty analysis for Level 1 flooding events. The uncertainty results are summarized as follows:

- Internal flooding CDF mean value = 8.8E-8/yr
- Internal flooding CDF 5 percent value = 3.1E-9/yr
- Internal flooding CDF 95 percent value = 2.2E-7/yr

As seen above, the absolute values of 5th percentile and 95th percentile are less than the internal events uncertainty results by a factor of about 10. This distribution gives the staff confidence that the U.S. EPR internal flooding CDF is within the Commission's CDF objective of 1E-4/yr.

19.1.4.6.2.8 *Flooding PRA Insights*

Based on the internal flooding assessment, the applicant obtained several 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.
- Flooding in the SB 1 or SB 4 is dominated by the seal LOCA scenarios, because the flood would cause a complete loss of seal cooling to two of the RCPs, and a single failure in the isolation of the RCP seals would result in a seal LOCA. Seal LOCA sequences contribute to more than 30 percent of the flooding events CDF.
- Dependencies between support systems are also important 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.

The staff finds that the applicant has appropriately identified and documented risk insights from the internal flooding assessments, consistent with the U.S EPR design information provided in the FSAR and internal flooding model.

19.1.4.6.2.9 *Level 2 Flooding Analysis*

As described above, conservative flooding accident scenarios are developed by assuming that flooding could involve an entire building (eight scenarios in total), that would lead to the failure of all SSCs in the building, and that the total building flooding frequency is applied to that scenario. A key Level 2 assumption is that an unisolated flood in the annulus which results in the loss of instrumentation and signals to and from the containment fails all Level 2 operator actions.

Flooding scenarios are quantified using the same fault tree and event tree logic used in the internal events evaluation.

Approximately 76 percent of the LRF for flooding events are early containment failures by hydrogen flame acceleration induced containment rupture (Release Category RC304, containment failure before vessel failure). About 18 percent are thermally-induced SGTRs (RC702). Sequences involving consequential seal LOCAs are significant (about 38 percent) LRF contributors.

The sensitivity of the results to the phenomenological events is 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. Flooding LRF results are sensitive to the value of basic events related to

flame acceleration loads and in-vessel steam explosions. The events are assessed as having a very low probability, and increasing the probability to one has a very large numerical impact, though the applicant considers this probability to be physically unreasonable.

The sensitivity to the combined unavailability of feedwater and manual primary depressurization results in a significant impact on the thermally-induced SGTRs.

The calculated LRF values for internal flooding events are listed in Table 19.1-11 of this report.

Table 19.1-11 Level 2 Risk Metric Results for Internal Flooding

Risk Metric	Point Estimate	Quantile		
		Mean	5th percentile	95th percentile
LRF	1.1E-09/yr	1.2E-09/yr	1.0E-12/yr	1.2E-09/yr
CCFP	0.018	0.014	--	--

The LRF results for flooding events are dominated by severe accident phenomenological events, in particular, 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.

19.1.4.6.2.10 *Staff Evaluation*

The applicant performed the internal flooding PRA commensurate with the level of detail available and made conservative assumptions, where detailed information was not available, to bound the flooding analysis. The staff finds that the U.S. EPR flooding analysis is reasonable and sufficient to identify potential vulnerabilities and to lend insight into the design which can be used to support design certification.

The staff finds that the applicant's flooding analysis provides reasonable accident sequences and CDF and LRF estimates to draw the conclusion that the U.S. EPR design is capable of withstanding severe accident challenges from internal floods in a manner superior to operating plants.

Based on the preceding discussion, the staff concludes that the approach and results of the internal flooding PRA described in the FSAR Tier 2, Revision 1, Section 19.1.5.2, "Internal Flooding Risk Evaluation," are acceptable and meet the Commission's goals of less than 1.0E-4/yr for CDF and less than 1.0E-6/yr for LRF. The U.S. EPR internal flooding analysis has provided useful safety insights for COL information items and RAP.

The staff expects that COL holders will update and upgrade the information in the design-specific internal flooding PRA to incorporate site-specific information as part of the site-specific PRA development required by 10 CFR 50.71(h)(1) as follows:

> No later than the scheduled date for initial loading of fuel, each holder of a combined license under subpart C of 10 CFR part 52 shall develop a level 1 and a level 2 probabilistic risk assessment (PRA). The PRA must cover those initiating events and modes for which NRC-endorsed consensus standards on PRA exist one year prior to the scheduled date for initial loading of fuel.

19.1.4.6.3 FSAR Tier 2, Section 19.1.5.3: Internal Fires Risk Evaluation

The applicant performed internal fire analysis in the design certification PRA, accounting for the good spatial separation of the safety structures, systems, and trains in the U.S. EPR. The worst PRA scenario resulting from the failure of all SSCs in the FA is modeled, and the total area fire ignition frequency is applied to the scenario. To assess the internal fire risk, for each building containing SSCs credited in the internal events PRA, the applicant performed the following steps:

- Estimated fire frequency based on the available industry experience.
- Assumed that each fire will grow to be a fully developed fire.
- Analyzed possible fire scenarios for the location, and based on the PRA model, selected the worst-case scenario.
- Credited automatic fire suppression, if the specific fire did not affect it. Manual fire suppression was only credited in the MCR.
- Credited 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.
- Applied the total building/FA frequency to the worst scenario and calculated the corresponding CDF and LRF.

Since the analyzed fire locations were all designed to be separated by three-hour fire barriers, the propagation between areas was not considered. The applicant did not utilize any fire-damage models, since all equipment inside a FA was assumed to fail.

Based on the information summarized above, the staff concludes that the applicant's modeling approach for U.S. EPR internal fire assessment is conservative, and acceptable.

19.1.4.6.3.1 *Internal Fire Ignition Frequencies*

Fire Areas Selected for Internal Fire Risk Evaluation

The applicant utilized the partition of the U.S. EPR plant into FAs as defined in Appendix 9A of the FSAR Tier 2, Fire Hazard Analysis (FHA). The numerous FAs were then grouped into a limited number of PRA fire areas (PFAs) that contain SSCs modeled in the internal events PRA, and where a loss of equipment due to a fire would have a similar impact on the plant response.

U.S. EPR FHA FAs and corresponding FAs modeled in the fire PRA are defined in FSAR Tier 2 Table 19.1-62. The PFAs described in FSAR Tier 2, Table 19.1-62 were then grouped as fire scenarios by selecting one PFA as representative of symmetrical PFAs. The fire scenario was defined and modeled as occurring in the chosen PFA; its frequency was defined as the sum of fire ignition frequencies for all the PFAs represented by the scenario.

Fire Frequencies for the Selected Fire Areas

The applicant used the method described in RES/OERAB/S02-01, "Fire Events – Update of U.S. Operating Experience 1986-1999," to estimate U.S. EPR fire ignition frequencies. Each

evaluated PFA was matched with a corresponding generic location in that reference. Correction factors were 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, the method described in NUREG/CR-6850 was used. The NUREG/CR-6850 method defines plant-wide fire ignition frequencies for each type of component. An ignition frequency for a specific U.S. EPR PFA was derived by the percentage of components in that area for each component type. This method was used for three PFAs (i.e., 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 plant-specific spatial database, general arrangement drawings, and FHA.

The transient fires were not specifically considered in the analysis. It was assumed that they are enveloped in the used generic fire frequencies. For the areas where component specific frequencies have been used (i.e., transformer yard, MFW/MS valve room, and containment), it was assumed that a transient contribution would be very limited.

In an October 9, 2008, response to RAI 66, Question 19.01-23, regarding the above assumption that the transient contributions in the transformer yard and MFW/MS valve room would be limited, the applicant described that the assumption was made based on an engineering judgment. It is unlikely that transient combustibles would be present or stored in these areas, because maintenance activities at power are not expected there and these areas are not on the access paths to the other areas. The applicant will be re-evaluating the assumptions on transient combustible contributions when maintenance procedures and plant-specific experience are available. COL Information Item 19.1-9 listed in FSAR Tier 2, Table 1.8-2 is provided to ensure that assumptions used in the PRA remain valid for the as-to-be-operated plant.

The PFA frequencies and their basis are provided in FSAR Tier 2, Table 19.1-63. Because these frequencies are based on limited information, the CNI distribution was used to model uncertainties in the estimated values.

The staff noted that the estimated ignition frequency of fire area PFA-CNTMT “Pressurizer Compartment,” of 1.9E-5/yr is low and, thus, the staff issued RAI 66, Question 19.01-29, requesting that the applicant provide a justification for this frequency. In an October 9, 2008, response, the applicant stated that, due to the large size and small combustible loading of the PFA, a fire that would affect all components is not postulated. Instead, a specific analysis of vulnerable locations was performed. Reactor coolant pump fires due to oil leakage have been the source of most fires in-containment in operating history. Due to the specific oil collecting system described in FSAR Tier 2, Section 5.4.1.2.2, the applicant concluded that this event could not occur in the U.S. EPR. Reactor coolant pump fires are, therefore, not analyzed as a credible fire scenario. Consequently, a scenario involving a spurious opening of a PSRV was chosen to represent fires in the containment.

The frequency of 1.9E-05/yr was applied to the fire scenario, “fire in the pressurizer compartment,” assuming spurious opening of one of three PSRVs or both MOVs on one of the two SADV trains. It was obtained by multiplying the area ignition frequency of 4.9E-5/yr by the conditional probability of a hot short induced spurious operation of the pressurizer valves/train.

The ignition frequency of 4.9E-5/yr was estimated using the NUREG/CR-6850 method. The conditional probability of a spurious actuation in the event of a fire was calculated for the considered pressurizer valves (three PSRVs and two SADV MOVs). Each PSRV is powered through two different divisions that are routed to two pilot SOVs. Spurious opening of the valve

could occur only if two simultaneous hot shorts occur in two trains. Similarly, in order to open a primary depressurization train, two simultaneous hot shorts have to occur for two MOVs in series that are supplied from two different divisions. Using NUREG/CR-6850, Appendix J, the probability of one hot short was estimated to be 0.33 for SOVs and 0.17 for MOVs. Thus, the frequency of a fire with a valve opening was calculated to be (4.9E-5/yr * 0.33) + (4.9E-5/yr * 0.17) = 1.9E-05/yr.

The staff examined the RAI 66, Question 19.01-29 response and disagreed with the conclusion that stated the RCP fires could not occur in the U.S. EPR and could be excluded from the fire analysis. Thus, the staff issued RAI 227, Question 19-302, requesting that the applicant revise the fire area PFA-CNTMT frequency to correctly address RCP and containment fires or provide further justification. In addition, the staff also requested that the applicant provide justification for the exclusion of the transient ignition frequency associated with the containment hotwork.

In a July 6, 2009, response, the applicant stated that the sentence from the response to RAI 66, Question 19.01-29 was not intended to mean that RCP fires could not occur. Instead, the meaning of that sentence was that RCP oil fires with a high heat release were extremely unlikely and, therefore, were not considered as a credible fire scenario in the containment. Small fires such as a motor fire, limited oil fire, and pump casing insulation fire could occur, but would only affect the pump itself. The consequences of such an event would be limited to a reactor trip with one RCP unavailable, and its frequency would be negligible compared to the general transient frequency.

The oil collection system is designed such that an oil leakage from any location of the pump is captured and directed to an oil collection tank. Therefore, an oil spill onto the containment floor, which is a prerequisite to a significant fire, is precluded. The oil collection system is a passive component, thus the probability of its failure combined with an oil leak and a fire ignition would be extremely low.

In order to justify the exclusion of the RCP fires from the fire scenarios considered in the containment, the applicant evaluated a few possible RCP fire scenarios including fires of the pump itself and pump fires including possible failures of the oil collection system. Two failure modes of the oil collection system were considered with the likelihoods assigned as: a minor leak with an estimated likelihood of 0.1, and a major oil spill with an estimated likelihood of 0.01. The RCP fire ignition frequency of 6.1E-3/yr was taken from NUREG/CR-6850 (14 percent from electrical fires (8.5E-4/yr) and 86 percent from oil fires (5.2E-3/yr)). The results of the evaluation are represented in Table 19.1-12 of this report.

Table 19.1-12 Sensitivity Study of RCP

RCP Fire Scenario	Consequences	Frequency (1/yr)	CCDP	CDF (1/yr)	% of Fire CDF
Pump Fire	Loss of one pump	6.1E-03	3.6E-08	2.2E-10	0.12%
Pump Oil Fire with a Failure of Lube Oil Collection System (limited leak)	Loss of one SG	5.2E-04	2.1E-07	1.1E-10	0.06%

RCP Fire Scenario	Consequences	Frequency (1/yr)	CCDP	CDF (1/yr)	% of Fire CDF
Pump Oil Fire with a Catastrophic Failure of Lube Oil Collection System (major spill)	Loss of two SGs	5.2E-05	1.1E-06	5.7E-11	0.03%

The applicant did not consider transient combustible fire frequency, stating that it is unlikely that the transient combustibles would be present or stored in containment pressurizer area, given that maintenance activities at-power are not expected there and the area is not on the access paths to the other areas.

The staff further examined the response and found that the estimated conditional core damage probability (CCDP) of 1.1E-6 for the RCP fire scenario of, "Pump Oil Fire with a Catastrophic Failure of Lube Oil Collection System (major spill)," is low compared to the calculated CCDP of 8.7E-5 given an electric motor fire in the containment as described in the responses to RAI 66, Question 19.01-29 and RAI 97, Question 19-223. Thus, in RAI 269, Question 19-327, the applicant was asked to further describe in detail the three RCP fire scenarios analyzed in the response to RAI 227, Question 19-302, and justify why an RCP fire with a major spill would have a lower CCDP compared to an electric motor fire CCDP.

The applicant's response to RAI 269, Question 19-327 was received on September 17, 2009. The response is currently under review. **RAI 269, Question 19-327, which is associated with the above request, is being tracked as an open item.**

The staff found that the FSAR contains insufficient information on the correction factors (e.g., ratios and bases) used to adjust PFA fire frequencies, thus, RAI 66, Question 19.01-30 was issued, requesting that the applicant provide additional information. In an October 9, 2008, response, the applicant described that the three different types of correction factors applied to generic frequencies were derived from RES/OERAB/S02-01 as follows:

- Correction Factor 1 (CF1) is a ratio of the number of analyzed PFAs over the total number of the PFAs in the same location bin in the U.S. EPR.

- Correction Factor 2 (CF2) accounts for the specificity of the U.S. EPR with respect to the existing plants that are used as a database for the generic frequencies in the RES/OERAB/S02-01.

- Correction Factor 3 (CF3) is used to further divide the electrical busses fire ignition frequencies between ac and dc switchgear rooms.

The applicant included Table 19.01-30-1 in its response showing the detailed calculation of the PFA fire ignition frequencies including the values assigned for all correction factors (CF1, CF2, and CF3) and the bases of these values.

Regarding the analyzed PFAs, the staff finds the applicant excluded the EPGBs from the analysis. Thus, the staff issued RAI 66, Question 19.01-31, requesting that the applicant provide an explanation. In an October 9, 2008, response, the applicant stated that the EPGBs are excluded from the fire risk evaluation based on the impact of the plant response, which is limited to a loss of one EDG train. The effects on fire CDF were evaluated to be insignificant.

Using the RES/OERAB/S02-01 EPGB fire frequency of 7E-3/yr, the applicant estimated the probability of losing an EDG due to a fire during the 24-hour mission time to be 2E-5. This value is small compared to EDG non-fire-related unavailability (i.e., EDG failure to start equal to 4.4E-3 and EDG failure to run for 24 hours equal to 2.8E-2) and thus, negligible.

Regarding the transformer yard fire frequency, the staff finds the transformers are the only fire source used in the fire frequency estimate. Thus, in RAI 66, Question 19.01-36, the staff requested the applicant to clarify the transformer yard fire sources and also provide the ratio of transformers in the transformer yard to the total transformers in the plant. In an October 9, 2008, response, the applicant stated that, the detailed design information regarding the transformer yard was not available at the time of the analysis. Transformers were assumed to be the dominant source of fire ignition in the transformer yard; therefore, it was the only source considered. The ratio of transformers in the transformer yard to the total number of transformers was set to one according to NUREG/CR-6850. Each transformer is designed to be separated from the others by fire barriers. The fire scenario only models a fire affecting a transformer feeding the safety divisions. Therefore, a factor of 2/5 was applied to the fire ignition frequency, because two out of five transformers feed the safety divisions.

In an October 9, 2008, response to RAI 66, Question 19.01-37, regarding the potential ignition sources for MFW/MS valve room, the applicant stated that the fire ignition frequency of 6E-4/yr for a single MFW/MS PFA (encompassing two divisions) is estimated using the NUREG/CR-6850 method, based on the number of components in the area. The only components identified in the area susceptible to ignite a fire are electric motors, pumps, and fans. A correction factor of 1.1 is also applied to account for the larger number of pumps. The details of the calculation are shown in Table 19.1-13 of this report. The methodology used to derive the frequency of the fire scenario is similar to the one used for the pressurizer compartment. The total fire ignition frequency for one PFA is multiplied by the number of PFAs (two) and the conditional probability of a spurious actuation. The details of the calculation of the scenario frequency are shown in Table 19.1-14 of this report.

Table 19.1-13 Fire Ignition Frequency for One MFW/MS Valve Room

Ignition Source	Generic Ignition Frequency (/yr)	Factors of the components on the location vs. the total components in the plant	Correction Factor	PFA-Specific Ignition Frequency (/yr)
Electric Motors	4.60E-03	0.040	--	1.8E-04
Pumps	2.10E-02	0.012	1.100	2.9E-04
Ventilation Subsystems	7.40E-03	0.018	--	1.3E-04
			Total	6.0E-4

Table 19.1-14 MFS/MS Fire Scenario Frequency (Fire with at Least One Spurious Opening)

Trains Considered	Total PFA Fire Ignition Frequency (/yr)	Single Hot Short Probability for SOV	Number of Hot Shorts Needed to Open the Train	Number of Trains	Spurious Opening Frequency (/yr)
MSRIV Train	1.2E-03	0.33	2	4	5.2E-04

The staff noted that the U.S. EPR fire PRA inappropriately used RES/OERAB/S02-01 as the basis for developing U.S. EPR fire ignition frequencies. The staff observes that the estimated fire frequencies in the referenced report are based upon data solely from 1993 to 1999. Fire frequencies based only upon this data are too limited, since more years have passed than corresponds to the 1993 to 1999 period to which this data set pertains. The staff determines that the fire ignition frequencies described in NUREG/CR-6850 is more appropriate to support fire PRA development, since NUREG/CR-6850 includes a much more extensive fire event database and supersedes those from other sources. The staff finds that the fire frequencies in RES/OERAB/S02-01 were developed for the reactor oversight purposes and would be inappropriate for use in developing the U.S. EPR fire PRA. Thus, in RAI 97, Question 19-223, the staff requested that the applicant provide further justification for the use of RES/OERAB/S02-01 as the basis for developing fire ignition frequencies and also validate the estimated frequency values.

In a December 12, 2008, response, the applicant stated that the RES/OERAB/S02-01 was selected as a source of fire ignition frequencies, because it limits the uncertainties associated with the amount of information available in the design certification phase in areas such as:

- Structures and equipment locations in the non-Nuclear Island (NI) locations
- Locations for certain equipment in NI locations (cables, junction boxes, lighting panels, radiation panels, etc.)
- Design for electrical switchgears, load centers, motor control centers and panels (vertical sections, number of breaker cubicles, etc.)

Because of the limitations, the applicant believed that the selection of RES/OERAB/S02-01 as a primary fire frequency source was prudent.

To address possible differences between fire frequencies obtained from RES/OERAB/S02-01 and NUREG/CR-6850, the applicant performed a sensitivity study where fire ignition frequencies are derived from NUREG/CR-6850. The distribution of ignition sources between fire areas was estimated based on information available in the design phase. Transient sources were estimated following the method of NUREG/CR-6850, Task 6.

Table 19-223-1 in the applicant's response shows the assumed distribution of ignition sources between the different fire areas and the resulting fire ignition frequencies. This table also compares the results of the NUREG/CR-6850 sensitivity evaluation with the current fire frequencies derived from RES/OERAB/S02-01 for different PFAs and for generic locations. The results of this comparison show that RES/OERAB/S02-01 underestimated the total fire frequency in switchgear rooms, overestimated the frequency for the control room, and gave

comparable frequencies for the Auxiliary Building, Turbine Building, solid waste system (SWS) pumphouse, and battery room. A comparison was not performed for the cable spreading rooms because of the limited amount of information available on cable loads and junction boxes at the design phase. The differences in the switchgear room frequencies are mainly attributed to a high frequency for electrical cabinets fires (4.5E-02/yr) in NUREG/CR-6850.

The results of the fire scenario CDF comparison are presented in Table 19-223-2 of the response.

The staff examined the applicant's response to RAI 97, Question 19-223, and noted that the response contained insufficient information to draw a conclusion about the sensitivity study performed and, thus, the follow-up RAI 227, Question 19-300 was issued, requesting that the applicant provide additional information including:

- The number of each ignition source in each PFA and the total number of items per equipment type in the generic locations that were used to establish the ignition source weighting factor

- The basis for the exclusion of air compressors, dryers, hydrogen tanks/fires from the fire frequency estimate and justification for the impacts of these components on the fire frequency

- Justification for the exclusion of cable fires (including self-ignited cable fires) from the fire frequencies

- Exclusion of cable fire impacts on the fire PRA

- The details on how the weighting factors for ignition frequency bins involving transient combustibles/activities were estimated and distributed

In a July 6, 2009, response, the applicant provided a table showing the elements used to calculate the ignition source weighting factors. The response also described that the hydrogen tanks and fires are included in the fire frequency for the TB, because they are part of the bin "turbine generator hydrogen." This bin was subsumed in the general category "Turbine Building."

The air compressors which supply the plant instrument air are expected to be located in the TB. Since the scope of the air compressor bin is limited to the main instrument air compressors, it was assumed that the frequency of the bin (2.4E-3/yr) could be added to the TB. This would change the fire frequency in PFA-TB from 5.7E-2/yr to 5.9E-2/yr and, likewise, the CDF from that scenario from 6.8E-10/yr to 7.0E-10/yr. Based on the applicant's response, the staff finds that inclusion of the air compressors increases the fire CDF by about 2E-11/yr, which is negligible.

The "dryers" bin in NUREG/CR-6850 corresponds to the clothes dryer, for which design information will be developed later in the design process. The applicant concluded that it is unlikely that these components would be located in any of the areas modeled in the fire PRA. Thus, the impact of their exclusion is found to be insignificant.

Cable fires are not included in the fire analysis, because details of cable routing, which are essential to derive the cable load weighting factors, are not available. Moreover, the U.S. EPR cables will be qualified by the Institute of Electrical and Electronics Engineers (IEEE), and will

therefore not be susceptible to self-ignition. Therefore, the only relevant fire ignition frequency for cables would be the cable fires caused by welding and cutting, which have a frequency of 1.6E-3/yr (Nuclear Auxiliary Building) and 2E-3/yr (plant-wide). The transient ratings for welding and cutting are shown in Table 19-300-3 of the response. Table 19-300-3 shows that all the PFAs have a welding and cutting transient rating of less than five percent, except for the FB, which has a very low contribution to the fire risk. Therefore, the applicant concluded that the impact of excluding cable fires was found to be small. The staff finds that the basis for excluding cable fires is reasonable, consistent with NUREG/CR-6850, and is therefore acceptable.

Transient fire ratings were calculated following the relative ranking approach presented in NUREG/CR-6850, Section 6.7.5.2. Transient fire ignition frequencies were distributed between all the buildings of the plant, not only the ones modeled in the fire PRA. Influence factors such as maintenance, occupancy, and storage were assessed for each fire area described in the fire hazard analysis based on engineering judgment.

The assigned influence factors for each fire area and the resulting transient normalized ratings for each building or group of buildings (SB mechanical areas) are shown in Table 19-300-2 of the response. The normalized transient ratings are the product of the number of buildings in the group times the number of fire areas in each building times the normalized transient rating of each area.

The normalized transient rating for a given PFA was obtained by multiplying the rating of the building by the fraction of the building fire areas that are located in the PFA. The calculation of the normalized transient ratings for each PFA is shown in Table 19-300-3 of the response.

The staff also noted that using either NUREG/CR-6850 main control board fire frequency or RES/OERAB/S02-01 control room fire frequency to represent U.S. EPR control room fire may not be appropriate. The fire ignition frequencies provided in these documents are primarily derived from the existing power plants equipped with analog technology. However, as designed, the U.S. EPR main control room is a compact cockpit-style; a workstation which is entirely driven by digital computers and visual display monitors rather than analog hardware. Thus, the staff issued RAI 227, Question 19-301 requesting that the applicant demonstrate that using MCR ignition frequency of either 2.6E-3/yr of NUREG/CR-6850 or 7.2E-3/yr of RES/OERAB/S02-01 is practical for the U.S. EPR.

In a July 6, 2009, response, the applicant stated that the U.S. EPR fire PRA takes limited credit for the digital nature of the main control room in evaluating the fire ignition frequency. A factor of 0.5 was applied to the RES/OERAB/S02-01 control room fire frequency of 7.2E-3 per year to account for the digital design of the control room, including fiber optic cables which are not susceptible to self-ignition and the presence of computers instead of analog control panels. There is no industry data available regarding the fire ignition frequency for digital control rooms; and the use of existing data for analog control rooms would be conservative. Applying the 0.5 factor allows some credit to be taken for the improvement in fire risk brought by the digital design, while still producing a conservative frequency.

The staff concludes that, although it is not practical to use the fire database of RES/OERAB/S02-01 to support the fire frequencies development, the estimated U.S. EPR fire ignition frequencies including the MCR fire frequency described in the FSAR are acceptable based on the sensitivity study using the NUREG/CR-6850 fire frequency method, which results in a total fire CDF increase of about only five percent. For a future validation of the U.S. EPR

fire ignition frequencies, the applicant will add the following assumption to the FSAR Tier 2, Table 19.1-109:

> It is assumed that when the final number of fire ignition sources is known for each PRA fire area, the conclusion that fire ignition frequencies obtained using RES/OERAB/S02-01 are comparable to those obtained by using NUREG/CR-6850 will remain valid.

Inclusion of the above assumption, which is associated with RAI 227, Question 19-301, is being tracked as a Confirmatory Item 19-301.

19.1.4.6.3.2 *Fire Scenarios*

To estimate the internal fire risk, the applicant defined the worst fire scenarios, one for each selected area. In all but one case (containment pressurizer area), a fire in a PFA was assumed to disable all components located within that area. The PFAs were further grouped by selecting one PFA as representative of multiple symmetrical PFAs.

Where applicable, the applicant considered spurious actuation of systems caused by simultaneous electrical hot shorts. The applied probability of a hot short, given a fire, is 0.17 for an MOV and 0.33 for an SOV as described in NUREG/CR-6850.

Automatic fire suppression was credited when available and if not affected by the fire. Two 100 percent capacity diesel engine-driven fire pumps are installed to ensure that suppression could be credited even if a consequential LOOP occurs. Manual suppression was credited only in the MCR, because it is constantly manned.

Fire scenarios were quantified using the same fault tree and event tree logics used in the Level 1 internal events PRA. Mitigating systems that had been assumed to be unavailable in a fire scenario were not credited. The 15 fire scenarios selected in the internal fires PRA are defined in FSAR Tier 2, Table 19.1-64. This table includes (1) fire scenario identifier and description, (2) the effects on mitigating systems, (3) the suppression credited, and (4) the scenario frequency and its basis.

In an October 9, 2008, response to RAI 66, Question 19.01-18 regarding the method used to examine and modify the internal events PRA HEPs to account for the potential impacts of fire events, the applicant stated that the HEPs were doubled for the fire scenario modeling the MCR fire to account for the stress associated with the MCR fire and the MCR evacuation, potential impacts from smoke and heat, limited equipment/indication availability, and possible communications difficulties. The HEP adjustments were based on a doubling of the stress-related PSF. HEPs for the fire scenario outside the MCR were not changed. The impact of the fires outside of the MCR on the operator performance was not evaluated as being significant enough to change HEP values based on the following considerations:

- All operator actions credited in these fire scenarios are performed from the MCR; no local actions are credited.
- Equipment/indication losses are not significant for these scenarios.
- Fire induced stress and communications difficulties for the fires outside of the MCR are considered to be limited.

- The impact of the fires outside of the MCR on the smoke and heat in the MCR or the availability of lighting is not considered likely.

To assess the impact of HEP on the fire CDF, the applicant performed a sensitivity study as summarized below:

- Fire CDF (base case) = 1.8E-7/yr
- Fire CDF (sensitivity case: all HEPs set to 95th percentile) = 4.7E-7/yr
- Increase = 168 percent

Compared to similar results for the internal events, where the corresponding increase is 257 percent, the fire scenarios are slightly less sensitive to the HEP values.

In an October 9, 2008, response to RAI 66, Question 19.01-19, regarding the selection of conditional fire event tree used to quantify the fire CDF, the applicant indicated that the choice of an event tree (ET) to represent a specific fire scenario was based on the similarity in the expected plant response. In general, fire scenarios resulting in a specific plant response (i.e., general transient, LBOP, LOCCW, LOCA, spurious opening of an MSSV) were quantified using the appropriate ET, with additional mitigating system unavailabilities. Table 19.1-15 of this report indicates the corresponding fire scenarios and ETs, as well as the fire-induced unavailable system for each scenario.

Table 19.1-15 Event Trees Used to Quantify Fire Scenarios

Fire Scenario	Description	Event Tree	Effects on Mitigating Systems
Fire-SB14-AC	Fire in Switchgear Room of Safeguard Building 4 (or 1)	31BDA (Loss of divisional AC)	All class 1E and non-class 1E AC Buses in SB4 unavailable.
Fire-SB23-AC	Fire in Switchgear Room of Safeguard Building 2 (or 3)	31BDA	All class 1E and non-class 1E AC Buses in SB2 unavailable.
Fire-SB14-DC	Fire in the DC Cabinets Room of Safeguard Building 4 (or 1) - I&C rooms included	31BDA	All class 1E and non-class 1E DC and I&C Buses in SB4 unavailable.
Fire-SB23-DC	Fire in the DC Cabinets Room of Safeguard Building 2 (or 3) - I&C rooms included	31BDA	All class 1E and non-class 1E DC and I&C Buses in SB2 unavailable.
Fire-SB-MECH	Fire in the Pump Room of any Safeguard Building	31BDA	EFW4, CCWS4, CCWS CH2, MHSI4, LHSI4, SAHR unavailable
Fire-MS-VR	Fire on the top of SB 4 (or 1), in the MFW/MS valve	MSSV (Spurious	Spurious opening of MSRT on SG4, an increase in the

Fire Scenario	Description	Event Tree	Effects on Mitigating Systems
	room	opening of a main steam safety valve)	probability of MS isolation failure on SG4 and SG3
Fire-FB	Fire in the Fuel Building	GT (General Transient)	CVCS trains 1 and 2 and EBS trains 1 and 2 unavailable
Fire-TB	Fire in the Turbine Building	LBOP (Loss of Balance of Plant)	MFW and SSS unavailable
Fire-SWGR	Fire in the Switchgear Building	LBOP	SBODGs, 12-hour and 2-hour batteries, and all non-class 1E buses unavailable
Fire-BATT	Fire in one of the 4 Battery Rooms	31BDA	2-hr Battery Div 4 unavailable
Fire-ESW	Fire in the Essential Service Water Building	LOCCW (Loss of Component Cooling Water)	UHS4 unavailable.
Fire-xFYard	Fire in the transformer yard	GT	Loss of one class 1E transformer.
Fire-CSR	Fire in the Cable Floor (Room under the MCR)	31BDA	All Div 4 control power unavailable
Fire-MCR	Fire in the Main Control Room	Dedicated event tree transferring to LBOP	Failure to transfer to RSS results in core damage; success transfers to the LBOP event tree with all HEPs doubled
Fire-PZR	Fire in the pressurizer compartment	SLOCA	Primary bleed unavailable

The staff noted that the U.S. EPR fire PRA does not address whether damages due to a fire to cables routed through a specific fire area would have any impact on components located outside of that area. Thus, the staff issued RAI 66, Question 19.01-20 requesting that the applicant clarify this area. In an October 9, 2008, response, the applicant stated that, based on the basic concepts of cable routing, the fire scenarios were defined such that damage to cables routed through a specific PFA would either have no impact on components located outside of the PFA, or the cable damage was implicitly modeled in the fire scenario.

Regarding the modeling of electrical hot shorts, the staff issued RAI 66, Question 19.01-24, asking the applicant how the hot shorts were analyzed in the fire PRA given limited information available on cable routing during the design phase. In an October 9, 2008, response, the applicant stated that, for each fire in the selected fire area, it was assumed that all equipment

located in the area and all the cable routed through the area are failed. An analysis of hot shorts would not affect the conservatism of this analysis. Hot shorts are only identified and analyzed for two areas: a spurious opening of an MSRT by a fire in the MFW/MS valve room and a spurious opening of a PSRV or SADV train by a fire in the containment pressurizer area. The conditional probabilities of hot shorts for a motor-operated valve and for a solenoid-operated valve were obtained from NUREG/CR-6850, Appendix J. Spurious system actuation was not analyzed for the fires in the MCR, because the fiber optic cables in this area are not considered susceptible to hot shorts.

In RAI 66, Question 19.01-44, the staff asked that the applicant describe whether any credit was given for fire-induced LOOP recovery. In an October 9, 2008, response, the applicant stated that, in the U.S. EPR fire risk evaluation, no fires were identified that could lead to a LOOP. Transformer yard fires, based on the fire barriers, are not likely to include multiple transformers. For the fire-induced consequential LOOP, recovery within one hour was credited. It was assumed that consequential LOOPs after fire events are recoverable similar to the other consequential LOOPs, because, although they occur due to a fire-related trip or controlled shutdown, they are not directly caused by equipment that has been damaged by fire.

The staff finds that the applicant clearly described the potential fire-induced LOOP recovery in its response and, therefore, the response is acceptable. The staff also finds that the FSAR contained insufficient information on the control room fire analysis. Therefore, in RAI 66, Question 19.01-34, the staff asked the applicant to provide the following information:

- The basis for control room evacuation of 90 minutes given a fire
- Operator actions/procedures required for transferring control of the plant to the RSS (e.g., timing, location of transfer switch, etc.)
- Systems/functions that could be controlled from the RSS
- Random failure probability of RSS given a successful transfer
- The basis for operator failure probability of 7E-5

In an October 9, 2008, response, the applicant provided the following information. Regarding the basis for control room evacuation of 90 minutes given a fire, the applicant stated:

> The SPAR-H methodology, which was used to calculate the HEP for transfer of control to the RSS, relies on estimates of the time available and the time needed for the operator action. The time available parameter, 90 minutes, is a representative time based on the estimated time from the start of the MCR fire until the undesired consequence (core damage) is irreversible.
>
> A fire in the MCR is assumed to cause an event similar to a LBOP, which is modeled in the PRA as a turbine trip with unavailability of the main condenser, MFW, SSS, closed cycle cooling water, and conventional service water.
>
> The time available for this operator action is based on the representative time window available for operator action during a loss of all feedwater transient. For an event involving total loss of secondary side cooling, representative MAAP runs indicate that core damage can be prevented if operator action to restore cooling is

taken within 90 minutes. This is conservative, because the MCR fire will not impact performance of the protection system or automatic actuation of EFWS.

Regarding operator actions/procedures required for transferring control of the plant to the RSS, the applicant stated:

> The design features for the transfer of control of the plant to the RSS have not been finalized; therefore, specific actions/procedures required for transferring control of the plant to the RSS have not been developed. However, requirements for the transfer have been defined such that:
>
> - The transfer must be in a different fire area than the MCR and within close walking distance from the MCR.
> - The transfer must disable the MCR control and provide a seamless transfer to the RSS controls.

Further, in a July 21, 2009, response to the follow-up question (RAI 252, Question 19-314), the applicant agreed to include the above requirements on transferring control of the plant to the remote shutdown station in Item 17 of FSAR Tier 2, Table 19.1-102. **Inclusion of the above, which is associated with RAI 252, Question 19-314, is being tracked as Confirmatory Item 19-314.**

Regarding systems/functions that could be controlled from the RSS, the applicant stated:

> The RSS is able to control all the systems and functions necessary to bring the plant to and maintain it in a safe shutdown state through a combination of the PICS and SICS.
>
> The RSS includes two fully functional PICS workstations. The PICS in the RSS will have a different number of workstations and monitors than in the MCR; however, their functionality will be the same as the MCR workstations. This enables all plant systems and functions to be controlled from the RSS.
>
> In addition, the RSS will have a SICS workstation that provides a manual reactor trip and a minimum inventory of controls, displays, and alarms for manual control of systems to achieve and maintain safe shutdown.

Regarding random failure probability of RSS given a successful transfer, the applicant stated:

> The designs of the RSS and of the RSS transfer require divisional independence to be maintained, such that an electrical failure in one safety division can not impact another safety division. Physical independence and electrical isolation is also required in the RSS between safety-related systems and non-safety-related systems. Therefore, a complete random failure of the RSS is unlikely, and is not included in the PRA.

The staff finds that with the completely redundant design of RSS described in the response, the random failure probability of the RSS is low and can be excluded from the PRA model.

Regarding the basis for operator failure probability of 7E-5, the applicant stated:

> The HEP associated with control room evacuation includes the decision to evacuate the MCR and the action of switching controls to the RSS. The egress route from the MCR to the RSS is a short walk that is protected with fire barriers, emergency lighting, smoke confinement system, and positive differential air pressure. The HRA assumes 15 minutes to perform the evacuation and transfer control to the RSS. In the case of successful transfer, the PRA transfers to the LBOP event tree. If additional operator actions are needed after the transfer (e.g., to restore cooling), then the HEPs for the subsequent operator actions (performed from the RSS) are doubled.
>
> The operator failure probability for RSS transfer has been assessed using the SPAR-H human reliability methodology (NUREG/CR-6883). This results in a failure probability of 2E-5 for the cognitive portion and a failure probability of 5E-5 for the execution portion. Therefore, the total HEP is 7E-5.

Additionally, in a July 21, 2009, response to RAI 252, Question 19-315, regarding the credits taken for reducing MCR evacuation HEP, the applicant performed a sensitivity analysis to quantitatively calculate the impact on the HEP estimate. This sensitivity case resulted in a CDF of 6.2E-9/year by increasing the HEP to 2E-3. Based on the sensitivity performed, the staff finds that using 7E-5 for MCR evacuation HEP would have a small impact on the total Fire CDF. In addition, the applicant committed that based on the PRA assumption of a 15-minute median time to complete the action (MCR evacuation and RSS transfer), the following assumption will be added to the FSAR Tier 2, Table 19.1-109, Item 74 to support this HEP:

> It is assumed that the time needed to transfer control from the MCR to the RSS will be approximately 15 minutes or less and that there will be a procedure for MCR evacuation, which will contain clear abandonment criteria and instructions for transfer of control to the RSS.

Inclusion of the above assumption in the FSAR, which is associated with RAI 252, Question 19-315, is being tracked as Confirmatory Item 19-315.

The staff recognizes that this HEP represents a potential risk-significant operator action; however, because the applicant will be tracking this operator action in accordance with the HRA/HFE integration plan described in the FSAR Tier 2, Section 18.6 as stated in its response, the staff finds it acceptable.

The staff reviewed the U.S. EPR fire scenarios and related information provided in the applicant's responses to RAIs, and concludes that the applicant has appropriately identified and analyzed all important fire scenarios, except for the RCP fire scenario. As mentioned in Section 19.1.4.6.3.1 of this report, in RAI 269, Question 19-327, the applicant was requested to justify why an RCP fire with a major spill would have a lower CCDP compared to an electric motor fire CCDP. The response is currently being reviewed by the staff and is being tracked as an open item.

19.1.4.6.3.3 *Results from the Internal Fire Risk Evaluation*

The total point estimate CDF from internal fire events was calculated to be 1.8E-7/yr. This value is well below the NRC goal of 1E-4/yr as described in SECY-90-016, and is therefore acceptable.

Significant Initiating Events

All fire scenarios/initiating events modeled and their contributions to the internal fire CDF are given in FSAR Tier 2, Table 19.1-65. As shown in this table, 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 due to the importance of electrical Divisions 1 and 4 for the supply of front-line and support systems. 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. 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 SWGR Building. The fire in the SWGR Building has effects comparable to an LBOP initiating event with a loss of non-safety electrical power and SBO DGs. Its relatively high risk is caused 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.

Significant Sequences and Cutsets

The applicant identified two fire-specific failure patterns as follows:

1. A fire in SB 1 could result in a failure of the CCWS CH 1. The fire disables the Division 1 running CCWS train and the corresponding switchover valves, thereby disabling a switchover to the CCWS 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. 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 CCWS 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 significant cutsets for the internal fires are shown in FSAR Tier 2, Table 19.1-66. In this table, the first 100 cutsets are organized into 12 groups based on the associated initiating events and on their similar impact on mitigating systems. The corresponding sequence in the ET is provided for each group. The top 100 cutsets represent over 76 percent of the total fire CDF.

In the top 100 cutsets, two cutsets (fires in the MFW/MS valve room and the MCR) dominate the fire risk, with individual contributions of about 15 percent to the fire CDF. 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 2,300.

Significant SSCs, Operator Actions and Common Cause Events

FSAR Tier 2, Table 19.1-67 through Table 19.1-73 show the important contributors to the internal CDF based on the FV importance measure (FV greater than or equal to 0.005), or the RAW importance measure (RAW greater than or equal to 2).

FSAR Tier 2, Table 19.1-67 shows the top risk-significant SSCs 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.

FSAR Tier 2, Table 19.1-68 shows the top risk-significant SSCs 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.

FSAR Tier 2, Table 19.1-69 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.

FSAR Tier 2, Table 19.1-70 shows the risk-significant human actions based on the RAW importance measure. Only four operator actions are considered important based on their RAW value: (1) Transfer to the RSS following an MCR fire, (2) Operator failure to initiate RHR cooling in four hours, (3) Operator failure to recover room cooling locally, and (4) Operator failure to initiate a feed and bleed for transient events.

FSAR Tier 2, Table 19.1-71 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.

FSAR Tier 2, Table 19.1-72 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.

FSAR Tier 2, Table 19.1-73 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. 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.

19.1.4.6.3.4 *Key Assumptions*

The key assumptions related to the modeling of fire events are summarized below:

- It is assumed that a fire in any fire area or building will fail all equipment at this location.
- 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 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.

- 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).

In an October 9, 2008, response to RAI 66, Question 19.01-22, regarding the probabilities of 0.1 and 0.5 assigned to main steam isolation failures, the applicant stated that, in the MFW/MS valve room fire scenario, all valves in the room (including the MSIVs) were assumed to be affected. The probabilities of 0.1 and 0.5 represent the probability of a specific failure mode of fail open. The fire scenario assumes the spurious opening of an MSRIV. The consequences of a spurious opening of an MSRIV are greater if additional SGs are not isolated, which would occur if the associated MSIVs fail to close. Given a fire that causes a spurious opening of an MSRIV in Division 4, the conditional probabilities that the Division 4 and Division 3 MSIVs (located on top of the same SB) will fail open are estimated to be 0.5 for the nearest Division 4 MSIV and 0.1 for Division 3 MSIV, which is separated by a wall.

In a November 5, 2008, response to RAI 66, Question 19.01-39, regarding the assumptions on the cable spreading room (CSR) and CSR separation measures, the applicant stated that the separation measures for the cable floor, which is referred to as the CSR, are addressed in the FSAR Tier 2, Section 9.5.1.2, with revisions as presented in the response to RAI 20, Question 09.05.01-22:

> The cables to the MCR are routed through the cable floor. The cable floor is a separate fire area from the MCR assigned to Division 2 of the Safeguard Buildings. Safety-related cables from each of the other three divisions (1, 3, and 4) are routed from the cable floor to the MCR sub-floor area in the MCR via separate non-combustible cable ducts, having a minimum fire resistance rating of three hours.

In addition, there is physical separation between Class 1E and Non-Class 1E cables. Criteria for cable separation are addressed in the FSAR Tier 2, Section 8.3.1.1.9. Incorporation of feedback from non-safety-related cable routing, and updates to the PRA, are performed in accordance with the PRA maintenance and upgrade process described in FSAR Tier 2, Section 19.1.2.4.

The staff reviewed the FSAR and the applicant's responses to the RAIs and finds that the assumptions specific for the U.S. EPR fire PRA were developed consistent with the U.S. EPR design and NUREG/CR-6850. COL Information Item 19.1-9 calls for a review of as-designed and as-built information to confirm that the assumptions used in the PRA remain valid. The COL applicant must confirm the validity of the key assumptions associated with the PRA and the plant-specific PRA must be updated to account for site-specific design information and design changes or departures from the certified design in accordance with 10 CFR 52.79(d)(2).

19.1.4.6.3.5 *Sensitivity Analysis*

The applicant performed a series of sensitivity studies to evaluate the impact of the PRA modeling assumptions on the fire CDF, including the assumptions related to the internal fires analysis. The results are shown in FSAR Tier 2, Table 19.1-74. Several insights were drawn from the sensitivity cases analyzed as follows:

- The fire CDF is less sensitive compared to most parameters that impact internal events CDF, such as common cause events grouping or assumptions on LOOP recoveries and diesel generator (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 slightly less for fire events than for internal events CDF. The fire CDF shows a higher sensitivity to assumptions on the seal LOCA probability and the volume control tank (VCT) unavailability. 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.

- 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 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 also has a high importance value in the internal fire risk.

- The fire CDF is found to be sensitive to an assumption of a fire affecting both an MSRT and an MSIV.

- The modeling assumption of a complete separation of the safety and non-safety divisions in the CSR is found to have a high impact on the fire CDF.

- The fire CDF is also sensitive to the HVAC recovery due to interdivision ventilation dependencies. A large number of the modeled fire scenarios result in the unavailability of one safety division, thus a total loss of an electrical division which supplies the running CCWS pump could, without operator intervention, disable the second division through a loss of HVAC.

Based on the sensitivity studies performed by the applicant, subsequent identification of the most risk-significant systems, components, and operator actions, during a fire event, the staff concludes that the applicant has appropriately identified the insights in accordance with the guidance provided in the SRP.

19.1.4.6.3.6 *Uncertainty Analysis*

The applicant quantified uncertainty on the Level 1 Fire PRA results using a process similar to that described for internal events. Parametric uncertainty was represented by selecting an uncertainty distribution for each parameter type including fire initiating events.

The results of the uncertainty evaluation for the Level 1 fire events CDF are presented in FSAR Tier 2, Figure 19.1-18 and summarized below:

- CDF Internal Fire Events mean value = 2.1E-7/yr
- CDF Internal Fire Events 5 percent value = 9.5E-9/yr
- CDF Internal Fire Events 95 percent value = 7.0E-7/yr

As seen above, the 95th percentile CDF value is more than two orders of magnitude below the NRC goal of 1E-04/yr. Therefore, the staff finds it acceptable.

19.1.4.6.3.7 *Fire PRA Insights*

The applicant identified several fire PRA insights as summarized below. The two dominating cutsets, namely, Fires in the MFW/MS Valve room and MCR, 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 CCWS.

RCP 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 SSCs are risk-significant based on their FV, but none of them dominates. The safety significance of components to the internal fires risk is equally distributed among systems and plant functions, thus no obvious vulnerability in the U.S. EPR design with respect to the mitigation of the credible fire scenarios.

Based on the information described in the FSAR as summarized above, the staff concludes that the applicant has provided an adequate description of the design-specific fire PRA, as well as its results including uncertainty and sensitivity studies, sufficient for the staff to obtain risk insights about the U.S. EPR design as described in the SRP.

19.1.4.6.3.8 *Level 2 Fire Analysis*

As described above, the applicant developed conservative fire accident scenarios by assuming that fires could engulf the entire fire area, leading to the failure of all SSCs in the fire area, and that the total area fire ignition frequency is applied to that scenario. No fire-damage models and associated computer codes were used, since all equipment inside a fire area is assumed to fail. A key Level 2 PRA assumption was that a fire in the main control room with operator failure to evacuate fails all Level 2 operator actions that may be required in the early stages of the severe accident.

Fire scenarios were quantified using the same fault tree and event tree logic used in the internal events evaluation. Approximately 80 percent of the LRF for fire events are early containment failures by hydrogen flame acceleration induced containment rupture (Release Categories RC303 and RC304 containment failure before vessel failure). About 17 percent are TI-SGTRs (RC702). Sequences involving consequential seal LOCAs are significant (over 50 percent) LRF contributors.

The applicant assessed the sensitivity of the results to the phenomenological events by considering what the impact on the results, in terms of LRF, would be if the phenomena either would surely occur, or would surely not occur. It was determined that fire LRF results are sensitive to the value of basic events related to flame acceleration loads and in-vessel steam explosions. The events were assessed by the applicant as having a very low probability of occurrence; increasing the probability to unity (a physically unreasonable assumption) resulted in an estimate of a very large increase in the LRF.

The calculated LRF values for internal fire events are listed below in Table 19.1-16.

Table 19.1-16 Metric Results for Level 2 Internal Fire Events

		Quantile		
Risk Metric	**Point Estimate**	**Mean**	**5th percentile**	**95th percentile**
LRF	3.6E-9/yr	3.8E-9/yr	3.6E-13/yr	3.3E-9/yr
CCFP	0.02	0.018		

The results for LRF for internal fire events are dominated by severe accident phenomenological events. The specific issue 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.

The significant contribution of temperature-induced SGTR to the fire LRF is partly due to the high contribution of seal LOCAs to the fire CDF. Core damage following a seal LOCA [1.52 cm (0.6 in.) or 5.08 cm (2 in.) equivalent LOCA] is a dominant precursor of high-temperature-induced SGTR.

Temperature-induced steam generator tube rupture sequences (RC702) play a significant role in LRF for fire events. Sensitivity studies found that LRF did not significantly increase due to this failure mode even in the bounding case of assumed concurrent unavailability of the feedwater and the depressurization functions.

19.1.4.6.3.9 *Uses of EPR Internal Fire PRA in the Design Process*

The applicant indicated that the results of the fire PRA were not used explicitly in the fire protection analysis. No fire protection features in RG 1.189, "Fire Protection for Nuclear Power Plants, October 2009," were eliminated as a result of the fire PRA, and no fire protection features were added as a result of the fire PRA. No potential weaknesses and vulnerabilities were identified that might be considered for additional fire protection features.

19.1.4.6.3.10 *Staff Evaluation*

Based on its review, the staff concludes that the design-specific fire PRA developed by the applicant provides the insights needed to determine whether fire vulnerabilities exist for the U.S. EPR design. The applicant's responses to the staff's RAIs are reasonable and acceptable, with an exception of the response to RAI 269, Question 19-327, on the estimate of RCP fire CCDP, which is under review. The applicant has provided an adequate description of the fire PRA, as well as its results, sufficient for the staff to obtain fire risk insights in conformance with

the SRP. The calculated fire CDF of 1.8E-7/yr is well below the NRC goal of 1E-4/yr as described in SECY-90-016. The applicant has sufficiently evaluated uncertainties in the fire PRA, in part by performing sensitivity studies, and identified important equipment and operator actions, as well as other internal fire related insights.

The staff confirmed the U.S. EPR was designed with high levels of redundancy and separation of safety divisions to provide inherent protection against internal fire hazards. The design includes four-train redundancy, location of safety trains in separate buildings, and separation and fire barriers between divisions of control and power cables. This reflects a qualitative and quantitative reduction of internal fire risk compared to operating plants.

The staff also finds that based on the applicant's risk importance studies, the contributions of mitigating SSCs to the internal fires are evenly distributed, thus there are no specific dominant vulnerabilities in the U.S. EPR design with respect to the mitigation of the fire events.

19.1.4.6.4 FSAR Tier 2, Section 19.1.5.4: Other Externals Risk Evaluation

The applicant did not develop a PRA for external events, but instead performed a qualitative screening analysis to assess the risk impacts of high wind, tornado, external flooding, and external fire. The risks resulted from other external events such as aircraft impact, transportation accident, dam failure, hurricane, tsunami, lightning, turbine generated missile, etc., are not addressed in the FSAR Chapter 19. These external events are considered as site-specific events and, thus, the applicant chose not to evaluate such external events at the design certification stage.

The applicant included COL Information Item 19.1-7 in FSAR Tier 2, Table 1.8-2 to ensure that the risk impacts from the external events will be re-evaluated and addressed by the COL applicants. COL Information Item 19.1-7 states that, "A COL applicant that references the U.S. EPR design certification will perform the site-specific screening analysis and the site specific risk analysis for external events applicable to their site."

19.1.4.6.4.1 *High Winds and Tornado Risk Evaluation*

All U.S. EPR Seismic Category I structures housing safety-related equipment were designed to meet the standards for high winds and tornadoes. The U.S. EPR Seismic Category I structures were designed to withstand a high wind speed of 233.35 km/h (145 mph). In addition, these structures were designed to meet the design-basis tornado wind characteristics of Tornado Intensity Region 1 as characterized by a maximum tornado wind speed of 370.15 km/h (230 mph) [296.12 km/h (184 mph) maximum rotational speed, 72.42 km/h (46 mph) maximum translational speed]. These structures were also designed to the design-basis tornado missile characteristics specified in Section 3.5.1.4 of NUREG-0800. The U.S. EPR Seismic Category I structures include:

- RB and RB annulus
- SBs
- EPGBs
- ESWS pump structures

- ESWS cooling water structures
- FB

The most limiting impact from a tornado or high wind would likely be a LOOP. Because the U.S. EPR has a robust design with four independent EDGs providing power to the safety buses and two SBO diesels to back up the EDGs, and because the EDG buildings are designed as Seismic Category I structures and based on the risk assessment of LOOP events described in the internal events PRA, the staff determines that the conditional risk associated with tornado/wind-induced LOOP is not significant.

The staff finds that, with the high winds and tornado structural design features in combination with onsite power supplies, the risk from high wind and tornado is not significant. Since the U.S. EPR is designed to handle tornadoes and is already analyzed for LOOP events, the staff does not consider it necessary to analyze design-basis tornados and high winds probabilistically.

19.1.4.6.4.2 *External Flooding Evaluation*

FSAR Tier 2, Section 19.1.5.4.2 indicates that the safety-related systems and components housed in the Seismic Category 1 buildings are also protected from external floods and groundwater by the flood protection measures provided in FSAR Tier 2, Sections 2.4 and 3.4. These protection measures are evaluated as part of the staff's review of FSAR Tier 2, Sections 2 and 3. The protection measures are identified as follows:

- Structures and penetrations are designed to withstand the buoyancy loads and hydrostatic pressure loads.
- Portions of the buildings located below grade elevation are protected from external flooding by water stops and water proofing.
- All exterior wall and 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.
- Roofs of the buildings are designed to prevent the undesirable buildup of standing water.
- Roofs are designed to withstand a rainfall rate up to 49.28 cm per hour (19.4 in. per hour).
- The design static roof load for rain, snow, and ice is 4.788 kPa (100 lb/sq ft).

The staff agrees with the applicant's conclusion that with the flood protection measures embedded in the U.S. EPR design and in combination with the U.S. EPR as described in FSAR Tier 2, Section 2.4 for building location relative to the probable maximum flood and maximum groundwater elevation, the risk from external flooding events is not significant. In addition, Section 2.4.3 of the FSAR states that "[a] COL applicant that references the U.S. EPR design certification will provide site specific information to describe the probable maximum flood of streams and rivers and the effect of flooding on the design."

19.1.4.6.4.3 *External Fire Evaluation*

FSAR Tier 2, Section 19.1.5.4.3 states that the structural design of safety-related structures, the physical arrangement of safety-related structures, and the cleared zones surrounding plant structures would provide significant protection from 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). The CRE is designed to have isolation capability in the event of external fire/smoke. The CRACS is designed to maintain a positive pressure to prevent uncontrolled/unfiltered leakage. The CRACS can support occupancy for 8 people for 70 hours without outside makeup air. In addition, portable self-contained breathing apparatuses are available for use by the control room operators.

The staff agrees with the applicant's conclusion that with the described external fire design features above and in combination with the U.S. EPR as described in FSAR Tier 2, Chapter 3 for structural design, the risk from external fire and smoke events is not significant.

19.1.4.6.4.4 *Staff Evaluation*

The staff reviewed FSAR Tier 2, Section 19.1.5.4, and finds that the U.S. EPR has a robust design to cope with the tornado, high wind, external flooding, and external fire events. Based on the information provided in the FSAR, the staff concludes that the applicant has appropriately addressed the potential impacts of external events on plant risk, in conformance with the SRP.

19.1.4.7 *FSAR Tier 2, Section 19.1.6: Safety Insights from the PRA for Other Modes of Operation*

19.1.4.7.1 FSAR Tier 2, Section 19.1.6.1: Level 1 PRA for Other Modes of Operation

The information in FSAR Tier 2, Section 19.1.6.1 relates to the following regulatory requirement:

> 10 CFR 52.47(a)(27): Provide a description of the design-specific PRA and its results.

In addition, this information relates to four acceptance criteria from SRP Section 19.0, as summarized below.

- The staff should ensure that the applicant has used the PRA results and insights, including those from uncertainty analyses, importance analyses, and sensitivity studies, in an integrated fashion to identify and establish specifications and performance objectives for the design, construction, testing, inspection, and operation of the plant. Specifically, PRA results and insights are input to ITAAC; TS; RAP; and COL action items.

- For designs that have evolved from the technology of currently operating plants, the results of the PRA should indicate that the design represents a reduction in risk compared to operating plants. The staff should perform a broad (qualitative and quantitative) comparison of risks by initiating event category between the proposed design and operating plant designs to identify the major design features that contribute to the lower risk of the proposed design compared to existing designs.

- The staff should consider the impact of data uncertainties on the risk estimates. In addition, the staff should review the applicant's risk importance studies to obtain insights about the systems, components, and human actions that contribute the most in achieving the low risk level assessed in the PRA, as well as the failures that contribute the most to the assessed risk. The staff should also review the applicant's sensitivity studies performed to determine (1) the sensitivity of the estimated risk to potential biases in numerical values, (2) the impact of the lack of detail, and (3) the sensitivity of the estimated risk to previously raised issues.

- The staff should confirm that the assumptions made in the applicant's PRA during design development and certification, in which a specific site may not have been identified or all aspects of the design may not have been fully developed, are identified in the design certification application such that they can be addressed by the COL application.

19.1.4.7.1.1 *Description of PRA and its Results*

According to 10 CFR 52.47(a)(27), design certification applications must include a description of the design-specific PRA and its results. As discussed above in Section 19.1.4.4.2, this requirement is intended to be a qualitative description of insights and uses, as well as some quantitative PRA results, such that the staff can perform the review, ensure risk insights were factored into the design, and make the evaluation findings described in the SRP.

For the Level 1 shutdown PRA, this regulatory requirement has been satisfied by the description of the PRA methodology and results presented in FSAR Tier 2, Sections 19.1.6.1 and 19.1.6.2, tables providing information on initiating events, cutsets, importance measures, and sensitivity studies; and figures presenting calculations of the time until level reaches the top of active fuel (TAF), initiating event and plant operating state (POS) contributions, and uncertainty results. A summary of this information is provided in the following sections.

The quality of the PRA development process was discussed above in Section 19.1.4.2; the discussion of the other acceptance criteria in following sections addresses specific details of the PRA.

19.1.4.7.1.2 *Methodology and Approach*

Section 19.1.6.1, "Description of the Low-Power and Shutdown Operations PRA," of the FSAR provides a detailed description of the applicant's approach to developing the LPSD PRA. The methodology includes defining POS, identifying the initiating events, analyzing the accident sequences, modeling the plant systems, performing an HRA, and quantifying the full model.

POS Definition. The applicant defined multiple POSs based on three key characteristics of LPSD operation: RCS level, RCS integrity, and number of RHRS trains available. Additionally, as shown in Table 19.1-17 of this report, the states can be differentiated by operating mode, RCS temperature and pressure, and the number of SGs available for heat removal. Although the table does not show it, the C and D POS are separated into "d" (shutting down, before refueling) and "u" (starting up, after refueling) sub-states. This separation reflects the different decay heat levels as a function of time after the reactor trip, as well as the new fuel added during refueling.

Table 19.1-17 Plant Operating States Used in LPSD PRA (Shutting Down)

POS	A	B	CA1	CA2	CA3	CB	D	E	F
Start Time (hr)	N/A	N/A	8			44	92	104	344
Decay Heat (MW)	N/A	N/A	37.2			23.7	20.4	17.3	17.3
TS Mode(s)	1 and 2	3 and 4	4	4 and 5	5	5	6	6	6 (core offload)
RCS Temperature	nominal	nominal to 120 °C (248 °F)	120 °C to 100 °C (248 °F to 212 °F)	100 °C to 55 °C (212 °F to 131 °F)	55 °C (131 °F)	55 °C (131 °F)	55 °C (131 °F)	55 °C (131 °F)	N/A
RCS Pressure	nominal	nominal to 3.17 MPa (460 psia)	3.17 MPa to 2.62 MPa (460 psia to 380 psia)	2.62 MPa (380 psia)	2.62 MPa to 103.4 kPa (380 psia to 15 psia)	103.4 kPa (15 psia)	103.4 kPa (15 psia)	103.4 kPa (15 psia)	N/A
RCS Level	normal	normal	normal	press-urizer 90% to solid	press-urizer solid	mid-loop	mid-loop	cavity flooded	N/A
RCS Integrity	closed	closed	closed	closed	closed (press-urizer degas line open)	vent to nitrogen system (degas line open)	head off	head off	N/A
RHRS Trains Operating	N/A	N/A	2/4	4/4	4/4	4/4	4/4	¾	N/A
SGs Available	4/4	4/4	4/4	2/4	2/4	2/4	0	0	N/A
Containment Status	closed	closed	open	open	open	open	closed	open	open

POS A corresponds to the at-power condition already modeled in detail. POS B is also considered to be addressed by the at-power model, because the plant configuration required by TS in MODE 3 is similar (all SGs are required to be operable when the control rods are

energized; also, safety injection on low pressurizer pressure or low saturation pressure (P_{sat}) is required by TS). In the at-power model, the initiating event frequencies assume the plant is operating at power all year. Therefore, the staff finds it acceptable to assume POS A and B are bounded by the at-power model.

POS CA represents hot and cold shutdown (TS MODES 4 and 5) when there is level in the pressurizer, with cooling by RHRS. The sub-states within CA are modeled as a single state with the characteristics of CA_2. In RAI 2, Question 19-23, the staff requested further justification of this modeling. In an April 30, 2008, response, the applicant asserted that the differences between CA_2 and the other two states are not judged significant. Specifically, the applicant stated that CA_{d2} conservatively envelopes CA_{d3} conditions. RCS temperature and pressure are higher in CA_2 than in CA_3, while the other conditions are the same. However, CA_{d2} does not envelop CA_{d1} in a conservative way. Only two RHRS trains are operating in CA_{d1}, so a loss of RHRS is more likely than in CA_{d2} when four trains are running. The applicant states that a total loss of heat removal by both RHRS and SGs is still less likely in CA_{d1} because four SGs and the SSS pump are available (two SGs and the SSS pump are unavailable in CA_{d2}), so the selection of CA_{d2} conditions for simplified modeling is appropriate. The staff reviewed the results and insights of the shutdown PRA and determined that this simplification does not affect the conclusions drawn about the PRA.

POS CB represents cold shutdown (TS MODE 5) with level reduced to mid-loop. In POS D, level is also assumed to be at mid-loop, but the reactor vessel head is off and the plant is in refueling mode (TS MODE 6). In RAI 2, Question 19-11, the staff requested a more detailed description of this POS. In an April 30, 2008, response, the applicant clarified that the mid-loop level assumption is conservative relative to time-to-boil and was selected to account for various ways outages could be conducted. Filling and draining of the reactor cavity are also included in POS D. The combination of mid-loop level and head removed is not necessarily an actual operational condition; rather, it provides the boundary condition for the POS. The applicant states that the decision to operate at mid-loop with the reactor vessel head off will be made by the COL applicant. The staff concludes that the current treatment is acceptable, given that it provides a boundary condition because the PRA considers mid-loop both with and without a large vent in the RCS. The COL holder will update the PRA prior to fuel load and reassess any important operational assumptions.

POS E and F complete the set of POS and describe the refueling process. In POS E, the reactor cavity is flooded, providing a much larger water volume for the time-to-boil calculations. In POS F, the reactor vessel is completely defueled, with the fuel assemblies in the spent fuel pool (SFP). Therefore, POS F is not modeled to determine its contribution to CDF.

The durations of each POS are listed in FSAR Tier 2, Table 19.1-91. These durations are used to scale the per-day initiating event frequencies (see below) to values appropriate for each POS, as the applicant clarified in an April 30, 2008, response to RAI 2, Question 19-13. In RAI 2, Question 19-19, the staff requested clarification of the assumed refueling cycle and shutdown duration. In an April 30, 2008, response, the applicant outlined several assumptions made to develop the total shutdown duration:

- An 18-month refueling cycle
- Normal refueling outage duration of 14 days (i.e., 9 days/yr on average)
- Forced outage average duration of 5 days/yr (3 in MODE 4 and 2 in MODE 5)

- Additional days shut down, proportionally distributed among different POS, to achieve a 94 percent plant availability (because of this adjustment, the refueling cycle length is less significant)

The effect of this approach on the assumed decay heat is discussed below. However, the staff considers the general approach to be acceptable, because it considers both normal and refueling outages, as well as the expected capacity factor of the plant, to provide an estimate at the design stage. The PRA maintenance process described previously will ensure that any changes to the assumed refueling cycle or capacity factor are factored into the PRA.

Initiating Events Assessment. A unique set of initiating events is identified during shutdown. Specifically, the applicant modeled initiating events that can affect the key shutdown safety functions of inventory control and heat removal. The four main categories of initiating events are:

- Loss of RHRS: RHRS component failures, LOOP events, or losses of support systems such as CCWS or ESWS can lead to failures of RHRS. As clarified in an April 30, 2008, response to RAI 2, Questions 19-13, 19-16, and 19-17, support system failures and LOOP events are modeled directly in the loss of RHRS initiating event fault tree. In POS CA_d, four trains are initially assumed to be running. In POS CB_d and D_d, three trains are assumed to be running, with one in standby. In POS D_u, CB_u, and CA_u, two trains are assumed to be running, with two in standby. (TS require only two trains of RHRS to be operable in MODE 5. This discrepancy is discussed below in the section on use of the PRA to develop specifications and objectives.)

- LOCA: Loss of reactor coolant through leaks or diversions in the RHRS can result in a loss of RHRS pump suction. Because the reactor coolant returns to the IRWST, it is available for injection to the RCS. This initiating event is modeled in all POS but POS F. The frequency is derived from the generic SLOCA frequency, flow diversion analysis, and fault tree analysis.

- ISLOCA: An unisolated leak or break in RHRS piping outside containment causes a loss of reactor coolant. The break flow is not available for injection to the RCS. This initiating event is modeled in all POS but POS F. The frequency is derived from pipe break frequencies and the probability that operators isolate the break.

- Uncontrolled level drop: If the operators do not stop draining reactor coolant when RCS level reaches mid-loop, the RHRS pumps can cavitate and fail, causing a loss of RHRS. This initiating frequency is derived from fault tree analysis for the mid-loop POS (CB and D).

Screened Initiating Events. Several initiating events typically found in the shutdown PRAs of operating plants are not included explicitly in the U.S. EPR model. These events are low-temperature overpressure (LTOP) events, failure of temporary pressure boundaries, and boron dilution.

LTOP Events. LTOP events, caused by additional injection when the pressurizer is water-solid (POS CA), are not modeled. In RAI 2, Question 19-14, the staff requested that the applicant justify this exclusion. In an April 30, 2008, response, the applicant stated that the pressurizer is

expected to be solid for only about 10 hours and that an overpressure event would likely result in a LOCA that could be mitigated with secondary cooling and one MHSI pump. The applicant provided a simplified calculation reflecting the human error (inadvertent start of a pump), the failure of all PSRVs and RHR suction relief valves, and the assumption that no mitigation is available. The resulting CDF of 1.2E-12/yr is less than 0.1 percent of the total shutdown CDF. Therefore, the staff concludes that the risk contribution of an unmitigated overpressurization is low enough that the event can be excluded.

LTOP events could also cause a PSRV to stick open, resulting in a LOCA. In RAI 26, Question 19-181, the staff requested additional information on the likelihood that the PSRVs will stick open. In an August 15, 2008, response, the applicant stated that the PSRVs are designed to reduce the likelihood that they will fail to re-close and provided a generic industry failure probability of 3E-3. During an audit of the applicant's PRA, the staff compared the estimated LTOP-induced LOCA frequency (stuck-open PSRV probability times the LTOP human error frequency postulated by the applicant) to the LOCA frequency in POS CA. The initiating event frequencies were comparable; however, the conservatism in the estimate and the low contribution of LOCA in POS CA to the total shutdown risk give the staff confidence that the exclusion of LTOP-induced LOCAs does not significantly impact the results and insights from the shutdown PRA.

The impact of a stuck-open PSRV following an energy addition event (e.g., loss of RHRS) is modeled explicitly in the loss-of-RHRS model by the "TR LOCASD" top event. This top event considers transient-induced LOCAs caused by PSRVs failing to re-close, RCP seal LOCAs for POS when the RCPs are operating, and failures of the RPV or pressurizer vents to close. In RAI 142, Question 19-266, the staff requested that the transient-induced LOCA phenomenon-be described in the FSAR. In a January 8, 2009, response, the applicant committed to add information on this top event to FSAR Tier 2, Section 19.1.6.1.5. The staff confirmed that Revision 1 of the U.S. EPR FSAR, dated May 29, 2009, contains the changes committed to in the RAI response.

Temporary Pressure Boundaries. The failure of temporary pressure boundaries such as nozzle dams or thimble seals is not modeled. In RAI 26, Question 19-174, the staff requested additional information on these boundaries. In a September 25, 2008, response, the applicant provided its assumptions regarding temporary pressure boundaries, as summarized below.

- Nozzle dams are not expected to be used, except during mid-cycle maintenance outages when full core off-load is not desirable. SG maintenance will be performed at mid-loop with no fuel in the RPV. RCS operating conditions will be considered in the specification of nozzle dams to provide assurance that nozzle dams will not fail.

- Plant procedures that cover reduced inventory operation will govern the installation of nozzle dams and the establishment of adequate venting to prevent pressurization of the vessel upper plenum following a loss of RHRS.

- Freeze seals are not expected to be used.

- In-core instrumentation is installed on the RPV head rather than through the bottom of the vessel.

- There are no other temporary reactor coolant system pressure boundaries as defined by NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," September 1993, and NUREG-1512, "Final Safety Evaluation Report Related to the Certification of the AP600 Standard Design," September 1998.

The staff confirmed that Revision 1 of the U.S. EPR FSAR, dated May 29, 2009, contains Item 82 added to Table 19.1-109 to reflect these assumptions. The new entry reads:

> Nozzle dams are not required during a plant shutdown, but may be used infrequently during mid-cycle maintenance, when full core off-load is not desirable. Appropriate RCS operating conditions will be considered in the specification of nozzle dams to provide reasonable assurance that nozzle dams will not fail.
>
> Plant procedures that cover reduced inventory operation will govern the installation of nozzle dams and the establishment of adequate venting to prevent pressurization of the RPV upper plenum due to a postulated loss of decay heat removal.
>
> Nozzle dams are the only U.S.– EPR-related temporary reactor coolant system boundary as specified by NUREG-1449 and NUREG-1512. Freeze seals are not expected to be used; they will not be part of the maintenance procedures for the U.S. EPR.

The statement about in-core instrumentation is consistent with the arrangement illustrated in FSAR Tier 2, Figure 4.4-10, "Arrangement of Incore Instrumentation (Side View)," and the RPV functional arrangement in FSAR Tier 1, Figure 2.2.1-2, "Reactor Pressure Vessel Functional Arrangement." It is also described in FSAR Tier 2, Section 5.3.3.1.3 and included in FSAR Tier 2, Table 19.1-102 as Item 20. Therefore, this design feature does not need to be included in FSAR Tier 2, Table 19.1-109.

Because the applicant has clearly documented in the FSAR design features and assumptions related to temporary pressure boundaries, the staff concludes that the exclusion of temporary pressure boundary failures from the PRA is acceptable.

Boron Dilution. Inadvertent dilution of the RCS is not modeled. However, the U.S. EPR includes a safety-related system (see FSAR Tier 2, Sections 7.3.1.2.11, 9.3.4.2.3.4, and 15.4.6) that monitors RCS boron concentration and isolates the CVCS if boron dilution is detected. The system and its isolation signals are required by TS during shutdown. In RAI 14, Question 19-132, the staff asked the applicant to justify exclusion of this initiating event. In a July 11, 2008, response, the applicant stated that the potential for boron dilution is unlikely and would be slow-evolving and self-regulating if it occurred. Given the applicant's response, the added protection of the boron dilution system and the lower significance of boron dilution compared to other initiating events in previous PRA models, the staff concludes that the exclusion of inadvertent dilution is appropriate.

Modeling of External Events. The risk associated with seismic events during shutdown was not addressed in the FSAR Chapter 19. Thus, in RAI 349, Question 19-331, the staff requested that the applicant describe the accident sequence analysis, HCLPF sequence assessment, results, key assumptions, and insights from the seismic risk evaluation during LPSD conditions.

RAI 349, Question 19-331, which is associated with the above request, is being tracked as an open item.

Floods and fires during shutdown are addressed with a statement that the risk is enveloped by that estimated in the at-power model. The at-power flooding and fire CDF estimates are calculated as if the plant operated at power all year (see the evaluation of FSAR Tier 2, Sections 19.1.5.2 and 19.1.5.3). This assessment is applicable for initiating events that are common to both at-power and shutdown states. However, the staff requested additional evaluation for shutdown-specific initiating events, control of barriers and transient combustibles during shutdown, MCR fires, and other external events.

Shutdown-Specific Initiating Events. In RAI 138, Question 19-251, the staff requested additional information to justify that the at-power assessment envelops shutdown-specific initiating events induced by an external event. In a December 19, 2008, response, the applicant identified three shutdown-specific fire and flood initiating events not assessed at power:

- Event 1: Flooding in the annulus propagates to SBs 2 and 3, disabling both running RHR trains.

- Event 2: Fire-induced hot short that causes an uncontrolled level drop (a leak outside of containment).

- Event 3: Fire-induced hot short that causes a flow diversion (LOCA) through one of the pathways identified in a July 11, 2008, response to RAI 14, Question 19-143.

The applicant estimated the frequency of Event 1 to be 5.E-8/yr based on the annulus flooding frequency, the POS in which the condition can occur, and the probability that the applicable RHR trains are running. This frequency is two orders of magnitude less than the total loss of RHR frequency used in the shutdown PRA. In this scenario, trains 2 and 3 of CCWS, MHSI, and EFWS, as well as both CCWS CHs (assuming CCWS trains 2 and 3 are running) would also be affected by the initiating event. The applicant's estimated the CDF associated with this scenario to be 1.2E-13/yr, which is insignificant compared to the 2.4E-8/yr CDF from all losses of RHR.

The frequency of Event 2 was estimated to be 1E-5/yr based on the FB fire frequency, the POS in which the condition can occur, and the conditional probability of a hot short. This frequency is nearly three orders of magnitude less than the total uncontrolled level drop frequency used in the shutdown PRA. CVCS is also affected by this initiating event. The CDF associated with the scenario was estimated to be 4.9E-12/yr, which the applicant determined to be insignificant compared to the 1.6E-8/yr CDF from all uncontrolled level drops.

The applicant stated the frequency of Event 3 to be 2E-5/yr for valves in the SBs and 6E-9/yr for valves in containment. These estimates are based on the relevant fire frequencies, the shutdown duration, the probability of a hot short, and the probability of isolation failure. Fires in containment are not evaluated further because of the low calculated frequency, the large containment volume allowing heat dissipation, and the limited heat release rate of combustibles in containment. Fires in an SB can affect the relevant train of CCWS and MHSI, SCWS (if the fire is in SB 4), and the CCWS CH. The CDF associated with the scenario was estimated to be 1.7E-8/yr, about two percent of the CDF from all LOCAs during shutdown. Since LOCAs during shutdown contribute about 30 percent of shutdown CDF, the CDF contribution of Event 3 is expected to be less than 1 percent.

In RAI 197, Question 19-281, the staff requested that a summary of this information be added to the FSAR. In an April 10, 2009, response, the applicant committed to add the requested summary to FSAR Tier 2, Section 19.1.6.1.8. The applicant concluded that, based on the bounding nature of the at-power fire and flood evaluations and on the low risk impact of the shutdown-specific internal hazards, the risk from fires and floods evaluated in the at-power model envelops the risk during shutdown. The staff confirmed that Revision 1 of the U.S. EPR FSAR, dated May 29, 2009, contains the changes committed to in the RAI response.

After reviewing the applicant's description of the shutdown-specific fire and flood scenarios and the associated sensitivity studies, the staff concludes that these scenarios are not significant contributors to the shutdown PRA. Therefore, the qualitative discussion of fires and floods is acceptable.

Barriers and Transient Combustibles. The control of barriers and transient combustibles has the ability to increase risk during shutdown. In RAI 2, Question 19-20, the staff requested additional information about these issues. In an April 30, 2008, response, the applicant provided the requested information.

The at-power internal flooding PRA defines entire buildings as flood areas. FSAR Tier 2, Section 19.1.5.2.1.2 states that division walls serve as flood barriers below the 0 m (0 ft) elevation. Above the 0 m (0 ft) elevation, watertight doors and openings for water flow to lower building levels prevent water ingress into adjacent divisions.

As stated in Item 64 of FSAR Tier 2, Table 19.1-109, automatic isolation of ESWS and DWDS on high sump level ensures that floods caused by breaks in these systems are contained below ground level. In a February 19, 2009, response to RAI 131, Question 09.02.01-25, the applicant committed to revise the FSAR to clarify that signals from the SB sump level instruments are safety-related and that no operator action is required to isolate ESWS in a large flooding event. The staff confirmed that Revision 1 of the U.S. EPR FSAR, dated May 29, 2009, contains the changes committed to in the RAI response. In RAI 14, Question 19-138, the staff asked whether the sensors and isolation signals that cause the pump trip are operable during shutdown. In a July 11, 2008, response, the applicant stated that the sensors and isolation signals are assumed operable during shutdown, and that COL Information Item 19.1-9 is provided to confirm that this assumption remains valid. In addition, Item 64 in FSAR Tier 2, Table 19.1-109, describes automatic and manual isolation of ESWS and DWDS and (as the applicant stated in a December 19, 2008, response to RAI 138, Question 19-253, on the operability assumption of sensors and isolation signals during shutdown) applies to both at-power and shutdown conditions.

The walls between the FB and SBs 1 and 4 have doors at the -9.45 m (-31 ft) elevation and are not credited as flood barriers. Therefore, according to the applicant, the flood barriers credited in the at-power PRA are not likely to be challenged during shutdown. The applicant notes that the doors that separate the RB annulus from SBs 2 and 3 at the 0 m (0 ft) elevation may be open during certain phases of shutdown. In this case, the open doors would actually have a positive effect; FSAR Tier 2, Section 19.1.5.1.2.3 indicates that core damage is assumed if the doors do not fail open and water level reaches the connection boxes for the control and power cables.

Similarly, most of the fire areas in the at-power fire risk assessment encompass a whole building. In the SBs, most fire areas are located on different floors, where direct propagation can occur only through floor and ceiling fire barriers, which are not likely to be removed during shutdown. Indirect propagation could occur via stairways or airshafts, but these areas have no

significant amount of combustible material. In a July 11, 2008, response to RAI 14, Question 19-139 on the fire barriers, the applicant clarified the fire areas that are separated by a fire-rated door, which could be opened during shutdown. In RAI 53, Question 19-201, the staff asked the applicant to address how these doors will be controlled. In a September 22, 2008, response, the applicant stated that administrative controls will define the control of fire barriers during shutdown and provided the results of a sensitivity study in which the at-power fire PRA was modified to merge fire areas separated only by a fire-rated door. The sensitivity case resulted in an at-power fire CDF increase of 26 percent. However, the fire barriers would only be removed during shutdown, so the impact of open doors on the sequences that apply both at power and during shutdown is less than one percent. Therefore, the staff concludes that possible challenges to the integrity of fire doors as barriers during shutdown do not have a large impact on the assumption that the shutdown fire risk is enveloped by the at-power model.

In addition, the shutdown PRA assumes that control of transient combustibles and limiting maintenance activities applies to operating RHRS trains and supporting systems. Physical separation makes it possible to implement controls during maintenance in shutdown to protect operating trains. The PRA assumes that written procedures to cover the fire protection program are implemented and maintained. Item 23 in FSAR Tier 2, Table 19.1-108 and Item 58 in FSAR Tier 2, Table 19.1-109 provide additional assurance that these assumptions will remain valid in the as-built, as-operated plant.

Main Control Room Fires. The RSS is only required to be operable during MODES 1, 2, and 3 per TS 3.3.3; however, the at-power PRA considers transfer to the RSS following a MCR fire. In RAI 197, Question 19-282, the staff requested that the applicant discuss the availability of the RSS during shutdown. In an April 10, 2009, response, the applicant revised FSAR Tier 2, Table 19.1-109 to include the assumption that the RSS is available in all POS with fuel in the core. The RSS is also included in RAP, which will include measures to ensure its availability (e.g., maintenance rule compliance) as discussed in the staff's evaluation of FSAR Tier 2, Section 17.4. Based on these administrative controls, the staff concludes that there is sufficient assurance that the RSS will be available following a potential MCR fire during shutdown.

The staff observes that the low CDF from MCR fires occurring at power depends on a fire frequency of 4.2E-4/yr and an HEP for the transfer action of 7E-5. In October 9, 2008, response to RAI 66, Question 19.01-34 on the control room evacuation, the applicant stated that MCR fires are assumed to cause an LBOP, after which 90 minutes are available to take action; the HEP is based on these assumptions. In RAI 227, Question 19-299, the staff requested additional information on the applicability of the at-power HEP to shutdown scenarios. In a July 6, 2009, response, the applicant stated that running RHR trains would continue to operate without need for operator intervention. The applicant committed to revise the FSAR to indicate that loss of the MCR during shutdown would not, by itself, result in an initiating event. **Inclusion of the above commitment, which is associated with RAI 227, Question 19-299, is being tracked as Confirmatory Item 19-299.**

In addition, the applicant performed sensitivity studies related to two scenarios:

- A fire in the MCR increases the likelihood of an operator-induced ULD initiating event during drain-down.

- A fire in the MCR disables all operator actions, because the RSS may not be available.

These cases resulted in CDF increase of 8.6E-10/yr, approximately 1.5 percent of the shutdown CDF. The applicant compared this value to the CDF evaluated for MCR fires in the at-power model; if this CDF estimate were scaled down to the fraction of year shut down, it would be larger than the sensitivity case result. Based on this sensitivity study, and the understanding that MCR fires would not cause an initiating event, the staff concludes that MCR fires are not significant contributors to shutdown risk.

Other External Events. A quantitative analysis of other external events (e.g., high winds) was not performed specifically for shutdown modes. In a December 19, 2008, response to RAI 138, Question 19-251 on the external events during shutdown, the applicant stated that the evaluation of these events for power operation in FSAR Tier 2, Section 19.1.5.4, considers both power operations and shutdown, and these external events do not cause shutdown-specific initiating events. The shutdown-specific fire and flood initiating events described above all originate in safety-related structures resistant to external events. In addition, external events may cause a LOOP, which is already modeled in the shutdown PRA. Based on this information, the staff agrees that other external events are not likely to cause shutdown-specific initiating events and that the at-power evaluation also applies to shutdown.

Analysis of Accident Sequences. Core damage at shutdown is defined as uncovering the core − the point at which RCS level reaches TAF. As in the at-power model, to constitute success, an accident sequence must reach a safe, stable end state for 24 hours. Liquid heat-up and bulk boiling equations are used to calculate the time to TAF given loss of heat removal and subsequent loss of inventory. The parameters used in these equations (e.g., coolant temperature, coolant volume, decay heat load, and heat input from RCPs) vary depending on the time after shutdown and the POS. FSAR Tier 2, Figure 19.1-20, "Time to TAF - Level 1 Shutdown," plots the approximate time for coolant level to reach TAF during shutdown. In RAI 14, Question 19-131, the staff observed that the applicant extended POS durations based on multiple outage types and estimated plant availability. For a real outage, the time of entrance into a given POS may be earlier than the sum of the estimated POS durations; therefore, the decay heat level may be higher than that assumed in the PRA. In a July 11, 2008, response, the applicant indicated that the design certification PRA does not correspond to any specific outage and that any difference caused by earlier POS entrances would not be significant enough to change the conclusions from the shutdown PRA. The applicant cited conservative assumptions in the decay heat modeling (especially the use of the beginning decay heat for the entire POS), slow changes in the decay heat curve, and the length of time available for operator actions as support for its position.

In RAI 142, Question 19-267, the staff asked for additional information about credited operator actions for which—at a higher decay heat—the time available would be less than that allowed. In a January 8, 2009, response, the applicant provided the results of a sensitivity study using the decay heat levels associated with earlier POS entry times. The applicant identified four operator actions with less time available because of the higher decay heat level and adjusted the HEPs accordingly. The total increase in shutdown CDF for the sensitivity study was approximately 2.2 percent. This effect is dominated by the HEP of 1.0 for the operator action to start RHRS in POS DD; less than 25 minutes was projected to be available for this action. The staff concludes that the conservative assumptions used in the sensitivity study and resulting small impact are sufficient to demonstrate that the POS entry time assumptions do not distort the results and insights of the average-outage PRA.

Based on these success criteria, the applicant developed unique event trees for shutdown using the same methodology as in the at-power model. These event trees are collected in FSAR Tier

2, Appendix 19B, “Event Trees for Core Damage Sequences Initiated During Low Power Operation.”

System Modeling. The same systems are modeled in the shutdown PRA as in the at-power PRA. However, some of the systems operate differently or are unavailable during shutdown. FSAR Tier 2, Table 19.1-89, “System Availability During Shutdown,” lists which systems are available in each POS. In addition, some success criteria are relaxed because of the reduced temperature, pressure, and decay heat during shutdown. The applicant identified several specific differences:

- RHRS is normally operating with suction from the hot legs, rather than in standby LHSI mode with suction from the IRWST. RHRS pumps are no longer actuated by a safety injection signal when temperature and pressure fall below the P14 permissive setpoints [180 °C and 32 bars (356 °F and 464 psia); see FSAR Tier 2, Section 7.2.1.3.9]. Therefore, standby pumps must be started by the operator.

- To protect against cavitation, the operating RHRS pumps trip on low loop level. Failure of this protective trip fails the RHRS pumps, but success of the trip allows the operator to restart the pumps later.

- To protect against ISLOCA, the appropriate RHRS train is isolated and the pump tripped when high sump level is detected in an SB.

- MHSI is actuated by a safety injection signal based on low delta-P_{sat} in POS CA and low loop level in POS CB, D, and E. This signal is described in FSAR Tier 2, Section 7.3.1.2.1.

- During POS C, the P13 permissive must automatically reset to allow automatic EFWS operation. The P13 permissive is validated when three of four hot leg temperature readings fall below 95 °C (203 °F) (see FSAR Tier 2, Section 7.2.1.3.8).

- Only the normal pressure control mode of the MSRTs is required. When pressure and temperature fall below the P14 permissive setpoints, the partial cooldown function of the MSRTs is disabled, and the MSRT opening pressure is reduced to 999.7 kPa (145 psia).

- Only two RCPs are running in POS CA, so only two pumps must trip on a loss of pump cooling. Seal cooling is not required during shutdown because of the reduced temperature and pressure.

- The CVCS charging function is not credited for injection during shutdown. However, automatic isolation of the CVCS low-pressure reducing station is modeled during an uncontrolled draindown event. Failure of this isolation function results in a diversion of IRWST water outside containment.

- Only one SG volume, rather than all four, is needed during an SBO.

- Only one or two PSRVs may be needed for primary bleed, rather than the three needed at power. However, the shutdown model currently assumes that three

PSRVs are required, given the modeling uncertainty described above for the at-power model.

- IRWST cooling is not required when the RPV head is off.

The applicant made two other major assumptions in the system modeling. First, IRWST suction strainer plugging is modeled with the same probability as in the at-power model. The applicant acknowledges that maintenance work during shutdown could cause a higher plugging probability, but states that the probability is dependent on foreign material control procedures that are not yet available. Item 14 of FSAR Tier 2, Table 19.1-108 states that the IRWST design and plant procedures (e.g., foreign material control) provide reasonable assurance that the strainer plugging probability is low. COL Information Item 6.3-1, listed in FSAR Tier 2, Table 1.8-2, states that the COL applicant "will describe the containment cleanliness program which limits debris within containment." The staff concludes that this COL item is sufficient to ensure that the strainer plugging probability is reasonable.

The second major assumption is that all preventive maintenance occurs in POS E (one division at a time), except for maintenance on the two unavailable SGs in POS CA_d and CB_d. Item 57 in Table 19.1-109 provides the details of this assumption so that it can be verified for the as-built, as-operated plant. The availability of equipment is discussed in more detail in Section 19.1.4.7.1.3 of this report.

Human Reliability Analysis. As in the at-power PRA model, the post-initiator HEPs for shutdown were estimated using SPAR-H. The probability estimates stem from a comparison of the time available (based on the time to TAF, calculated for specific initiating events) to the time needed for diagnosis and action. In RAI 2, Question 19-21, the staff requested additional detail on the modeling of low-probability operator errors in the shutdown PRA. In an April 30, 2008, response, the applicant stated that "expansive" time is assumed for both diagnosis and action when five or more hours are available. For two operator actions, 8 or more hours are available, so an additional PSF of 0.5 is included in both diagnosis and action HEPs. In these cases, a shift change is likely to have occurred, increasing the chances of diagnosing and correcting the problem. In an April 30, 2008, response to RAI 2, Question 19-18 regarding the assumption that all performance shaping factors (PSF) for operator actions are assumed to be optimal, the applicant clarified that all other PSFs are assigned a nominal value of one, which is recommended when insufficient information is available to choose a more specific value.

FSAR Tier 2, Section 19.1.6.1.6 describes the operator actions and associated alarms and indications that are assumed in the shutdown PRA model. Certain operator actions are included in the initiating event analyses. Operators are expected to start a standby RHRS train when one is lost, isolate RHRS flow diversions before RCS level drops to the low loop level setpoint, and stop uncontrolled level drops during the draindown to mid-loop. Operator error is also included as a contributor to the uncontrolled level drop initiating event.

When RHRS is lost, operators may need to take several actions: Start the standby RHRS train, establish either feed and bleed (if the vessel head is on) or coolant makeup (if the vessel head is off), and establish IRWST cooling. The applicant expects that the operators will have cues such as event-related indication (e.g., system trouble or no flow), RCS and RHR temperature and pressure, vessel level, IRWST temperature, and containment temperature and pressure.

If a loss of inventory occurs, operators may need to establish makeup: Start the standby RHRS train, establish primary bleed (if makeup is available but secondary cooling is not), isolate the break or flow diversion, and establish IRWST cooling. The applicant expects that the operators

will have cues such as RHR failure indication (e.g., system trouble or no flow), RCS and RHR temperature and pressure, VCT and coolant storage levels, IRWST level and temperature, and containment temperature and pressure.

Operator actions associated with support systems such as electrical and HVAC are the same as in the at-power model. In an April 30, 2008, response to RAI 2, Question 19-21 on the modeling of low-probability human failures in the shutdown PRA, the applicant stated that these systems are operated in a similar manner at shutdown and should have similar cues, timing, and procedures as assumed in the at-power model. Specifically, the operator error to start a maintenance HVAC train when the safety-related train fails (OPF-SAC-1H), has specific indications for failure of a safety-related system. Because similar cues are expected, the staff concludes that it is acceptable to assume that these operator actions can be modeled the same way at power and during shutdown.

In RAI 14, Question 19-141, the staff requested a discussion of the modeling of pre-initiator human errors in the shutdown PRA. In a July 11, 2008, response, the applicant clarified that pre-initiator HEPs are modeled the same as in the at-power model. The applicant stated that this treatment is conservative, because recovery of human errors is easier during shutdown with maintenance crews present. The staff considers it appropriate to assume that pre-initiator human errors (e.g., mis-calibration) are no more likely to disable SSCs required during shutdown than SSCs needed following initiating events after power. Therefore, this treatment is acceptable.

Model Quantification. As with the at-power model, the applicant quantified the event and fault trees together using the RiskSpectrum® computer code. A 1E-20 truncation limit and a 1E-6 relative truncation limit are used in the quantification, resulting in over 90,000 minimal cutsets for all POS. Uncertainty analyses were performed using Monte Carlo simulation within the RiskSpectrum® program, using the probability distributions associated with initiating event frequencies, failure rates, CCF probabilities, and HEPs. Sensitivity studies were also performed to address uncertainty in success criteria and assumptions made in the PRA model. These uncertainty and sensitivity studies are discussed below.

19.1.4.7.1.3 *Significant Accident Sequences Leading to Core Damage*

FSAR Tier 2, Figure 19.1-22 shows that operation at mid-loop contributes 75 percent of the shutdown risk. Mid-loop with the vessel head on (POS CB) accounts for two-thirds of this contribution, while POS D (where mid-loop level is assumed and the vessel head is off, even though the level is likely to be higher than mid-loop for most of the POS) contributes the rest. POS CA contributes the bulk of the remaining risk.

FSAR Tier 2, Table 19.1-90 presents the initiating events whose accident sequences contribute more than one percent to the overall shutdown CDF. The most significant initiating events are uncontrolled level drops in POS CB_d and D_u (about 30 percent of CDF), a LOCA in POS CB_d (more than 10 percent of CDF), and a loss of RHRS in POS CB_d (more than 10 percent of CDF).

As in the at-power model, LOOP events are significant contributors to shutdown risk. LOOP is modeled as a failure event in the fault trees rather than a separate initiating event; therefore, the contribution of LOOP events to shutdown CDF can be estimated by the FV value for the LOOP basic event. Cutsets that include LOOP contribute about 40 percent of the total shutdown risk.

The applicant has provided a proposed table (FSAR Tier 2, Table 19.1-130) that lists all sequences contributing more than one percent to shutdown CDF. As stated in Section 19.1.4.4, "FSAR Tier 2, Section 19.1.4: Safety Insights from the Internal Events PRA for Operations at Power," of this report," inclusion of this table in the FSAR is being tracked as **Confirmatory Item 19-285**. For each sequence, the table provides the related event tree, sequence number, sequence identifier, total frequency, and description. Because the same event tree sequence is used for evaluation of multiple POS, the staff combined multiple table entries to produce the three sequences below, representing about 80 percent of the shutdown CDF.

- SD RHR C-15 (1.8E-8/yr): Losses of RHRS during POS CA or CB, followed by failures of EFWS, MHSI, LHSI, and SAHRS (dominated by total losses of ac power that initiate the event and disable all mitigation), resulting in a loss of all heat removal.

- SD ULD-3 (1.4E-8/yr): Uncontrolled level drops caused by failure (mechanical or operator) to stop draining during either POS CB_d or D_u, followed by long-term failure to isolate the drain path, resulting in water from the IRWST being pumped into the RCS and out the drain path outside containment. When the IRWST empties, makeup to the RCS is no longer possible.

- SD LOCA C-30 and D-3 (1.4E-8/yr): LOCA during POS C, D, or E (the most likely of which are spurious valve operations that the operator fails to isolate), followed by failure of MHSI and LHSI (dominated by CCF of the injection check valves), resulting in a loss of inventory makeup.

FSAR Tier 2, Table 19.1-92, "U.S. EPR Important Cutset Groups - Level 1 Shutdown," to which Table 19.1-130 refers, describes the sequences in more detail by presenting the top 100 cutsets in 15 groups, representing over 60 percent of the total CDF. This treatment provides a slightly different ranking and total frequency, because many lower-frequency cutsets are included in the total sequence frequencies in FSAR Tier 2, Table 19.1-130. The top seven cutset groups are listed below:

- Group 5 (16.5 percent): This group represents a loss of RHRS in POS C, followed by failure of all heat removal via EFWS, MHSI, LHSI, and SAHRS. In the representative cutset, the loss of RHRS in POS CB_d occurs because of a LOOP that is not recovered within 1 hr. CCF of the EDGs causes CCWS to fail, disabling MHSI and the RHRS heat exchangers. Failure of the Division 1 SBODG causes EFWS to fail, since only the Division 1 and 2 SGs are available in POS C, and fails SAHRS. Similar combinations of failures also occur in POS CA_u, CA_d, and CB_u.

- Group 13 (12.9 percent): This group represents a LOCA in POS C, followed by a failure of safety injection. In the representative cutset, an RHRS relief valve opens prematurely in POS CB_d, the operator fails to isolate the flow diversion, and both MHSI and LHSI fail because of a CCF of the common injection check valves.

- Group 1 (12.0 percent): This group represents an uncontrolled level drop in POS D in which both automatic and manual isolation of the CVCS low-pressure reducing station fail. In the representative cutset, the level drop occurs in POS D_u, the reducing station MOVs fail to close by a common cause, and the operator

fails to isolate the reducing station. Mitigating systems are available, but the RCS is slowly drained outside the containment, leading to core damage.

- Group 2 (11.9 percent): This group represents a sequence similar to Group 1, but in POS CB. In the representative cutset, the level drop occurs in POS CB_d, the reducing station MOVs fail to close by a common cause, and the operator fails to isolate the reducing station. Mitigating systems are available, but the RCS is slowly drained outside the containment, leading to core damage.

- Group 14 (5.3 percent): This group represents a LOCA in POS D or E, followed by a failure of safety injection. Similar to that in Group 13, the representative cutset includes premature opening of a RHRS relief valve in POS D_u, failure of the operator to isolate the flow diversion, and CCF of the MHSI and LHSI common injection check valves.

- Group 15 (1.6 percent): This group represents an ISLOCA caused by an RHRS pipe break in POS CB_d or E. In the representative cutset, the pipe break occurs outside containment and cannot be isolated because of failure of the PAS and an operator error. Core damage is assumed regardless of the availability of mitigating systems.

- Group 6 (1.4 percent): This group represents a loss of RHRS in POS C, followed by failure of all heat removal via EFWS, MHSI, LHSI, and SAHRS. In the representative cutset, the loss of RHRS in POS CB_d occurs because of a LOOP that is not recovered within one hour. CCF of the EDGs causes CCWS to fail, disabling MHSI and the RHRS heat exchangers. The operator fails to crosstie electrical divisions, disabling the MSRTs and EFWS. Finally, failure of the dedicated heat sink disables SAHRS. Similar combinations of failures also occur in POS CA_u, CA_d, and CB_u.

19.1.4.7.1.4 *Risk-Significant Failures*

The equipment failures, human errors, and CCFs significant to U.S. EPR shutdown risk are tabulated in FSAR Tier 2, Tables 19.1-93 through 19.1-98, ranked by their RAW and FV importance measures.

The most risk-significant equipment failures, ranked by FV importance, are failures of a single EDG or SBODG, LHSI isolation check valve, or CVCS low-pressure reducing station isolation MOV. These failures relate to LOOP and level-drop initiating events, which are both important in the shutdown PRA. EDG and SBODG failures appear in cutsets that contribute about 30 percent and 20 percent of the CDF, respectively. The LHSI check valve failure appears in cutsets that contribute about 20 percent of the CDF. Failure of the low-pressure reducing station isolation MOV appears in cutsets that contribute about 20 percent of the CDF. When equipment failures are ranked by RAW importance, the most important failures are all electrical: A single 480V load center, 6.9kV switchgear, or 480V MCC. If the load center or switchgear were always certain to fail, CDF would increase by a factor of about 50. If the MCC always failed, CDF would increase by a factor of about 40.

The most risk-significant human error for both FV and RAW importance is failure of the operator to isolate the CVCS low-pressure reducing station, the action needed to mitigate an uncontrolled level drop. This human error appears in cutsets that contribute 25 percent of the shutdown CDF. Overall CDF would increase by a factor of more than 4,500 if the operator

never isolated this location when needed. When ranked by RAW importance, operator failure to start the maintenance HVAC trains after the safety-related trains fail is also important. If the operator never performed this action, shutdown CDF would increase nearly 100 times. Two more operator actions are important based on their FV values: Operator failure to isolate an RHRS flow diversion in POS CB, and operator failure to stop draindown at mid-loop. These human errors appear in cutsets that contribute about 20 percent and 10 percent of the CDF, respectively.

As in the at-power model, CCFs have a much larger effect on overall risk, because they can disable one or more systems. The RAW rankings show that CCFs that disable the safety-related batteries, injection from the IRWST, or the HVAC system are most important. In addition, all CCFs of I&C have high RAW values, because these failures can prevent multiple safety systems from actuating.

As stated previously, the tables provided in the FSAR do not include all failures with importance measures above the thresholds stated on page 19.1-54 of the FSAR (RAW of 2 or FV of 0.005); instead, components and failure modes are grouped to identify risk-significant components. In a July 11, 2008, response to RAI 14, Question 19-126, the applicant confirmed that the complete list of equipment failures and operator actions above the thresholds was used as input to other programs (e.g., RAP). In the same response, the applicant submitted 36 tables of specific failures and importance measures for the staff's review. This additional information gave the staff confidence that the most important equipment failures and operator actions were captured in the FSAR and that the appropriate input was provided to other programs.

19.1.4.7.1.5 *Insights from the Uncertainty and Sensitivity Analyses*

Uncertainty Analysis. The applicant quantified parametric uncertainty in the CDF results using a process similar to that discussed above for the at-power model, by propagating uncertainty distributions within the RiskSpectrum® software.

FSAR Tier 2, Figure 19.1-23 shows the results of the parametric uncertainty evaluation for the shutdown PRA. The CDF point estimate reported in the FSAR is 5.7E-8/yr, and the mean CDF from the uncertainty analysis is about twice as high at 9.9E-8/yr. As discussed above in Section 19.1.4.4.2.4 of this report, the Monte Carlo sampling approach uses the same value for each failure probability within a correlated "state-of-knowledge" group. For cutsets that involve failures of multiple redundant pieces of equipment, the correlation results in a mean value that is larger than the product of the mean values of the event probabilities.

The uncertainty analysis presented in the FSAR does not include the modeling uncertainty cases described above in the evaluation of FSAR Tier 2, Section 19.1.4.1. Cases 1 and 2, related to EFWS and feed-and-bleed success criteria, are less important to the shutdown PRA results because of the lower decay heat at shutdown. However, Case 3, related to HVAC recovery assumptions, is relevant to shutdown operations. In RAI 14, Question 19-35, the staff requested that the applicant evaluate this case. In a July 11, 2008, response, the applicant provided the results of this uncertainty case, showing less than a 10 percent change in both the point estimate and mean CDF. Therefore, the staff concludes that the impact of modeling uncertainty on shutdown CDF is much less significant than for the at-power internal events CDF.

Sensitivity Analyses. The applicant also performed 12 sensitivity cases to evaluate the impact of modeling assumptions on the shutdown CDF. The results of these cases are tabulated in FSAR Tier 2, Table 19.1-100. Based on these studies, the applicant obtained several insights:

- The shutdown CDF is more sensitive to CCFs than the at-power CDF. If CCFs are not considered, CDF decreases by more than 80 percent. If the EDGs and SBODGs are put in the same CCF group, CDF approximately quadruples.

- The results are sensitive to HEP values. CDF would approximately double if all HEPs were set to their 95th percentile values. However, the specific room cooling operator action that is very important in the at-power model would only increase the shutdown CDF by a factor of 1.5 if the operators never took the action.

- The shutdown CDF is sensitive to the assumption of Division 4 UHS availability during an SBO, which did not have a significant impact on the at-power results. CDF increases by about 30 percent if the SBO crosstie for the dedicated ESWS train is not credited.

- If preventive maintenance on one division of safety systems occurs in POS D_u and CB_u as well as POS E, shutdown CDF increases by about 50 percent.

In addition to the sensitivity studies documented in the FSAR, the applicant performed numerous sensitivity studies to support RAI responses. Generally, these sensitivity studies demonstrated that a particular modeling assumption or simplification questioned by the staff had no significant impact on the results and insights of the PRA. That is, they do not represent key sources of uncertainty for the PRA.

In summary, 10 CFR 52.47(a)(23) requires that the applicant describe the design-specific PRA and its results. The discussion above provides the staff's evaluation of the applicant's description of the Level 1 shutdown PRA and its results, as well as related issues raised in RAIs. The staff reviewed detailed results including data, sequence, and importance measures and requested justification for specific aspects of the PRA described in the FSAR. This review was sufficient to determine that the Level 1 shutdown PRA appropriately reflects the U.S. EPR design. Additional discussion related to the scope, level of detail, and technical adequacy of the PRA in general was discussed in the staff's evaluation of FSAR Tier 2, Section 19.1.2 above. Therefore, the staff concludes, based on the detailed information described above, that the applicant has provided an adequate description of the design-specific shutdown PRA, as well as its results, sufficient for the staff to obtain risk insights about the U.S. EPR design.

19.1.4.7.1.6 *Use of PRA to Establish Specifications and Objectives*

The SRP states that the staff should ensure that the applicant has used the PRA results and insights in an integrated fashion to identify and establish specifications and performance objectives for the design, construction, testing, inspection, and operation of the plant. The staff evaluates this acceptance criterion by reviewing PRA input to the design process (FSAR Tier 2, Section 19.1.3.4), PRA input to other programs (FSAR Tier 2, Section 19.1.7), and the applicant's list of COL information items.

Shutdown PRA input is important to development of TS and other operating requirements. The staff observed that FSAR Tier 2, Sections 5.4.7.2.1 and 19.1.6.1.7 describe design features to address shutdown and mid-loop operations. However, most of these features initially had little or no coverage in TS.

In RAI 2, Question 19-27, the applicant was requested to discuss the treatment of important design features in TS, describe how each feature is credited in the PRA, and provide a

sensitivity study crediting only systems required to be operable during shutdown according to TS. In a May 30, 2008, response, the applicant stated that TS requirements for CCWS and ESWS are determined by the systems they support, such that CCWS and ESWS trains supporting the required RHRS trains during shutdown also must be operable. In addition, the applicant's response stated that shutdown risk will be managed through a combination of TS and administrative controls that will be developed using NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management," dated December 1991. In FSAR Tier 2, Table 19.1-108, Item 13 states that NUMARC 91-06 should be considered when developing the plant-specific operations procedures.

NUMARC 91-06 provides high-level risk management guidance; more specific procedural actions are detailed in GL 88-17, "Loss of Decay Heat Removal," October 17, 1988. The applicant provides information related to GL 88-17 in several locations in the FSAR. FSAR Tier 2, Section 5.4.7.2.1 lists 10 design features that address shutdown and mid-loop operations per GL 88-17. The GL 88-17 entry in FSAR Tier 2, Table 15.0-60 states that the loss of decay heat removal is addressed "through the automatic actuation of MHSI on a low RCS loop level signal during non-power operation." In addition, various entries in FSAR Tier 2, Tables 19.1-108 address the relevant expeditious actions and programmed enhancements suggested in GL 88-17.

Table 19-27-2, provided in the response to RAI 2, Question 19-27, lists RAW values for the systems used during shutdown. In RAI 26, Question 19-176, the staff observed that several design features (e.g., SIS, CVCS letdown isolation, and MHSI) would increase average shutdown CDF to a value comparable to the Commission's safety goals if they were not available during shutdown. Neither the low loop level SIS nor the MHSI system was initially required by TS in MODES 5 and 6. The loop level sensors are used to isolate letdown, stop the LHSI pumps, and start makeup with the MHSI pumps on low loop level. Although they were not included in the list of RAW values in the response to Question 19-27, Table 19.1-98 indicates that CCF of these sensors is of high importance. The IRWST was also not included in this list, but Table 19.1-97 indicates that CCF of the IRWST (because of check valve or strainer failure) is extremely important. The staff requested a sensitivity study specifying guaranteed failure for all operator actions, equipment, and sensors related to systems that are not required for shutdown.

In an October 31, 2008, response to Question 19-176, the applicant provided the results of additional sensitivity studies in which systems not required by TS during shutdown were unavailable. The unavailable equipment corresponds to several of the shutdown design features identified in FSAR Tier 2, Section 5.4.7.2.1. The results of these sensitivity studies (rounded from the values in the RAI response) are reproduced in Table 19.1-18 of this report.

Table 19.1-18 Sensitivity Case Results for Minimal TS Compliance

Case ID	Unavailable Equipment	CDF (/yr)	Factor Increase from Base CDF
Base case		5.7E-8	1
176-1	EFWS trains 1-4	3.3E-7	6

Case ID	Unavailable Equipment	CDF (/yr)	Factor Increase from Base CDF
176-2	Signals for RHRS pump protective trip on hot leg low-low level	1.5E-6	26
176-3	SIS low loop level signals (MHSI pumps)	2.8E-6	49
176-4	CVCS low pressure reducing station isolation on hot leg low-low level signal	1.7E-6	30
176-5	SB sump signals for automatic isolation of RHRS breaks outside containment	1.5E-6	26
176-6	MHSI trains 1-4	4.5E-6	79
176-7	IRWST sump strainers	2.9E-3	5E4
176-8	RHRS pumps 3 and 4	2.4E-6	42

Only complete unavailability of the IRWST would increase shutdown risk above the Commission's safety goals—without the IRWST, all LOCA events would lead to core damage. However, unavailability of other systems or signals would increase shutdown risk by factors of approximately 6 to 80. The largest impact comes from MHSI, both unavailability of the trains themselves and unavailability of the actuation signal on low loop level.

In RAI 142, Question 19-269, the staff requested that the applicant justify the lack of TS requirements for which sensitivity studies were performed in response to Question 19-176. In a March 6, 2009, response, the applicant committed to revise the TS to include requirements for the IRWST and MHSI during MODES 5 and 6. The staff confirmed that Revision 1 of the U.S. EPR FSAR, dated May 29, 2009, contains the changes committed to in the RAI response. In a June 30, 2009, response to RAI 103, Question 16-138, the applicant separately committed to add a TS requirement for automatic SIS actuation on low loop level. **RAI 103, Question 16-138 is being tracked as Confirmatory Item 16-138.** A summary of these changes follows.

- TS 3.3.1: This specification for the PS ensures the availability of the RCS loop level signal and automatic SIS actuation on low loop level during shutdown.

- TS 3.5.6: This specification for the IRWST ensures the availability of a borated water source for the MHSI pumps in MODE 5.

- TS 3.5.7: This specification for the IRWST ensures the availability of a borated water source for the MHSI pumps in MODE 6. The requirements include the contained water volume of the refueling cavity, refueling canal, and IRWST due to fuel handling requirements. The boron requirements are addressed in TS 3.9.1.

- TS 3.5.8: This specification ensures the availability of MHSI pumps for RCS makeup from the IRWST in MODES 5 and 6.

Based on the extensive sensitivity studies performed by the applicant, subsequent identification of the most risk-significant systems during shutdown, and TS developed to control the availability of these systems, the staff concludes that the applicant has appropriately used the PRA as an input to developing specifications and objectives for shutdown states. In addition, the documentation of assumptions and insights in FSAR Tier 2, Tables 19.1-108 and 19.1-109 provides additional assurance that necessary equipment will be available during shutdown through a combination of TS requirements and administrative (e.g., NUMARC 91-06) guidance.

The staff also reviewed the applicant's development of PRA-based insights, as defined above in the evaluation of FSAR Tier 2, Section 19.1.4.1. FSAR Tier 2, Tables 19.1-102, 19.1-108, and 19.1-109, described above, include insights and assumptions related to shutdown risk. For example, FSAR Tier 2, Table 19.1-108 includes the importance of mid-loop level control. Several of the insights relate to the development of shutdown procedures, including the use of NUMARC 91-06 as guidance. Therefore, the tabulation of insights provides a ready reference to U.S. EPR designers to ensure that PRA insights are considered in future design development. As stated previously, FSAR Tier 2, Table 19.1-109 lists important modeling assumptions that need to be reviewed for applicability in a future plant-specific PRA update in response to both COL Information Item 19.1-9 and 10 CFR 50.71(h)(1). Items 50 through 58, 82, and 83 of this table relate specifically to shutdown PRA assumptions. The staff expects to use FSAR Tier 2, Table 19.1-109 in its confirmation that both the COL information item and the regulation have been met. Therefore, based on the information provided in the FSAR, the staff concludes that the applicant has appropriately identified and documented insights and assumptions from the shutdown PRA.

19.1.4.7.1.7 *Reduction of Risk Compared to Operating Plants*

Qualitative Improvements. For designs that have evolved from the technology of currently operating plants, the results of the PRA should indicate that the design represents a reduction in risk compared to operating plants. The U.S. EPR design-specific PRA demonstrates this risk reduction because of new design features, a conservative operational strategy, and additional TS requirements.

Design Features. The evaluation of FSAR Tier 2, Section 19.1.3 above provides a qualitative assessment of the ways that the U.S. EPR design has achieved this risk reduction, as presented in FSAR Tier 2, Table 19.1-2, "Features for U.S. EPR that Address Challenges for Current PWRs." Although none of these design features specifically relate to shutdown risk, many of them are applicable at shutdown as well as at power. Specific design features that reduce risk at mid-loop are identified in FSAR Tier 2, Section 5.4.7.2.1, as discussed in the previous section.

In addition, FSAR Tier 2, Table 19.1-102, lists the design features (such as automatic level control at mid-loop and closure of containment hatches during shutdown) that contribute most to the low shutdown risk estimated for the U.S. EPR design. These features were described above in the evaluation of FSAR Tier 2, Section 19.1.3. Because these features are critical to achieving the stated risk reduction, each table entry includes references to FSAR Tier 1, FSAR Tier 2, and COL information items where the feature is described in more detail, providing assurance that the as-built plant will match the as-designed plant.

The staff also observes that the four-train design of the U.S. EPR, as well as the requirements of the at-power TS, allow for significant maintenance to be performed while the plant is operating. As a result, the plant would be expected to shut down less often to perform system maintenance, reducing the frequency of shutdown and, thereby, shutdown initiating events. In

addition, less maintenance is expected to be needed during shutdown, meaning that more mitigation equipment will be available if an initiating event occurs. Therefore, on a qualitative basis, the U.S. EPR is expected to have a lower shutdown risk than currently operating plants.

Operational Strategy. Another important insight is the strategy of full-core offload during refueling outages. As described in FSAR Tier 2, Section 9.1.2 and 9.1.3, the SFP is designed to accommodate a full-core offload. In a September 25, 2008, response to RAI 26, Question 19-174 regarding the use of nozzle dams in the U.S. EPR steam generators at shutdown, the applicant stated that steam generator maintenance is expected to be performed at the 3/4 loop level with no fuel in the reactor vessel. Item 82 in FSAR Tier 2, Table 19.1-109, documents this assumption:

> Nozzle dams are not required during a plant shutdown, but may be used infrequently during mid-cycle maintenance, when full core off-load is not desirable. Appropriate RCS operating conditions will be considered in the specification of nozzle dams to provide reasonable assurance that nozzle dams will not fail.
>
> Plant procedures that cover reduced inventory operation will govern the installation of nozzle dams and the establishment of adequate venting to prevent pressurization of the RPV upper plenum due to a postulated loss of decay heat removal.

Although the shutdown PRA models mid-loop operation both with and without steam generators available, a realistic shutdown may require only draining the RCS just below the vessel flange so the vessel head can be removed. The steam generators could remain available until a large opening is made in the RCS. That is, the RCS level would be higher and more mitigating systems would be available than currently modeled. Therefore, the staff considers full-core offload an operational strategy that provides a significant reduction of risk compared to operating plants. Because the assumption is included in FSAR Tier 2, Table 19.1-109, the staff expects that COL holders implementing a different refueling strategy would update the PRA as needed to reflect the change.

TS Requirements. Finally, the addition of MODE 5 and 6 TS for MHSI and the IRWST provides for further risk reduction during shutdown, since unavailability of these systems would increase risk significantly. These systems are not included in the standard TS for operating plants; their inclusion represents an improvement in the suite of equipment that is available during shutdown, resulting in the low shutdown risk estimated by the U.S. EPR PRA.

Quantitative Improvements. The risk metrics discussed above also demonstrate a quantitative reduction in risk compared to current operating plants. The highest estimate of shutdown CDF provided by the applicant is a mean value of 9.9E-8/yr, including parametric uncertainty. In comparison, the staff estimated in SECY-97-168, "Issuance for Public Comment of Proposed Rulemaking Package for Shutdown and Fuel Storage Pool Operation," dated July 30, 1997, that shutdown CDF at PWRs implementing voluntary practices based on NUMARC 91-06 ranged from 8E-5/yr to 2E-6/yr. Additionally, the staff summarized various shutdown risk studies in SECY-00-0007, "Proposed Staff Plan for Low Power and Shutdown Risk Analysis Research to Support Risk-Informed Regulatory Decision Making," dated January 12, 2000. This paper included studies from Surry (5E-6/yr at mid-loop), Zion (1.8E-5/yr), and Seabrook (4.5E-5/yr). Finally, a generic PWR shutdown CDF of 5E-5/yr was estimated in NUREG/CR-5015, "Improved Reliability of Residual Heat Removal Capability in PWRs as Related to Resolution of Generic Issue 99," dated May 1988. Therefore, the U.S. EPR design, even when parameter

uncertainties are considered, represents a quantitative reduction in risk compared to current operating plants.

In addition, the SRP directs the staff to compare U.S. EPR risk to current operating plants' risk by initiating event category. A comprehensive comparison, such as that provided in Table 19.1-5, "Comparison of U.S. EPR Risk to IPE Results," of this report, for internal events at power, is not easily done for shutdown risk. Therefore, the staff examined various available studies. These studies define different initiating events, and often LOOP and support system failures are modeled as separate initiating events rather than part of the loss of RHRS as in the U.S. EPR PRA. However, some insights can be drawn from the information in SECY-00-0007. At Seabrook, loss of RHRS initiators contributed 82 percent of CDF (about 3.7E-5/yr), with LOCAs contributing the remaining 18 percent (about 8.1E-6/yr). For the U.S. EPR, both of the initiating events are major contributors to shutdown risk, but with lower absolute CDF values. The U.S. EPR shutdown PRA also considers uncontrolled level drops, which contribute about 30 percent of the shutdown CDF. An analysis of various LOCA scenarios caused by operator error at Sequoyah resulted in CDF estimates of 1E-7/yr to 8E-5/yr. For the U.S. EPR, the sum of the LOCA-initiated CDF estimates is lower, about 1.6E-8/yr. Therefore, the U.S. EPR contributions by initiating event are similar in relative terms and lower in absolute terms, with the additional initiator of uncontrolled level drops specifically analyzed.

Based on the information presented above, the staff concludes that the U.S. EPR shutdown PRA reflects a qualitative and quantitative reduction of risk compared to operating plants.

19.1.4.7.1.8 *Uncertainty, Importance, and Sensitivity Studies*

According to the SRP, the staff should consider the impact of data uncertainties on the risk estimates. In addition, the staff should review the applicant's risk importance studies to obtain insights about the systems, components, and human actions that contribute the most to the assessed risk, as well as the failures that contribute the most in achieving the low risk level assessed in the PRA. The staff should also review the applicant's sensitivity studies performed to determine (1) the sensitivity of the estimated risk to potential biases in numerical values, (2) the impact of the lack of detail, and (3) the sensitivity of the estimated risk to previously raised issues.

Impact of Uncertainty

Parameter Uncertainty. As discussed above, FSAR Tier 2, Figure 19.1-23 shows the effects of parameter uncertainty on the shutdown CDF estimate. Because of the state-of-knowledge correlation defined previously, the mean CDF (the risk metric requested in NRC guidance, as well as the ASME PRA standard) is about 75 percent higher than the point estimate CDF.

The applicant has taken a systematic approach to quantify uncertainty in the evaluation of U.S. EPR risk. FSAR Tier 2, Figure 19.1-23 shows that the shutdown CDF ranges from a 5th percentile value of about 5E-9/yr to a 95th percentile value of about 2E-7/yr. This range is broader than that of the at-power PRA, but the absolute values are less than 10 percent of the at-power CDF estimates. This distribution gives the staff confidence that the U.S. EPR CDF is within the Commission's CDF objective of 1E-4/yr.

Modeling Uncertainty. As discussed for the at-power PRA, modeling uncertainty is a significant issue at the design stage. The applicant made numerous assumptions when developing the shutdown PRA, both for convenience (e.g., defining discrete POS) and because of lack of knowledge (e.g., maintenance assumptions). Section 19.1.4.7.1.6 of this report,

describes the approach taken by the applicant to ensure that this modeling uncertainty is appropriately documented so that it can be addressed in the future. Modeling uncertainty is discussed below, as it was investigated by the applicant (via uncertainty cases) and the staff (via a screening approach). The evaluation of FSAR Tier 2, Section 19.1.4.1 above, provides a detailed discussion of additional sources of uncertainty that apply to the shutdown PRA as well.

Uncertainty Cases. As discussed above, the shutdown PRA uncertainty analysis does not include the modeling uncertainty cases performed for the at-power model. Cases 1 and 2, related to EFWS and feed-and-bleed success criteria are less important to the shutdown PRA results because of the lower decay heat at shutdown. In a July 11, 2008, response to RAI 14, Question 19-134, which requested that the applicant discuss the differences in modeling, assumptions, and equipment and operator dependencies that result in the different significance of HVAC failures to the shutdown PRA compared to the at-power PRA, the applicant clarified that HVAC failure events are less important in the shutdown PRA than in the at-power PRA, because LOOP and EFWS system function—both of which place demands on HVAC recovery—are less significant during shutdown. In a July 11, 2008, response to RAI 14, Question 19-135, which requested that the applicant provide an assessment of the impact on the shutdown PRA results of the HVAC modeling uncertainly case, the applicant provided the results of the HVAC uncertainty case, showing less than a 10 percent change in both the point estimate and mean CDF. The staff found the results of this analysis to be reasonable. Therefore, the staff concludes that the impact of the at-power modeling uncertainty cases on shutdown CDF is insignificant and does not affect the staff's conclusions about the design.

Failure Probabilities as Key Sources of Uncertainty. The staff also investigated which elements of the internal events at-power PRA could be considered key sources of uncertainty. Given that the CDF is about 6E-8/yr, this value would need to increase by a factor of more than 1,500 to challenge the 1E-4/yr CDF goal. Therefore, the failure probabilities of equipment and operator actions should be evaluated as potential key sources of uncertainty if the RAW value of the related basic event is above approximately 1,500.

The staff reviewed FSAR Tier 2, Tables 19.1-94 and 19.1-96 to 19.1-98 to determine which basic events exceed this RAW threshold. One operator action, isolation of the CVCS low pressure reducing station, has a RAW value greater than 1,500. Therefore, if the operator never performed this action when required, shutdown CDF could exceed the Commission's 1E-4/yr goal. In addition, several CCF basic events have RAW values greater than 1,500. Therefore, these failure probabilities could potentially be key sources of uncertainty, because CDF would exceed the 1E-4/yr goal if one of them were guaranteed to occur.

The staff then explored how high the failure probabilities for each of these identified basic events could increase before CDF would reach the 1E-4/yr threshold. In RAI 227, Question 19-285, the staff requested that the applicant provide the top 200 core damage cutsets for internal events, internal fire, internal flooding, shutdown, and the total at-power and shutdown model. On July 16, 2009, the applicant provided a response to this RAI. For each of these high-RAW basic events, the staff reviewed the top 200 cutsets from the shutdown model, provided by the applicant, to determine if the basic event appears. If not, the staff concluded that the failure would be unlikely to be a significant contributor to risk even if the probability were increased. If the basic event is included in one or more of the top 200 cutsets, the staff calculated approximately how large the failure probability would have to be for shutdown CDF to increase to 1E-4/yr. If the higher failure probability is too high to be plausible based on a comparison with available data, the probability is judged not to be a key source of uncertainty. If the failure

probability is plausible, then the basic event should be preserved as a potential key source of uncertainty.

In no case did the staff consider that the increased probability was plausible. Most of the probabilities would have to be greater than 0.1 for shutdown CDF to exceed 1E-4/yr. However, in four cases, the increased probabilities were too large to be realistic but small enough to warrant discussion, such that careful attention will be paid to these potential failures in the future. A list of these failures follows:

- **Operator failure to isolate the CVCS low pressure reducing station (OPE-ISOCSLPRS)**: A July 11, 2008, response to RAI 14, Question 19-142 regarding the accident sequences initiated by an uncontrolled level drop in various POS, provides a lengthy discussion of the operator failure to isolate the low-pressure reducing station. If level drops during shutdown (operator-induced or because of a spurious operation), the RHR pumps trip automatically, MHSI starts automatically, and the CVCS low-pressure reducing station is automatically isolated. If automatic letdown isolation fails and the operator does not manually isolate letdown via one of many valves, the SIS eventually pumps significant IRWST water out of containment through the letdown line and core damage is assumed. However, this operator action would have to increase to about 0.38 for shutdown CDF to exceed 1E-4/yr. The staff judges this HEP to be unreasonably high given the long time available to perform this action. Therefore, the staff concludes that modeling uncertainty associated with this operator action is unlikely to be a key source of uncertainty for the shutdown PRA.

- **CCF of IRWST sump strainers (JNK10AT001SPG_P-ALL)**: If all six of the IRWST strainers plug for a common cause (such as foreign materials left in containment or post-LOCA debris), no injection source drawing from the IRWST will succeed and a loss of inventory will lead to core damage. However, the CCF probability would have to increase to about 0.05 for shutdown CDF to exceed 1E-4/yr. Given that NUREG/CR-6928 lists a single-strainer plugging failure rate equivalent to a 1.7E-4 probability over 24 hours, the staff concludes that a CCF probability of 0.05 is too high to be reasonable. In addition, Item 14 in FSAR Tier 2, Table 19.1-109 indicates that IRWST design elements and plant procedures ensure that strainer plugging is unlikely, with reference to the relevant part of FSAR Tier 2, Chapter 6. Item 2 of FSAR Tier 2, Table 19.1-108 also provides the insight that these CCFs cause small LOCAs to the overall PRA results. Therefore, the staff concludes that modeling uncertainty associated with the IRWST strainer CCF probability is unlikely to be a key source of uncertainty for the shutdown PRA.

- **CCF of the LHSI and MHSI common injection check valves (JNG12AA004CFO_D-ALL)**: Similar to the IRWST strainers, if all four of the check valves that admit injection from LHSI and MHSI to the RCS fail to open, injection fails and a loss of inventory will lead to core damage. The CCF probability would have to be about 0.03 for internal events CDF to exceed 1E-4/yr. NUREG/CR-6928 estimates a failure probability of 1.3E-5 for a single check valve to open. Even if infrequent testing of these valves means that standby failures are more likely than estimated in NUREG/CR-6928, a CCF probability for all four valves of 0.03 is too high to be reasonable. Therefore, the staff concludes

that modeling uncertainty associated with the common injection check valve CCF probability is unlikely to be a key source of uncertainty for the shutdown PRA.

- **CCF of the safety-related batteries (BTD01_BAT__ST_D-ALL)**: If all four of the safety-related batteries fail after a LOOP, the PRA assumes that core damage results, because no instrumentation will be available to the operators. For shutdown CDF to exceed 1E-4/yr, the battery CCF probability must increase from 2.9E-7 to about 0.06. Given that the failure probability for a single battery is estimated as 5E-4 in the ALWR URD and 6.6E-4 in the PRA, a CCF probability of 0.06 is too high to be reasonable. In addition, FSAR Tier 2, Table 19.1-109 states the importance of this failure in Item 18 and the assumption of frequent monitoring in Item 27. Therefore, the staff concludes that modeling uncertainty associated with these batteries is not likely to be a key source of uncertainty for the shutdown PRA.

Risk Importance Studies

As discussed previously, risk importance studies address the following two general objectives: Risk reduction and reliability assurance. To meet these two objectives, the applicant evaluated the risk importance of failures in the PRA and provided lists of all failure events with FV values greater than 0.005 or RAW values greater than 2 in FSAR Tier 2, Tables 19.1-93 through 19.1-98, as supplemented by a July 11, 2008, response to RAI 14, Question 19-126 on the significant equipment and operator actions for all elements of the U.S. EPR design-specific PRA. These failures are considered “significant” by the ASME PRA standard.

Risk Reduction. FV importance is the fraction of the total risk that is associated with an SSC or operator action. This importance measure can be used to identify SSCs that would benefit the most from improved testing and maintenance to minimize equipment unavailability and failures.

A selection of the risk-significant failures presented by the applicant (only those with an FV importance of more than five percent) follows:

- Failure of a single EDG. LOOP is a significant initiating event for the U.S. EPR, and EDG failures appear in cutsets that contribute about 30 percent of the shutdown CDF.

- Failure of the operator to isolate the CVCS low-pressure reducing station. Operator action is important following an uncontrolled level drop, and this human error appears in cutsets that contribute about 25 percent of the shutdown CDF.

- Failure of a single SIS cold leg isolation check valve. This failure would disable a train of safety injection, and appears in cutsets that contribute about 25 percent of the shutdown CDF.

- Failure of a CVCS low-pressure reducing station isolation MOV. Closure of this MOV is important following an uncontrolled level drop, and failure of the MOV appears in cutsets that contribute about 25 percent of the shutdown CDF.

- Failure of a single SBODG. LOOP is a significant initiating event for the U.S. EPR, and SBODG failures appear in cutsets that contribute about 20 percent of the CDF.

- Failure of the operator to isolate an RHR flow diversion in POS CB. This failure appears in cutsets that contribute about 20 percent of the CDF.

- Failure of the operator to isolate an uncontrolled level drop. Operator action is needed to isolate a level drop before the RHRS pumps cavitate, and this human error appears in cutsets that contribute about 10 percent of the CDF.

- Failure of the operator to isolate an RHR flow diversion in POS D. This failure appears in cutsets that contribute less than 10 percent of the CDF.

This list of failures suggests that risk could be reduced by implementing design or operational changes related to electrical equipment (EDGs and SBODGs) and the SIS injection check valves. In addition, improvements to procedures, training, cues, or other human factors contributors that would reduce the likelihood of the human errors listed could have an impact on overall risk. Particularly, isolation of the CVCS low-pressure reducing station is an important human action that should be considered in the human factors analysis. However, given the low CDF reported above, even when uncertainty is included, it is likely that design changes would need to be justified based on deterministic as well as probabilistic considerations.

Reliability Assurance. RAW is the factor by which CDF increases when an SSC or operator action is assumed not to be there or to be failed (event probability is assumed to be one). RAW values help to identify important design features and assumptions that contribute to the "low risk" of the design. These features and assumptions should be captured in requirements to ensure that the risk remains low when such a plant is built and operated. In addition, the RAW importance measure is useful in identifying areas that need particularly good maintenance and training, since poor reliability of this equipment or frequent human errors would significantly increase the CDF estimate.

A selection of the risk-significant failures presented by the applicant (only those with a RAW value of more than 20) follows:

- All 26 CCFs listed in FSAR Tier 2, Tables 19.1-97 and 19.1-98. Common-cause failures remove the benefits of four-train redundancy by failing multiple trains at once. If they are certain to occur, as the RAW value reflects, an entire safety function may be lost. In addition, much of this equipment is assigned an extremely low CCF probability. Therefore, when this probability is set to 1.0, the relative change in CDF is much higher than that for a lower-reliability set of equipment.

- Failure of the operator to isolate the CVCS low-pressure reducing station. This action is needed to mitigate an uncontrolled level drop. If the operator always failed to take this action, shutdown CDF would increase by a factor of about 4,500.

- Failure of the operator to start maintenance HVAC trains after safety-related trains fail. An unrecovered failure of certain HVAC components can lead to multiple failures. Overall shutdown CDF would increase by a factor of about 100 if the operator never started maintenance HVAC trains when needed.

- Failure of a single 480V load center. Shutdown CDF would increase by a factor of about 50 if the load center were always certain to fail.

- Failure of a single 6.9kV switchgear. Shutdown CDF would increase by a factor of about 50 if the switchgear were always certain to fail.

- Failure of a single 480V MCC. Shutdown CDF would increase by a factor of about 40 if the load center were always certain to fail.

The list of failures suggests that special attention should be paid to any activities or design changes that could increase the likelihood of a CCF, because the low risk of the plant depends strongly on redundant equipment and low CCF probabilities. In addition, maintenance on the 6.9 kV switchgear and 480V load centers and MCCs should be of high quality to ensure that failure probabilities do not increase above those assumed in the PRA. Finally, operator training should appropriately emphasize isolation of the CVCS low-pressure reducing station and starting maintenance HVAC trains when needed, such that HEPs will remain as low as assumed in the PRA.

Sensitivity Studies

As outlined above, the applicant performed multiple sensitivity cases to evaluate the impact of modeling assumptions on the shutdown CDF. Based on these studies, the applicant concluded that the results are sensitive to HEP values, electrical power assumptions, and assumptions about operator recovery of HVAC.

None of these sensitivity cases resulted in a CDF point estimate more than an order of magnitude higher than the baseline estimate. In a sensitivity case that placed all diesel generators in the same CCF group, shutdown CDF approximately quadrupled, to 2.4E-7/yr. For all of the sensitivity cases, even if the mean value were an order of magnitude higher because of the state-of-knowledge correlation, the CDF estimate is still expected to be below 1E-4/yr. Therefore, the staff is confident that the U.S. EPR CDF is within the Commission's CDF objective.

Based on the information presented above, the staff concludes that the applicant has sufficiently evaluated uncertainties in the shutdown PRA, in part by performing sensitivity studies, and identified important equipment and operator actions.

19.1.4.7.1.9 *Assumptions During Design Certification*

The staff must ensure that the assumptions made in the applicant's PRA during design certification are identified such that they can be addressed by COL applicants. COL Information Item 19.1-9 addresses this topic, specifically mentioning a need to examine LPSD procedures.

The key assumptions in FSAR Tier 2, Section 19.1.6.2.5 are summarized as follows:

- POS CA_{d1}, CA_{d2}, and CA_{d3} are analyzed as a single POS.

- The decrease in decay heat over time is not considered in the time-to-TAF calculation.

- Maintenance on two SGs is assumed in POS CA_d and CB_d, and maintenance on all other systems (one division at a time) is assumed to occur in POS E.

- The charging system is assumed unavailable, even though it may be available in POS CA_d and CB_d.

- IRWST cooling is assumed unnecessary when the RPV head is off. It takes more than 3 days to boil off the IRWST if condensed steam is not returned to the tank.

- LOCAs through the RPV and pressurizer vents are not modeled. The pressurizer vent is normally open during shutdown, and the RPV vent is open at mid-loop and during startup. Because the pressurizer vent contains a flow restrictor, loss of inventory would be below the CVCS makeup capacity. The RPV vent is a 2.54 cm (1 in.) line, and operators would have significant time to isolate the vent or provide makeup before the core would be uncovered.

- Three of three PSRVs are required for feed and bleed, although two of two are expected to be adequate before refueling and one of two adequate after refueling.

- Transient-induced LOCAs require feed-and-bleed cooling for success, because the break size may not be large enough to provide sufficient bleed.

- The IRWST suction strainer plugging probability was not increased relative to the at-power model. The IRWST design and plant procedures (e.g., foreign material control) are expected to ensure that this probability is low.

- LTOP events when the pressurizer is solid are not modeled. As discussed above, the applicant provided additional information on this initiating event in an April 30, 2008, response to RAI 2, Question 19-14, which requested that the applicant provide justification for not including low temperature overpressure (LTOP) events, and an August 15, 2008, response to RAI 26, Question 19-181 regarding the mass or energy input that would cause the LTOP PSRV to open when the RCS is water-solid during shutdown. The assumption is preserved as Item 54 in FSAR Tier 2, Table 19.1-109.

Other areas for which modeling is not complete or for which assumptions have been made (such as HVAC recovery times, I&C details, calibration errors, and cooldown operator actions) are in different locations in Chapter 19. As a result of RAI 26, Questions 19-166 and 19-167 on the documentation of PRA assumptions and insights, the FSAR now includes Table 19.1-109, a list of the most important PRA assumptions (described in more detail above). In a May 30, 2008, response to RAI 2, Question 19-38 regarding the strategy of communicating PRA assumptions to the COL applicants, the applicant stated that it would be responsible for maintaining and updating the U.S. EPR design-specific PRA during the design and construction phases until ownership is transferred to the COL holder, no later than the time of the first fuel load, when the PRA must be fully updated. The documentation that is supplied to the COL holder at that time, in addition to the content in the FSAR, is the principal means of communicating all assumptions in the PRA. Before then, assumptions will be communicated as they relate to other efforts, such as the development of emergency procedures. The applicant states that PRA staff will be involved with procedure development to ensure PRA insights and assumptions are considered.

The staff concludes that the documentation of assumptions in the FSAR is sufficient to ensure that they will remain valid for the as-built, as-operated plant. Any changes to these assumptions will be incorporated in the PRA as part of the PRA maintenance process described above in the evaluation of FSAR Tier 2, Section 19.1.2. Addressing COL Information Item 19.1-9, to which FSAR Tier 2, Table 19.1-109 refers, is the responsibility of the COL holder.

19.1.4.7.2 FSAR Tier 2, Section 19.1.6.2: Level 2 PRA for Other Modes of Operation

The applicant's Level 2 PRA analysis of shutdown conditions takes the results of the at-power Level 2 PRA and applies them, with appropriate assumptions, to the results of the shutdown PRA analysis. This approach is intended to be bounding for the low power/shutdown conditions, for both the release category frequencies and for the severity of the source terms expected from accidents initiated from the low power or shutdown states.

The LPSD PRA includes several plant operating states (POS A to F) to represent plant and system configurations during shutdown evolutions. In the shutdown condition, the plant operating state is characterized by low pressure in the primary system. Two POS states are analyzed as power states: POS A (full power to hot standby) and POS B (hot standby to hot shutdown). The applicant's analysis of these follows the at-power internal events methodology.

In POS E (fuel load) the cavity is flooded, the RPV head is off, and the containment is open. POS F has the core off-loaded and is not analyzed in the Level 2 PRA.

In POS C, the RPV head is on the vessel, and the RCS is intact. This makes the primary system vulnerable to re-pressurization after core melt. The PSRV setpoint is reduced to 3.723 MPa (540 psi) to protect the RPV from cold over-pressurization events. This lower set point effectively eliminates temperature-induced creep rupture of hot legs and steam generator tubes, and reduces the probability of events associated with high-pressure melt ejection, such as DCH and RPV rocketing.

The transient initiating event was chosen as the core damage event that would most closely model the phenomenology and containment failure modes that would occur in State C. This non-LOCA initiating event reflects the fact that the primary system is intact and that it is possible to re-pressurize the primary system during the shutdown severe accident scenario. The results of the at-power analysis are modified to accommodate the changes in the severe accident phenomenology expected.

In POS D, the RPV head is removed, and the primary system remains at low pressure throughout the core melt and containment failure scenario.

The large LOCA initiating event was chosen as the core damage event that would most closely model the phenomenology and containment failure modes that would occur in Plant Operating State D. This plant operating state did not call for alteration of the at-power Level 2 PRA results in order to use the conditional failure probabilities for each RC.

The applicant's basic approach was to determine the frequencies of all of the non-ISLOCA release categories by calculating the conditional probability of each of the release categories from the chosen CDES. The key assumptions were:

- The ISLOCA sequences in POS C and D are directed to RC802. Since the source term is based on power operation, this is deemed conservative.

- The total CDF during POS E (equipment hatch off and not isolated) is directed to RC205 (at power large loss of containment isolation without SAHRS sprays). Since the source term is based on power operation and neither isolation nor SAHRS sprays are credited, this is deemed conservative.

- The source term used for each of the shutdown release categories (RCs) is the same as that reported in the at-power Level 2 analysis.

The conditional probabilities for the RCs were based on the full power analysis with some adjustments.

The applicant reviewed the accident sequences occurring at full power to identify relevant phenomena during shutdown scenarios. The principal phenomena considered include those associated with induced RCS rupture and hydrogen combustion. Although having a lower probability than during severe accidents at full power, induced SGTR was retained in the containment event tree model.

Hydrogen combustion loads were assessed based on the global AICC pressure. Flame acceleration loads were assessed using conservative gas mixing properties. The conditional probability of containment failure from hydrogen flame acceleration was estimated to be 0.032. The staff considers the applicant's approach to evaluating the phenomenology to be well-represented and appropriately conservative. System unavailabilities and configurations can affect the frequencies of some RCs, so some bounding analysis is appropriate. The staff reviewed the case chosen and finds it reasonable. The system failure probabilities in the Level 2 PRA model were not rigorously assessed for the shutdown-specific spectrum of core damage sequences.

19.1.4.7.3 LPSD Level 2 Results and Insights

The applicant calculated the LRF for LPSD operation as 5.7E-9/yr. The CCFP based on large release in POS C is 0.10 and in POS D is 0.026. In POS E (fuel load) the containment is open so that the conditional containment failure probability is unity. 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 RCs were found to lead to large release – RC201 through RC205, RC301 through RC304, RC702, and RC802. Even though the release fractions for RC206 in Plant Operating State D (FSAR Tier 2, Table 19.1-115) exceeds the guidelines for Large Release for iodine (I), cesium (Cs), and tellurium (Te), the applicant did not consider this as a large release because of the conservative nature of the process used for the estimation of release fractions with the primary system open.

A Level 2 PRA sensitivity analysis was performed to evaluate the impact of general modeling assumptions, with results very similar to the Level 1 PRA sensitivity analysis reported for CDF results.

The staff agrees with the applicant that the results of the Level 2 PRA analysis for shutdown states show that the containment is robust for severe accident phenomenological failures in shutdown conditions.

A majority of the LRF in POS C comes from the Interfacing LOCA contributions of RC802, and from containment isolation system contributions of RC201 through RC205. The remaining contributions are from containment failures before vessel rupture. In POS D, 42 percent of the contribution to LRF comes from Interfacing System LOCA, and 58 percent from RC201 through RC205. In POS E, 68 percent of LRF contributions come from RC802, with the remaining coming from RC201 through RC205.

For the non-ISLOCA Release Categories in POS C and D, the distribution of frequencies is comparable with the distribution seen in the Internal Events at-power analysis. The probabilities

for early containment failure are extremely low, as would be expected. The low pressure nature of POS D makes the induced SGTR (bypass) and high energy early containment failure modes highly unlikely.

Failures due to hydrogen combustion in the very early phases contribute less than in the at-power sequences, because the concentration of hydrogen in the pressurizer quench tank room is not seen in the low pressure sequences in POS D.

The sum of the LRF for all shutdown POSs is about 17 percent of the total (internal events, floods, fire and shutdown) LRF, verifying that shutdown states are small contributors to the overall LRF.

The applicant's analysis of shutdown conditions takes the results of the at-power level 2 PRA and applies it to the results of the shutdown PRA analysis. The applicant states that this approach is bounding for both the release category frequencies and for the severity of source terms. The staff needed to see support for this claim, so it issued RAI 22, Question 19-158, requesting that the applicant justify that the approach is bounding for the severity of source term, given that during shutdown conditions the reactor vessel is open, and air intrusion into the fuel assembly would enhance oxidation that can result in some fission products (most notably Ru (ruthenium)) transforming into more volatile valence states.

In a November 4, 2008, response, the applicant discussed the various combinations of RCS status, containment status, RCS inventory, and decay heat to determine the impact on accident progression and fission product releases. The applicant pointed to the MAAP limitations in addressing the evolution of such accidents and resulting source terms. In addition, FSAR Tier 2, Revision 1, Section 19.1.6.3 was expanded to include additional information on the assumptions on release frequencies and the associated source terms.

Generally, the applicant's discussions are satisfactory in addressing the RAI concerns. However, the discussion of the impact of air ingression on volatization of Ruthinium (Ru) references outdated reports to dismiss the potential for air ingression and volatization of Ru oxides. Nonetheless, the statement that "the phenomenon of air ingress and evolution of ruthenium oxides is not expected to affect the determination of Large Release Frequency (LRF)" may be accurate; however, the response does not address the potential impact of increased Ru release on the risk of early and latent fatalities, which could be important. The staff determined that an expanded discussion of the risk implication of air ingression and enhanced release of Ru should be included in the FSAR. The staff further determined that the potential impact of enhanced Ru on early and latent fatalities (as compared to the Commission's safety goals) should also be included through sensitivity calculations that consider increased Ru releases. Accordingly, the staff issued RAI 349, Question 19-333, requesting that the applicant provide additional information regarding air ingression and enhanced Ru release, and sensitivity calculations on the potential impact of increased Ru releases on early and latent fatalities. **RAI 349, Question 19-333, which is associated with the above request, is being tracked as an open item.**

19.1.4.8 *FSAR Tier 2, Section 19.1.7: PRA-Related Input to Other Programs and Processes*

As explained at the beginning of Section 19.1.4 of this report, the staff finds that the applicant appropriately described how the U.S. EPR design-specific PRA is used in the design process, in FSAR Tier 2, Sections 19.1.1.1 and 19.1.3.4.

The applicant does not use the PRA to support the reactor oversight process and Maintenance Rule implementation at the design certification stage. However, the assessment of PRA importance measures is used to provide input to the RAP. The PRA results from both Level 1 and Level 2 assessments are used for identifying the SSCs that are potentially risk-significant. The staff's complete evaluation of the U.S. EPR RAP is provided in Section 17.4 of this report.

As stated in FSAR Tier 2, Sections 19.1.1.1 and 19.1.1.4, the COL applicant will describe the uses of PRA in support of licensee programs such as the site-specific design process, reactor oversight process, and RAP implementation during the operational phase.

The U.S. EPR design is an LWR evolutionary design with no passive backup systems, thus the applicant need not address the RTNSS process.

Based on the foregoing, the staff concludes that the applicant has made proper use of the U.S. EPR PRA results and insights as an input to other programs and processes such as ITAAC, RAP, and COL information items as discussed in Chapters 17 and 19 of this report.

19.1.4.9 *FSAR Tier 2, Section 19.1.8: Conclusions and Findings*

Conclusions for FSAR Tier 2, Section 19.1 are provided in Section 19.1.6 below:

The calculated CDF, LRF and CCFP values for all at-power internal, fire, and flood events are listed in Table 19.1-19 of this report. The LPSD results are discussed separately above in the evaluation of FSAR Tier 2, Section 19.1.6.1.2.

Table 19.1-19 Risk Metrics for All Internal, Fire, and Flood Events

Risk Metric	Point Estimate	Quantile		
		Mean	5th percentile	95th percentile
CDF	5.3E-7/yr	7.4E-7/yr	8.7E-8/yr	2.0E-6/yr
LRF	2.6E-8/yr	3.6E-8/yr	7.1E-10/yr	1.1E-7/yr
CCFP	0.05	0.05	--	--

The point estimate contributions to the total LRF are 83 percent due to internal events, 13 percent due to fires, and 4 percent due to flood initiators. The total contribution of early containment failures to LRF is approximately 75 percent.

Both the point estimate and the 95th percentile LRF values (2.6E-08/ry and 3.6E-08/ry, respectively) are below the NRC goal and the U.S. EPR probabilistic design goal of 1E-6/yr.

The point estimate CCFP for large release sequences from internal events, internal flooding events, and internal fire events at power is 0.05, below the objective of 0.10.

Interestingly, the overall CCFP is numerically lower than the internal events-only value (0.076). This is a result of the CDF increasing proportionately more than the LRF when the three types of hazards (i.e., internal events, internal flooding, and internal fire) are summed.

19.1.5 Combined License Information Items

Table 19.1-20 of this report lists the combined license information items applicable to FSAR Tier 2, Section 19.1. These item numbers and descriptions in this table are taken from FSAR Tier 2, Table 1.8-2, "U.S. EPR Combined License Information Items."

Table 19.1-20 Combined License Information Items

Item No.	Description	FSAR Tier 2 Section	Action Required by COL Applicant	Action Required by COL Holder
19.0-1	A COL applicant that references the U.S. EPR design certification will either confirm that the PRA in the design certification bounds the site-specific design information and any design changes or departures, or update the PRA to reflect the site-specific design information and any design changes or departures.	19.0	Y	
19.1-1	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.	19.1.1.2	Y	
19.1-2	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.	19.1.1.3	Y	
19.1-3	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 any risk-informed applications being implemented during the operational phase.	19.1.1.4	Y	
19.1-4	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.	19.1.2.3		Y

Item No.	Description	FSAR Tier 2 Section	Action Required by COL Applicant	Action Required by COL Holder
19.1-5	A COL applicant that references the U.S. EPR design certification will describe the applicant's PRA maintenance and upgrade program.	19.1.2.4	Y	
19.1-6	A COL applicant that references the U.S. EPR design certification will confirm that the design-specific U.S. EPR PRA-based seismic margins assessment is bounding for their specific site.	19.1.5.1.2.4	Y	
19.1-7	A COL applicant that references the U.S. EPR design certification will perform the site-specific external event screening analysis for external events applicable to their site.	19.1.5.4	Y	
19.1-8	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.	19.1.1.1	Y	
19.1-9	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 SAMDA) remain valid with respect to internal events, internal flood and fire events (routings and locations of pipe, cable and conduit), and HRA analyses (development of operating procedures, emergency operating procedures and severe accident management guidelines and training), external events including PRA-based seismic margins HCLPF fragilities, and LPSD procedures.	19.1.2.2		Y

19.1.6 Conclusions

Because of the open items and the nature and extent of the confirmatory items identified in the text, the staff is currently unable to come to an overall conclusion on FSAR Tier 2, Section 19.1.

19.2 Severe Accident Evaluations

19.2.1 Introduction

This section of the design certification FSAR describes the approach taken by the applicant to resolve severe accident issues for the U.S. EPR design. In addition, the 10 CFR 50.34 (f)(1)(i) requirement that a plant-specific PRA be performed in order to seek improvements in the reliability of core and containment heat removal systems is addressed in Section 19.2.6 of the application.

19.2.2 Summary of Application

FSAR Tier 1: The following FSAR Tier 1 sections provide information on systems that are designed to mitigate a severe accident and are referred to in this FSAR section:

- Section 2.3.1 Combustible Gas Control System
- Section 2.3.2 Core Melt Stabilization System
- Section 2.3.3 Severe Accident Heat Removal System
- Section 2.4.14 Hydrogen Monitoring System

FSAR Tier 2: The applicant has provided FSAR Tier 2 description of the severe accident evaluation, summarized here in part, as follows.

The design features used to prevent and mitigate severe accidents are described in FSAR Tier 2, Section 19.2. Reference is made to AREVA NP Topical Report ANP-10268P (approved in an SER dated November 29, 2007), "U.S. EPR Severe Accident Evaluation," and computer code description as its analysis methodology and approach for resolving the severe accident issues.

The application addresses the five severe accident scenarios identified in Appendix A of SRP Chapter 19.0 (NUREG-0800), as follows:

1. Design measures for prevention of ATWS events include diverse scram actuation; mitigation features include automatic start of EFWS and availability of the EBS.

2. Decay heat removal system reliability, visible and audible indications, and provisions for preventing damage to heat removal pumps are identified as the means for preventing mid-loop operations events from causing loss of inventory or heat removal.

3. Availability of the SBODG is identified as the means for coping with the occurrence of an SBO event.

4. Protection against fires is described in terms of safety system availability to safely shutdown and maintain inventory and heat removal capability in the event of a fire.

5. According to the FSAR section, prevention of ISLOCA events is achieved through design of connected systems to at least full reactor coolant system pressure.

The application describes the U.S. EPR Containment Building design and the containment systems used for accident mitigation: The combustible gas control system (CGCS), core melt

stabilization system (CMSS), severe accident heat removal system (SAHRS), and hydrogen monitoring system (HMS).

The fundamental strategy employed by the U.S. EPR for accident mitigation is based on ex-vessel containment of core debris. The FSAR provides a detailed description of the progression of a hypothetical severe accident, including in-vessel fuel melt due to failure of all active injection systems, lower vessel head failure, molten core-concrete interaction inside containment, hydrogen generation, molten core stabilization, and cooling. The mitigating actions of the above-mentioned severe accident systems are described in the context of the accident progression.

Special cases of high pressure melt dispersal, fuel-coolant interaction, and containment bypass scenarios are also described, for which equipment survivability and containment venting are addressed.

As described in the FSAR, the CGCS limits the amount of hydrogen within the containment through passive recombination with oxygen, thus reducing the chance of combustion. At the controlled hydrogen levels, a global deflagration is calculated to be within the containment design capacity, and the risk of detonation is described as negligible.

Retention and coolability of ex-vessel core debris is reported by the applicant as being achieved by the CMSS. Following escape from the reactor vessel, the core melt is temporarily retained in the reactor cavity, following which the core melt relocates to the spreading compartment for cooling and long-term stabilization. Cooling of the core melt is provided by the SAHRS.

The FSAR states that the possibility of high pressure melt ejection is precluded from occurrence by the U.S. EPR design features. Similarly, the possibility of a steam explosion leading to containment failure is reported to be very small, based on probabilistic arguments.

The FSAR states, in summary, that the integrity of U.S. EPR containment is maintained for at least 24 hours following the onset core damage, and the CCFP is 0.076.

The FSAR describes the U.S. EPR severe accident management strategy in terms of an OSSA framework whose goal is to prevent or reduce all radiological release to the environment. The OSSA was developed by the applicant as a new approach to the severe accident management guidelines.

The interface of OSSA with the plant Emergency Operating Procedures (EOPs) is described, along with operator action for primary system depressurization. A summary of both short-term and long-term (12 hours after depressurization) actions is provided, concluding with the definition of melt stabilization and consideration of remediation.

As described in the FSAR, potential design improvements were identified from published industry documents and from a review of the top one hundred Level 1 PRA event scenarios. The resulting severe accident mitigation design alternatives (SAMDAs) were then screened against a set of seven criteria. Of the total 167 SAMDAs identified, none were selected for implementation. The applicant concludes that the U.S. EPR has a very low probability of core damage, and coupled with its severe accident mitigation design features provides significant protection to the public and the environment.

ITAAC: ITAAC items for this area of review are identified in the following FSAR Tier 1 tables:

- Table 2.3.1-2—CGCS Inspections, Tests, Analyses, and Acceptance Criteria
- Table 2.3.2-1—CMSS Inspections, Tests, Analyses, and Acceptance Criteria
- Table 2.3.3-3—SAHRS Inspections, Tests, Analyses, and Acceptance Criteria
- Table 2.4.14-2—Hydrogen Monitoring System ITAAC

Technical Specifications: There are no Technical Specifications for this area of review.

19.2.3 Regulatory Basis

The relevant requirements of the Commission regulations for this area of review, and the associated acceptance criteria, are given in Section 19.0 (Part II) of NUREG-0800 and are summarized below. Review interfaces can be found in Section 19.0 (Part I) of NUREG-0800.

Requirements and guidance for this chapter are included in 10 CFR, Section 52.47(a), and various NRC documents.

The relevant regulatory requirements are:

1. 10 CFR 52.47(a)(8) provides the information necessary to demonstrate compliance with any technically relevant portions of the TMI requirements set forth in 10 CFR 50.34(f), except paragraphs (f)(1)(xii), (f)(2)(ix), and (f)(3)(v).

2. 10 CFR 52.47(a)(23) provides a description and analysis of design features for the prevention and mitigation of severe accidents.

3. 10 CFR 52.47(b)(1) requires that a design certification application contain the proposed ITAAC that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act, and NRC regulations.

4. 10 CFR 50.44(c) requires combustible gas control for new reactors during design-basis and significant beyond design-basis accidents. 10 CFR 50.44(c)(1) requires that all containments must be capable of ensuring a mixed atmosphere. 10 CFR 50.44(c)(2) requires that all containments must either be inerted during normal operation or must limit hydrogen concentrations to less than 10 percent by volume. 10 CFR 50.44(c)(3) requires that containment designs that do not rely on an inerted atmosphere must be able to establish and maintain safe shutdown and containment structural integrity with systems and components capable of performing their functions during and after hydrogen combustion events. 10 CFR 50.44(c)(4)(ii) requires that equipment be provided for continuous monitoring of hydrogen in the containment building for accident management, including emergency planning. 10 CFR 50.44(c)(5) requires that the applicant must perform an analysis that demonstrates containment structural integrity. The analysis must address an accident that releases hydrogen generated from 100 percent fuel clad-coolant reaction accompanied by hydrogen burning. Systems necessary to ensure containment integrity must also be demonstrated to perform their functions under these conditions.

Acceptance criteria adequate to meet the above requirements are set forth in NRC guidance documents, as follows:

1. Commission papers (and associated SRM) SECY-90-016, SECY-93-087, and SECY-97-044, which provide guidance pertaining to features in new designs for preventing and mitigating the effects of severe accidents. In particular, guidance is provided on preventive features related to Anticipated transient Without Scram (ATWS), Mid-Loop Operations, Station Blackout, Fire Protection, and Intersystem LOCA, and on mitigative features related to hydrogen generation and control, core debris coolability, high-pressure core melt ejection, containment performance, and equipment survivability.

2. NRC Policy Statements: 50 FR 32138 (Section B on Policy for New Plant Applications), 59 FR 35461 (section stating Commission policy), and 60 FR 42622 (section stating Commission policy).

3. RG 1.70, Revision 3, "Standard Format and Content of Safety Analysis Report for Nuclear Power Plants," issued November 1978, provides guidance for meeting the 10 CFR 50.44(c)(5) requirement and specifies the following:

    - Steel containments meet the requirements of the ASME Code (edition and addenda as incorporated by reference in 10 CFR 50.55a(b)(1)), Section III, Division 1, Subarticle NE-3220, "Service Level C Limits," considering pressure and dead load alone (evaluation of instability is not required).

    - Concrete containments meet the requirements of the ASME Boiler and Pressure Vessel Code, Section III, Division 2, Subarticle CC-3720, "Factored Load Category," considering pressure and dead load alone.

    - At a minimum, the specific ASME Code requirements set forth for each type of containment will be met for a combination of dead load and an internal pressure of 310.3 kPa (45 psig).

4. SECY-93-087 and the Commission's SRM provide guidance for meeting the deterministic containment performance goal (CPG) in the evaluation of the passive ALWRs as a complement to the CCFP approach. The SECY-93-087 guidance with respect to the deterministic containment performance assessment is described as follows:

    - The containment should maintain its role as a reliable, leaktight barrier (e.g., by ensuring that containment stresses do not exceed ASME Service Level C limits for metal containment or factored load category for concrete containments) for approximately 24 hours following the onset of core damage under the most likely severe accident challenges, and following this period, the containment should continue to provide a barrier against the uncontrolled release of fission products.

19.2.4 Technical Evaluation

19.2.4.1 *FSAR Tier 2, Section 19.2.1: Introduction*

The applicant's description and analysis of the design features to prevent and mitigate severe accidents, in accordance with the requirements in 10 CFR 52.47(a)(23) is reviewed. This

review covered specific issues identified in SECY-90-016 and SECY-93-087, which the Commission approved in related SRMs dated June 26, 1990, and July 21, 1993, respectively, for prevention (e.g., ATWS, mid-loop operation, SBO, fire protection, and interfacing system LOCA) and mitigation (e.g., hydrogen generation and control, core debris coolability, high-pressure core melt ejection, containment performance, dedicated containment vent penetration, equipment survivability).

In addition, information provided by the applicant to satisfy the requirements of 10 CFR 52.47(a)(8) was also reviewed.

19.2.4.2 *FSAR Tier 2, Section 19.2.2: Severe Accident Prevention*

A summary of important features aimed at preventing the onset of severe accidents has been provided in the evaluation of FSAR Tier 2, Section 19.1.3.1.

19.2.4.2.1.1 *Anticipated Transients Without Scram*

For ATWS prevention and mitigation, the U.S. EPR is designed with the following features:

- A diverse actuation scram system with an independent reactor shutdown signal
- Automatic actuation of emergency feedwater under conditions indicative of an ATWS
- An extra borating system independent of the reactor protection system that can be used (manual initiation) to inject heavily borated water to safely shutdown the reactor

The effectiveness of these design features for addressing ATWS concerns has been evaluated in FSAR Tier 2, Section 15.8. Given these features, the U.S. EPR design-specific PRA demonstrated that ATWS provides an insignificant contribution to CDF. Note that in regard to LRF, the contribution is large (i.e., the steam line break inside containment followed by uncontrolled reactivity due to cooldown contributes approximately 75 percent of the approximately 57 percent contribution of ATI to LRF, as indicated in FSAR Tier 2, Table 19.1-26 and RC304 cutsets in FSAR Tier 2, Table 19.1-25).

19.2.4.2.1.2 *Mid-loop Operations*

During refueling or maintenance activities, the reactor coolant system is sometimes partially drained to a “mid-loop” level. The U.S. EPR design features for improved safety during shutdown and mid-loop operation include the following:

- Provisions for availability of reliable systems (four redundant safety related trains) systems for decay heat removal.
- Reactor pressure vessel water level instrumentation to provide reliable measurement of liquid levels in the vessel.
- Provision to prevent damage to the RHRS pump due to overheating or loss of adequate pump suction head.

- Instrumentation to provide reliable measurements to initiate RCS makeup (hot leg level sensor).

- Operational and procedural measures to provide reasonable assurance that the RCS remains stable. These measures include both preventing a loss of RHRS and enhanced monitoring criteria for timely response to a loss of RHRS.

- Provisions for maintaining containment closure or for rapid closure of containment openings.

The effectiveness of RHRS in mid-loop operation and the provision to prevent boron dilution during mid-loop operations are described in FSAR Tier 2, Sections 5.72 and 15.4, respectively.

19.2.4.2.1.3 *Station Blackout*

During a total LOOP, the safety-related electrical distribution system is powered from the onsite non-safety-related DGs. The U.S. EPR design, in accordance with the guidance in RG 1.155, "Station Blackout," includes two separate and independent SBO diesel generator units capable of powering at lease one complete set of the shutdown loads for 8 hrs. In the case of loss of all ac power including the SBO diesel generator units, then each division of the safety-related system independently isolates itself from the non-safety-related system, and uninterrupted power to safety-related loads of each safety-related load division is provided by the safety-related batteries of each division. Critical plant loads are then supported by a 12-hr non-class 1E battery until an ac power source can be recovered. Conformance of SBO DG units to the requirements of 10 CFR 50.63 is documented in the FSAR Tier 2, Section 8.4, "Station Blackout."

19.2.4.2.1.4 *Fire Protection*

The fire protection system (FPS) does not perform any safety-related function. The FPS serves as a preventive feature for severe accidents by reducing or eliminating the possibility of fire events that could induce transients, damage mitigation equipment, and hamper operator responses. SECY-90-016 specifies the following design criteria for evolutionary advance light water reactors:

> Therefore the evolutionary ALWR designers must ensure that safe shutdown can be achieved, assuming that all equipment in any one fire area will be rendered inoperable by fire and that re-entry into the fire area for repairs and operator actions is not possible. Because of its physical configuration, the control room is excluded from this approach, provided an independent alternative shutdown capability that is physically and electrically independent of the control room is included in the design. Evolutionary ALWRs must provide fire protection for redundant shutdown systems in the reactor containment building that will ensure, to the extent practicable, that one shutdown division will be free of fire damage. Additionally, the evolutionary ALWR designers must ensure that smoke, hot gases, or the fire suppressant will not migrate into other fire areas to the extent that they could adversely affect safe-shutdown capabilities, including operator actions.

The U.S. EPR FPS features as described in FSAR Tier 2, Section 9.5.1, and Appendix 9A are capable of providing assurance that, in the event of fire, the plant will not be subjected to the an

unrecoverable incident. The risk significance of fire in severe accidents is summarized in the evaluation of FSAR Tier 2, Section 19.1.5.2.

19.2.4.2.1.5 *Intersystem LOCA*

The U.S. EPR design conforms to the regulatory guidance associated with the ISLOCA as described in SECY-90-016 and SECY-93-087 in regard to the rupture strength design for systems connected to RCS. The systems that connect to the RCS in the U.S. EPR design include: Extra borating system; chemical and volume control system; and RHR system. The extra borating system and the chemical and volume control system piping that could be exposed to the RCS operating pressure are designed for a pressure of 24.993 MPa (3,625 psig). The RHR piping has been designed with an ultimate strength that exceeds that of the full RCS operating pressure. Given these design features, ISLOCA is not a significant contributor to initiating events or accidents.

Further details on these systems are provided in FSAR Tier 2, Sections 6.8, 9.3.4 and 5.4.7, respectively.

19.2.4.2.1.6 *Primary Depressurization System*

The PDS serves a unique role in the prevention and mitigation of severe accidents. It is an integral part of the severe accident management strategy. The PDS valves are intended to prevent RCS failure at high pressure, to avoid high-pressure core-melt ejection and direct containment heating, and to eliminate the possibility of containment bypass from induced SGTR. The effect would be to convert high-pressure core melt sequences to low-pressure sequences.

Operation of the PDS valves enables the introduction of core cooling employing all means available to the operators (i.e., feed and bleed operation). As such, the PDS is considered as the last preventive measure prior to the transition from EOPs to severe accident management guidelines (SAMGs).

19.2.4.3 *FSAR Tier 2, Section 19.2.3: Severe Accident Mitigation*

The U.S. EPR RB is composed of a Reactor Containment Building (RCB) and a Reactor Shield Building (RSB) separated by an annular region. The RCB is a post-tensioned concrete pressure vessel located inside the reinforced concrete RSB. A leak-tight steel liner plate covers the entire inner surface of the RCB, including the basemat. Within containment are the RCS, the ICWST, and parts of the main steam and feedwater lines. The containment includes a large free volume of approximately 7.93×10^4 m^3 (2.8×10^6 ft^3) and has a design pressure of 0.4275 MPa (62 psig).

The containment systems implemented for severe accident mitigation are the combustible gas control system, core melt stabilization system, and the severe accident heat removal system. A description of the containment's functional design is given in FSAR Tier 2, Section 6.2.1. The physical description of the containment is given in FSAR Tier 2, Section 3.8. FSAR Tier 2, Section 3.8.1.4.11 specifies results of the containment ultimate capacity pressure analysis.

19.2.4.3.1 Severe Accident Progression

Severe accident progression can be divided into two phases: An in-vessel stage and an ex-vessel stage. The in-vessel stage generally begins with insufficient decay heart removal and

can lead to melt-through of the reactor vessel. The ex-vessel stage involves the release of the core debris from the reactor vessel into the containment and resulting phenomena such as core-concrete interaction, fuel-coolant interaction, and direct containment heating.

19.2.4.3.1.1 *In-Vessel Melt Progression*

In-vessel melt progression establishes the initial conditions for assessing the thermal and mechanical loads that may ultimately threaten the integrity of the containment. In-vessel melt progression begins with uncovering of the core and initial heat-up, and continues until either (1) the degraded core is stabilized and cooled within the reactor vessel, or (2) the reactor vessel is breached and molten core material is released into the containment. The phenomena and processes in the U.S. EPR that can occur during in-vessel melt progression are similar to those for an existing PWR with a large, dry containment.

19.2.4.3.1.2 *Ex-Vessel Melt Progression*

The initial response of the containment to ex-vessel severe accident progression is largely a function of the pressure of the RCS at reactor vessel failure and the existence of water within the reactor cavity. If not prevented through design features, risk consequences are usually dominated by early containment failure mechanisms that could result from energetic severe accident phenomena such as HPME with direct containment heating and ex-vessel steam explosions. The long-term response of the containment from ex-vessel severe accident progression is largely a function of the containment pressure and temperature resulting from core-concrete interaction and the availability of containment heat removal mechanisms.

The U.S. EPR has incorporated a reliable depressurization system (discussed above) to provide assurance that, in the event of a core melt scenario, failure of the RPV would occur at a low pressure. Should the RPV fail at a high pressure, the design of the U.S. EPR containment provides a tortuous pathway from the reactor to the upper containment in an effort to decrease the amount of core debris that could contribute to DCH.

RPV failure at high or low pressure coincident with water present within the lower cavity could lead to fuel-coolant interaction with the potential for rapid steam generation or steam explosions. The U.S. EPR is designed so that there is a very low likelihood of water within the reactor cavity at the time of reactor vessel failure.

The U.S. EPR design incorporates a passive debris cooling device, CMSS, to cool the debris once the RPV is failed (see Section 19.2.3.3.3 in this report). Without such a device, contact of molten core debris with concrete in the lower cavity would lead to uncontrolled core concrete interaction (CCI).

19.2.4.3.2 Severe Accident Mitigative Features

The U.S. EPR design and operational features for mitigating the consequences of core damage and in preventing releases from containment that go beyond those found in current-generation plants are listed and described in FSAR Tier 2, Section 19.1.3.2. In summary, these are: The large robust containment, PDS, CMSS, and SAHRS. There is also a dedicated CGCS, and dedicated instrumentation and control features for use during severe accidents.

The U.S. EPR design and operational features for mitigating the consequences of possible releases from containment are listed and described in FSAR Tier 2, Section 19.1.3.3. These include containment spray via SAHRS and the Containment and Outer Shield Building.

More discussion of the mitigative features is provided in the following sections.

19.2.4.3.2.1 *External Reactor Vessel Cooling*

The U.S. EPR does not use external reactor vessel cooling to mitigate severe accidents. It relies on maintaining containment integrity through melt spreading and ex-vessel melt retention (i.e., the core melt stabilization system).

19.2.4.3.2.2 *Hydrogen Generation and Control*

The probabilistic PE of hydrogen combustion is discussed in the evaluation of FSAR Tier 2, Section 19.1.4.2.

Preventive and/or Mitigative Features. Hydrogen would be generated during severe accidents due to oxidation of fuel rod cladding, molten core-concrete interaction, and oxidation of other core and upper plenum structures. The U.S. EPR containment is not inerted; therefore, it has a dedicated CGCS to avoid the risk of containment failure due to fast deflagration or from accidental ignition of a critical gas mixture. The CGCS system is divided into two subsystems corresponding to their operational functions: The hydrogen reduction system (HRS) and the hydrogen mixing and distribution system.

The HRS consists of 41 large and 6 small passive autocatalytic recombiners (PAR) installed in various parts of the containment. Each PAR consists of a metal housing designed to promote natural convection with a gas inlet at the bottom and a lateral gas outlet at the top. The horizontal cover of the housing at the top of the recombiner protects the catalyst against direct water spray and aerosol deposition. Numerous parallel plates with a catalytically active coating (Pt/Pd substrate) are arranged vertically in the bottom of the housing. Hydrogen and oxygen in containment gas mixtures are recombined upon contact with the catalyst in the lower part of the housing. The heat from this reaction in the lower part of the recombiner causes a reduction in gas density in this area promoting natural circulation through the PAR and ensuring high efficiency of recombination. In the presence of oxygen, the PARs will automatically start if the threshold hydrogen concentration is reached at the catalytic surfaces.

The PAR locations and arrangement inside the equipment rooms and containment dome are such that they support global circulation within the containment, and thereby homogenize the atmosphere and reduce locally high hydrogen concentrations to below 10 percent by volume during various phases of accidents resulting in oxidation up to 100 percent of the zirconium surrounding the reactor core fuel, and ensure that the global hydrogen concentration can be maintained below the lower flammability limit of four percent by volume of the containment atmosphere in the long term. The PARs are installed above the floor to provide unobstructed inflow and easy access to facilitate maintenance. They are also arranged to avoid direct contact with spray water (despite their qualification to operate in the presence of water).

The hydrogen mixing and distribution system is designed to ensure that adequate communication exists throughout the containment to facilitate atmospheric mixing. Several of the equipment rooms surrounding the RCS are isolated from the rest of the containment during normal operation. In the event of an accident, communication is established between these equipment rooms, thereby eliminating any potential dead-end compartments where

non-condensable gases could accumulate. This ability to transform the containment into a single convective volume is supported by a series of mixing dampers and blowout panels.

Hydrogen concentration and distribution within various compartments of the containment are continuously monitored, and information is available to the main control room. Specifically, measuring points are located in the upper dome, SG compartments, pressurizer compartment, and the annular rooms.

Combustible Gas Control Design Evaluation. The U.S. EPR design-specific PRA considers that deflagration, flame acceleration, and deflagration-to-detonation transition should all be considered as potentially unfavorable loadings for the containment during a severe accident.

The applicant acknowledges that containment structural integrity must be maintained in accordance with 10 CFR 50.44(c), and described the U.S. EPR approach to combustible gas control as follows:

- The containment response is to be monitored to ensure that the pressure loads resulting from the accumulation and combustion of hydrogen could not exceed the containment ultimate capacity pressure limit. To provide reasonable assurance that structural integrity is not compromised, the containment is designed to withstand global hydrogen deflagration and flame acceleration.

- With regard to global deflagration, the adiabatic isochoric complete combustion (AICC) pressure was used as a bounding value for the pressure that could result should a single large deflagration occur. From FSAR Tier 2, Figure 19.2-7, "Tolerance Limit Plot of Containment AICC Pressure," the global maximum AICC pressure is approximately 723.95 kPa (105 psia) for all the uncertainty cases considered by the applicant. Clearly, this does not exceed the containment ultimate capacity pressure of 820.5 kPa (119 psig) (see FSAR Tier 2, Section 3.8.1.4.11 and FSAR Tier 2, Table 3.8-6).

The primary function of the CGCS is to prevent the global concentration of hydrogen from exceeding 10 percent by volume. This is accomplished through global convection and the distribution of the passive autocatalytic recombiners. The applicant analyzed the results of 59 scenarios in an uncertainty analysis, and determined that the global hydrogen concentration did not reach or exceed 10 percent by volume for any of them (FSAR Tier 2, Figure 19.2-6).

The pressure loads from a detonation or flame acceleration are the results of dynamic pressure caused by the combustion front, but the applicant noted that loads resulting from flame acceleration may not be bounded by AICC pressure. To eliminate the possibility of flame acceleration, a parameter termed the sigma index was calculated by the applicant for every compartment and every case analyzed. Based on an experimentally based limit, for scenarios where the sigma index is greater than 1.0, flame acceleration cannot be excluded. FSAR Tier 2, Figure 19.2-8, "Tolerance Limit Plot of Sigma Index for the Pump/SG Compartment," shows the sigma index for the pump/SG compartment (representative of the worst location) for all cases. The results show that the sigma index does not exceed 1.0 for any scenario where the hydrogen produced is less than or equal to that resulting from 100 percent oxidation of the Zircaloy cladding. The risk of flame acceleration or DDT in the U.S. EPR containment is stated by the applicant to be negligible, based on these analyses.

With respect to global deflagration, the post-combustion AICC pressure was calculated by the applicant to reach approximately 723.95 kPa (105 psia), which is below the containment

ultimate capacity pressure of 820.5 kPa (119 psig) (ASME Service Level C limit, failure of equipment hatch cover).

Staff Evaluation. The staff reviewed the CGCS and hydrogen monitoring system descriptions, and the applicant's analyses, to assure compliance with the specific requirements of 10 CFR 50.44(c), and finds that supporting detailed analyses of global and local hydrogen combustion scenarios in the U.S. EPR (with its features of a large robust containment, HMS, and PARs) are reasonable. However, additional information was required before the staff could accept the applicant's conclusion that the risks from hydrogen from flame acceleration or DDT were negligible.

In an August 8, 2008, response to RAI 6, Question 19-114, the applicant stated that the aforementioned calculation result was based on the realistic value of hydrogen production as opposed to that corresponding to oxidation corresponding to 100 percent of the zirconium inventory. The staff issued follow-up RAI 133, Question 19-235, requesting that the applicant address the consequences of global deflagration considering a hydrogen mass that corresponds to the oxidation of 100 percent of the core inventory of zirconium. In a December 8, 2008, response, the applicant stated that severe accident analyses using MAAP4 do not show 100 percent cladding oxidation. An alternate method was therefore chosen to simulate an equivalent of 100 percent cladding oxidation. The method applies model biases to promote hydrogen production while prohibiting the auto ignition of hydrogen created from MCCI. This ex-vessel hydrogen [about 0.59 metric tons (1,300 pounds)] is added to in-vessel hydrogen production [about 0.91 metric tons (2,000 pounds)] to represent 100 percent cladding coolant hydrogen production. The applicant concluded that the analysis indicates the sigma index for conditions corresponding to 100 percent cladding coolant reaction would not exceed 1.0 and, therefore, there is no potential for flame acceleration or detonation. After reviewing the applicant's response, the staff agrees that the risk from flame acceleration or detonation is negligible, because the applicant's analysis is consistent with other analyses familiar to the staff. Accordingly, the applicant's analysis shows a large margin to potential flame acceleration or detonation.

The staff performed confirmatory MELCOR calculations for a large number of representative accident scenarios. These calculations have confirmed that due to efficient recombination by PARs, there is little potential for formation of pockets of high hydrogen concentration inside the EPR containment, and a large deflagration would not result during any of these scenarios. As part of the confirmatory assessment, comparisons were made to the applicant's MAAP 4.0.7 calculations. Generally, the MAAP-predicted in-vessel hydrogen generation was higher than the MELCOR predictions. This was attributed, in large part, to the applicant's choice of a conservative value for the parameter multiplying the oxidation rate as modeled in MAAP. Nevertheless, both MAAP and MELCOR results showed that hydrogen concentration in the containment would remain low due to the effective recombination of hydrogen and oxygen by the PARs.

19.2.4.3.2.3 *Core Debris Coolability*

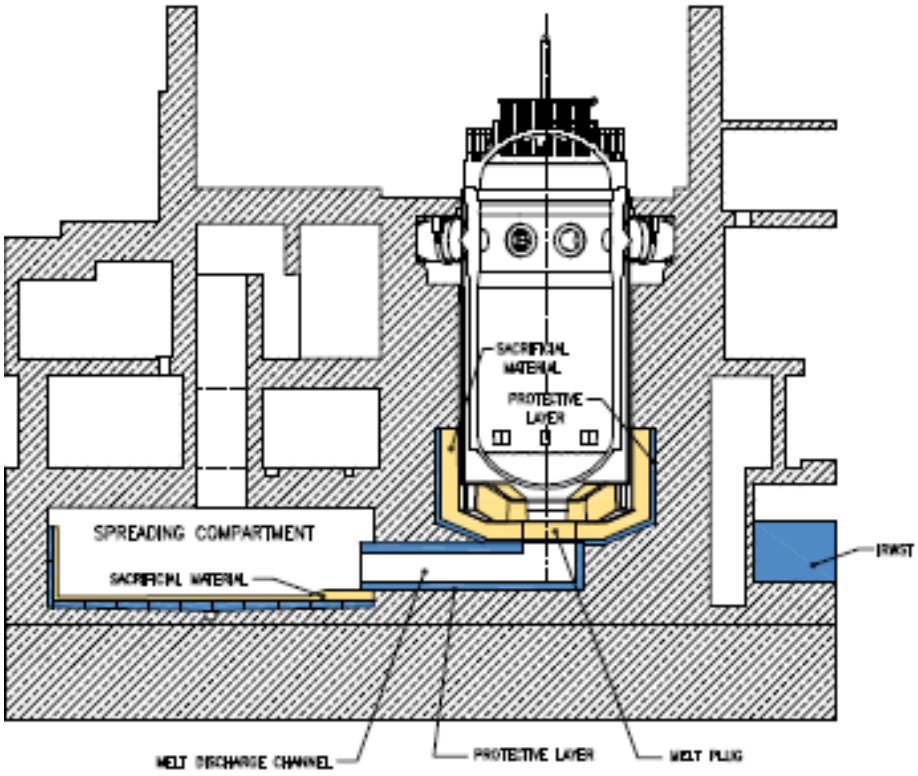
In a severe accident leading to core melt through of the reactor vessel, a potential exists for containment rupture if the molten core is not sufficiently cooled. The core melt stabilization system and the severe accident containment heat removal system are the U.S. EPR design features designed to ensure core debris coolability.

Core Melt Stabilization System (CMSS). The U.S. EPR is equipped with a dedicated ex-vessel system to accommodate molten core debris in a coolable configuration, including the entire core

inventory and reactor internals, should they melt and penetrate the RPV. The general configuration of the CMSS is provided below in Figure 19.2-1, "Core Melt Stabilization System." The goal of this system is to stabilize molten core debris before it can challenge the integrity of the containment, through the combined effects of the following features:

- Reactor Cavity
- Melt Plug
- Melt Discharge Channel
- Spreading Area and Cooling Structure

Figure 19.2-1 Core Melt Stabilization System



Underneath the U.S. EPR RPV, there are six vertical structures in the cavity aligned radially from a central melt plug, effectively creating six azimuthal sectors. These walls are designed to limit the downward expansion of the lower head resulting from contact with a molten pool and provide protection for the reactor cavity integrity in the event of an abrupt vessel failure that results in a large section of the lower head falling into the reactor cavity. These features are intended to ensure that the reactor cavity can withstand the loads resulting from RPV failure.

The applicant used MAAP 4.0.7, which has models to treat severe accident phenomena associated with core melt progression and debris coolability, to assess the viability of the core melt stabilization concept in the U. S. EPR. The various representative accident scenarios were simulated, and uncertainty analyses were carried out for each scenario. To account for modeling uncertainties, the reactor cavity was designed to provide a sufficiently long period for temporary melt retention. After vessel breach, the core debris would first confront a layer of

sacrificial material that must be penetrated before it can escape from the cavity. The applicant's analyses indicate that the ensuing time delays allow sufficient time for nearly all of the core debris to exit the vessel before the sacrificial layer is fully penetrated.

The sacrificial layer consists of a layer of siliceous concrete with high iron-oxide content for oxidation of the remaining Zirconium and Uranium within the melt, and ensuring a low melt temperature and viscosity for spreading. The sacrificial concrete layer covers a protective refractory material consisting of zirconia bricks, which have a low thermal conductivity and a mechanical strength greater than concrete, to confine the melt and insulate the RPV support structure in case of a local penetration of the sacrificial concrete. This protective layer "guides" heat transfer from the melt towards the metallic gate of the melt plug.

The staff raised some concerns about the structural integrity of the zirconia. It is a very brittle material, and it is subject to failure by thermal shock as a result of the monoclinic-to-tetragonal phase change at about 1,470 K (2,186 °F). The submittal did not address this issue and does not shed any light on the integrity of zirconia. Therefore, that the staff asked the applicant to demonstrate that the zirconia structural integrity can be maintained during the transients expected under U.S. EPR severe accident conditions. In a follow up to RAI 45, Question 19-189, the staff issued RAI 133, Question 19-231, requesting that the applicant provide the results of tests that demonstrate the integrity of the zirconia. In a December 8, 2008, response, the applicant informed the staff that testing for the zirconia brick assembly identified for the U.S. EPR has been performed, as stated in a September 19, 2008, response to RAI 45, Question 19-189, and that the results report was available for NRC inspection. The applicant also stated that the exact specification for the stabilized zirconia for the U.S. EPR would be developed later in the design process. The staff conducted an audit on March 26, 2009, for an in-depth understanding of these test results. As a result of the audit, further information was requested (RAI 236, Question 19-312). The applicant's response included information on material characteristics of the zirconia, the industrial knowledge base, and results of experimental data versus theoretical predictions for various severe accident loading conditions. The staff reviewed the response and realized that further clarification was required on matters related to material properties and experimental data. The staff issued follow-up RAI 349, Question 19-332. The staff is awaiting a response from the applicant. **RAI 349, Question 19-332, which is associated with the above request, is being tracked as an open item.**

Once the melt plug fails, the molten debris would flow from the cavity pit, through the melt discharge channel, and then into the core spreading room, where it would presumably be stabilized. The melt plug is constructed of a 4 cm (1.57 in.) thick aluminum plate topped with the same layer of sacrificial concrete as that within the cavity. At the end of the retention phase, the failure area would be large enough to achieve a complete and rapid relocation of the accumulated melt into the lateral discharge channel leading to the spreading compartment. The channel consists of a steel structure that is embedded within the structural concrete of the containment. Its bottom, sidewalls, and top are also layered with zirconia bricks.

The spreading compartment consists of a large horizontal concrete surface (about 170 m^2 or 1,830 ft^2) over which the molten core debris can be dispersed. The spreading compartment is a dead-end room (with the exception of a steam chimney, as described in FSAR Tier 2, Section 19.2.3.3.3.2) and is isolated from the rest of containment by flood and splash walls. These features prevent the direct inflow of water from sprays, leaks, or pipe breaks. The concrete of the spreading compartment covers a dedicated cooling structure would cool the molten core debris on all sides once filled by water from the IRWST. The sacrificial concrete layer protects the cooling structure against thermal loads resulting from melt spreading. It also

delays melt contact with the metallic cooling structure to ensure that the cooling elements will be flooded with water from the IRWST prior to the initial contact between them and the molten core debris. The arrival of the melt into the spreading compartment triggers the opening of spring-loaded valves that initiate the gravity-driven flow of water from the IRWST into the cooling structure and the spreading compartment.

Once the sacrificial concrete in the spreading compartment has been ablated by the molten core debris, the molten pool is not expected to penetrate the cooling structure. The combined cooling elements will form a series of parallel cooling channels that serve as flow paths for water from the IRWST to flow under the melt, along the sidewalls and onto the top of the molten core debris, cooling the melt from above and below, thus stabilizing it.

The CMSS is a non-safety-related system and was not designed to withstand a seismic event. The applicant argued that the combination of the low probability of a severe accident coupled with the low probability of a seismic event, results in an acceptably low frequency scenario, and then screened it from further consideration for the U.S. EPR. The staff agrees that the frequency is very low, but, from a severe accident mitigation perspective, warrants consideration of the consequences of failure to passively flood the core debris once it enters the spreading room. In an August 8, 2008, response to RAI 6, Question 19-93, providing the technical basis for selection of the maximum duration considered for assessing long-term containment challenges, the applicant showed a result from a calculation using MAAP 4.0.7 indicating that it would take about 9.5 days to penetrate the 4.4 m (14.5 ft) thick basemat for a case where it was assumed that there would not be any passive flooding. This time interval is much longer than the 24 hour guideline on maintaining containment integrity in SECY-93-087, so the staff finds the applicant's argument reasonable.

Severe Accident Heat Removal System. SAHRS is a dedicated single-train, non-safety related, thermal-fluid system used to control the environmental conditions within the containment following a severe accident. SAHRS has four primary modes of operation, each playing a role in controlling the environmental conditions within the containment so that its fission product retention function is maintained. These modes include:

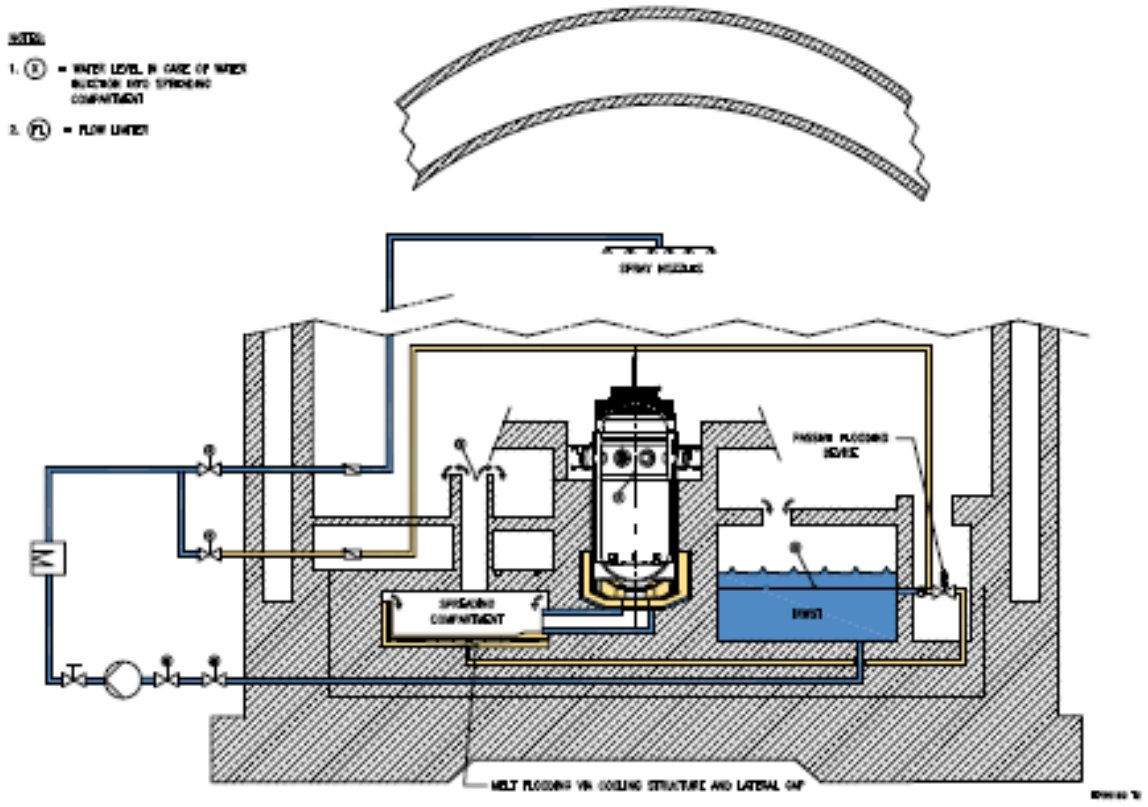
- Passive cooling of molten core debris
- Active spray for environmental control of the containment atmosphere
- Active recirculation cooling of the molten core debris and containment atmosphere
- Active back-flush of the IRWST

The SAHRS train is composed of a pump, suction line from the IRWST, heat exchanger, and three possible discharge pathways. The SAHRS heat exchanger transfers the residual heat from the containment to the ultimate heat sink via dedicated portions of CCWS and ESWS trains. The SAHRS, CCWS, and ESWS systems receive power from normal offsite grid sources or emergency and SBO diesel units. The general configuration of SAHRS is provided below in Figure 19.2-2, "Severe Accident Heat Removal System."

The three possible flow paths downstream of the pump and the heat exchanger are:

- To a containment spray system with a ring header and spray nozzles
- To the spreading area of the CMSS
- To the IRWST, in recirculation mode, under non-severe accident conditions

Figure 19.2-2 Severe Accident Heat Removal System



In containment spray mode, the flow path through the spray nozzle reduces containment pressure, temperature, and concentrations of airborne fission products, and the spray water and condensate flow back to the IRWST. In the recirculation mode, the flow path is used to cool the water in the IRWST.

Passive cooling of the CMSS starts when molten core debris reaches the spreading compartment, triggering the opening of a spring-loaded valve that initiates the gravity-driven flow of water from the IRWST into the spreading compartment. Water from the IRWST passes through a passive outflow reducer (POR) and fills the CMSS cooling structure, and then overflows into the spreading compartment until it is hydrostatically balanced with water from the IRWST. The water in the CMSS area boils off as steam and is released into the free volume of the containment through the steam chimney directly above the spreading compartment. As this process continues, the temperature and pressure within the containment will steadily increase. At this point, the SAHRS is configured to operate in the containment spray mode.

The system mode of operation for active cooling of the CMSS occurs once the containment spray has sufficiently reduced containment pressure. Under this mode of operation, the SAHRS feeds water via a recirculation flow path into the spreading area. As a result, the water pool in the cooling channels and on top of the melt will become subcooled, thus ending the evaporation process and lowering the potential for the continued release of fission products. In this mode of operation, the water level in the spreading compartment will rise to the top of the steam outlet chimney, overflow onto the containment floor, and drain back into the IRWST, where it can be recirculated back into the spreading area cooling system. Because the spreading compartment and the reactor cavity are connected through the opened gate and transfer channel, water will also enter the reactor cavity and submerge the vessel up to the level of the RCS piping. This establishes long-term cooling of any debris that has remained within the transfer channel, reactor cavity, or vessel itself.

A fraction of the SAHRS flow is used for sump screen back-flushing function within the IRWST. The system can operate in this mode while continuing operation in another containment cooling mode.

Staff Evaluation. The U.S. EPR design feature for addressing the guidance of SECY-90-16 for core coolability is CMSS, which provides floor space for debris spreading and quench capability to cool the debris. The design would provide retention and long-term stabilization of the molten core inside the containment. The applicant's analysis of the melt in the spreading area indicates a uniform thickness of molten debris over the spreading area ranging between 5.08 cm (2 in.) to 40.64 cm (16 in.) assuming a complete metallic or ceramic melt, respectively. The melt is cooled by gravity-driven flow of water from the IRWST during the initial cooldown, and by forced flow using the SAHRS pump over the long-term. The water passes through the cooling channels underneath the spreading compartment and then submerges the space behind the sidewalls and pours onto the melt surface.

The credible containment failure modes during debris coolability are basemat failure and containment over-pressurization. The major concern with regard to basemat protection is to keep the area heat flux below the critical value of 120 kW/m2 (11.15 kW/ft^2). The applicant's evaluations of heat flux from MAAP4-based uncertainty analyses indicate a worst-case scenario of about 79.65 kW/m^2 (7.4 kW/ft^2). The maximum temperature is calculated to be the melting point of the structure. The containment pressure as a consequence of flooding in the spreading area in a worse case uncertainty analysis was calculated to be about 0.5 MPa (74 psia), well below the containment ultimate pressure of 0.81 MPa (119 psia). These results indicate that the design (size and composition) of the CMSS provides sufficient margin to withstand a postulated severe accident.

The staff considers the CMSS design to be a reasonably engineered approach to collecting, capturing, and segregating the core debris into a long-term coolable and stable configuration. In conjunction with the SAHRS design, the overall approach would avoid basemat melt-through, and would maintain containment pressures and temperatures below ultimate failure values, passively in the short term and actively in the longer term.

Extensive NRC-sponsored MELCOR confirmatory calculations using the MELCOR 1.8.6 computer code to analyze the representative accident scenarios identified by the applicant have shown that:

- The time duration from vessel breach to reactor pit melt plug failure was found to be much shorter in MELCOR as compared to MAAP predictions.

- The MAAP-predicted debris temperature in the reactor pit before the melt plug failure was found to be 500 K (440.33 °F) to 600 K (620.33 °F) (higher than the MELCOR predictions; nonetheless, the MELCOR-predicted melt plug failure occurred sooner. It is apparent that the AREVA MAAP input parameter values were chosen in order to bias the results towards higher temperatures.

- MELCOR results showed that the entire core debris content may not be in the reactor pit by the time the reactor melt plug melt-through occurs. Nonetheless, the mass of any remaining core debris arriving into the reactor pit after melt plug failure was calculated to be small (approximately five percent). This delayed relocation can have implications in terms of ex-vessel energetic fuel coolant interactions, which the design of the reactor pit was intended to circumvent altogether.

- Differences in MELCOR and MAAP prediction of concrete erosion were found with the MELCOR-calculated erosion rate being lower than that of the MAAP prediction.

- Ex-vessel hydrogen production, in the absence of passive flooding of the containment, was reported to be higher in MELCOR even though the concrete erosion rate was lower than the MAAP-prediction. This anomaly is traceable in large part to differing in-vessel/ex-vessel splits in metal oxidation, and due to the absence of the metallic mass associated with the reactor core reflectors during the ex-vessel phase of the accident in the MAAP calculations.

- For most of the scenarios examined, the MELCOR-predicted debris temperature in the spreading compartment was shown to be lower due to lower initial debris temperature as compared with MAAP.

- Provided that full uniform spreading of the melt over the floor of the spreading compartment occurs, and provided that IRWST passive injection is initiated as designed, melt cooling and stabilization were predicted to take place by both MAAP and MELCOR. Nonetheless, for most of the scenarios examined, the predicted core debris cool-down rate on the spreading compartment floor was shown to be faster in MELCOR as compared to MAAP.

- The rate and magnitude of containment pressurization was shown to be significantly higher in MAAP as compared to MELCOR.

Based on the comparisons between MAAP and MELCOR simulations, the staff issued RAI 262, Questions 19-319 through 19-325, in order to better understand the sources of the differences, and possibly reduce their magnitudes. The applicant provided responses to these questions between August 31, 2209, and October 12, 2009. These responses are under staff review. **RAI 262, Questions 19-319 through 19-325, which are associated with the above request, is being tracked as an open item.**

19.2.4.3.2.4 *High-Pressure Melt Ejection*

Under conditions of high RCS pressure at the time of reactor vessel failure, a potential exists for the rapid ejection of molten core debris into the containment atmosphere, leading to rapid oxidation, hydrogen combustion, and convective energy transfer. This process is known as

DCH, which could lead to a rapid pressure increase in the containment, and potentially early containment failure. SECY-93-087 recommends that the evolutionary reactors include a depressurization system and cavity design features to reduce the RCS pressure and contain the ejected core melt. The U.S. EPR design includes two features that reduce the risk for HPME and DCH, and which are evaluated below.

Primary Depressurization System. The U.S. EPR design includes two dedicated severe accident depressurization valve trains, each of which consists of a DC-powered depressurization valve in series with an isolation valve connected to the pressurizer. The PDS valves are independent of the pressurizer safety relief valves. The objective of this design is to convert high-pressure core melt sequences into low-pressure sequences, so that a high-pressure vessel breach can be excluded.

The operator will actuate these valves when the core exit temperature exceeds 922 K (1,200 °F). The anticipated loads within the reactor cavity in the event of successful RCS depressurization (i.e., pre-vessel breach RCS pressure) would be well below the reactor cavity design load of 1.97 MPa (290 psia). As explained in FSAR Tier 2, Section 19.2.3.3.1, the reactor cavity is designed to withstand such pressure loads and to limit the downward expansion of the lower head from contact with the molten pool.

Timely operation of the depressurization valves is part of the accident management strategy and is very important to avert possible induced creep ruptures of hot legs or damaged steam generator tubes. In a December 8, 2008, response to RAI 133, Question 19-240(1), and 19-240(3), and a February 11, 2009 response to 19-240(2), the applicant provided the results of calculations showing the amount of time available between when the core exit temperature reaches 922 K (1,200 °F) and when induced steam generator tube rupture might be expected for varying degrees of tube damage. The results showed that 18 to 20 minutes would be available (assuming a hot leg would not fail first). These results establish the importance of prompt depressurization and the need for a good HRA assessment of the probability of failing to depressurize in time, and hence the potential impact on LRF and on accident management procedures. The staff is currently reviewing the applicant's response to RAI 133, Question 19-243 on severe accident management OSSA (see the discussion in Section 19.2.4.5). It is possible that, as a result of the review, a follow-up question will be sent asking for more information on how primary system depressurization will be addressed in OSSA, and how the applicant's HRA will be utilized in this regard. **RAI 133, Question 19-243, which is associated with the severe accident management review, is being tracked as an open item.**

Resistance to Core Melt Dispersal. The U.S. EPR reactor cavity is designed to significantly reduce the potential risk of HPME. The applicant hypothesized the most severe reactor vessel failure from the standpoints of both entrainment and fragmentation of melt to be a small penetration at the very bottom of the lower head. Under high pressure, debris particles would be driven from the reactor cavity region towards the remainder of the containment. Due to containment compartmentalization design, the particles must pass through the narrow gap between the reactor vessel and the reactor cavity, and travel towards the SG equipment room vents, (in the form of mixing dampers and rupture foils assumed to be open for promoting containment mixing) before entering the containment atmosphere. Therefore, the reactor cavity and containment configuration would create several flow resistance obstacles with a tortuous pathway. Hence, the design provides resistance to in-containment aerosol dispersal and a long residence time for HPME to occur, and allows plate-out and de-entrainment of aerosols along the path, thereby reducing and eliminating the potential for early containment failure due to DCH from ejected core debris.

Dispersal of the melt and aerosols through the reactor cavity cooling ventilation ducts after RPV failure under elevated pressure is tortuous, with entrainment and de-entrainment occurring along the path, thus causing significant reduction in materials entering the upper containment.

Staff Evaluation. With the exception of the item identified below, the staff concludes that the U.S. EPR design addresses the guidance of SECY-93-087 for HPME by providing:

- A reliable primary depressurization system capability to lower RCS pressure after loss of decay heat

- A reactor cavity and containment design with tortuous pathways to contain ejected core debris and prevent DCH

HPME is prevented by two manually-operated PDS valves. Following actuation of the PDS valves, the reactor depressurizes. The applicant's MAAP4 analysis of RCS pressure indicates a maximum pressure of less than 1.379 MP (200 psia). This pressure is below the design load on the reactor cavity. In the majority of the cases analyzed (over 86 percent), the expected RCS pressure was below 689.5 kPa (100 psia). This lower pressure eliminates the potential ejection of core debris. The core debris in an RPV lower head, or side wall, failure would immediately de-entrain on the reactor cavity walls. The in-containment aerosol dispersal would be limited due to tortuous pathways and long residence time. The conditional probability of DCH-induced containment failure probability due to HPME is evaluated by the applicant to be very small, on the order of 1.0×10^{-3}.

The staff believes that the impacts of the presence of core debris in pump and steam generator rooms need to be taken into account in preparing severe accident management guidelines. Staff review of the applicant's Operational Strategy for Severe Accidents Methodology is still ongoing (see the discussion in Section 19.2.4.5 of this report). Accordingly**, this issue is being tracked as an open item and is related to the open item discussed in Section 19.2.4.5.**

19.2.4.3.2.5 *Fuel-Coolant Interaction*

The containment function may be challenged by a rapid energy release during a FCI that results in a steam explosion. The term "steam explosion" refers to a phenomenon in which molten fuel rapidly fragments and transfers its energy to the coolant resulting in rapid steam generation, shock waves, and possible mechanical damage. To be a significant safety concern, the interaction must be very rapid and must involve a large fraction of the core mass. Steam explosions may occur either in-vessel or ex-vessel. The U.S. EPR design characteristics that inherently impede potential containment failure include:

- The additional structure surrounding the reactor vessel, which further mitigates adverse consequences of an in-vessel FCI-induced steam explosion by eliminating a clear path to the containment shell.

- The design of the core spreading compartment, which preserves a dry environment and eliminating the possibility of an ex-vessel steam explosion.

In-Vessel Steam Explosion. The in-vessel steam explosion was first hypothesized in WASH-1400, "Reactor Safety Study." The Steam Explosions Review Group (SERG) convened by the NRC in 1985 as SERG-1, and again in 1995 as SERG-2, focused on the alpha-mode of containment failure (α-failure). The applicant notes that both studies concluded that in-vessel steam explosion-induced containment failure probability is negligible. Severe accident

conditions for the U.S. EPR are not expected to alter this conclusion, because it has features similar to operating PWRs in this regard. The staff agrees with this conclusion.

Ex-Vessel Steam Explosion Effects. If core debris and water come into contact after vessel breach, fuel-coolant interactions can cause the containment pressure to increase. In certain circumstances, steam explosions could possibly occur, leading to a highly energetic pressure rise. The U.S. EPR design includes design measures that minimize the potential for ex-vessel steam explosions, such as an initially dry reactor cavity and dry core spreading area, the addition of silica-rich sacrificial material to the melt before ex-vessel flooding, and the controlled addition of water to the top of the melt after spreading.

The core spreading area could contain a thin layer of water film from steam condensation. Therefore, the only event that could lead to ex-vessel metal water interaction is during the initial quenching of the melt.

Staff Evaluation. The U.S. EPR addresses the impact of fuel-coolant interactions for the more likely scenarios by acknowledging the conclusions of various test programs and of expert groups established to assess this issue. Nonetheless, the staff cautions that the principal reactants, water and high-temperature metallic and oxide masses, are present, and configurations can be imagined that result in FCI-developed containment loads that challenge containment integrity (i.e., in-vessel scenarios) or cavity structure loads that can damage the U.S. EPR CMSS effectiveness (i.e., ex-vessel scenarios).

Because of the large uncertainties associated with low probability events such as FCI, the likelihood of containment failure by steam explosion cannot be resolved through traditional deterministic analysis; therefore, the applicant carried out a probabilistic evaluation. For this evaluation, separate analyses were performed assessing containment or cavity structure failure probability from either in-vessel or ex-vessel scenarios. The uncertainty distributions were developed based on the available literature citations (e.g., SERG-2 report), experiments, or analysis. Values for corium debris quantities used for the analysis were taken from the U.S. EPR MAAP4 calculations.

The results from the applicant's analysis conclude that the probability of in-vessel steam explosions leading to containment by alpha-mode failure or reactor cavity damage by steam explosions or lower head missiles would be very small (less than 1E-3). These conclusions are consistent with expectations and expert assessment of in-vessel steam explosions for other PWRs. In addition, the applicant claimed that the ex-vessel scenario is not credible for containment failure because of its distance from the containment boundary and because the probability of reactor cavity structure failure was also evaluated to be very small (less than 1E-4).

The estimated dynamic loads resulting from ex-vessel steam explosions based on the analyses performed for other PWRs (for similar conditions) under NRC sponsorship have shown that the potential impulse loads ranging from approximately 10 to 300 kPa (1.45 to 43.51 psi). On July 2, 2009, the applicant provided a detailed response to RAI 133, Question 19-230. The staff evaluated the revised estimates of the cavity structural integrity for dynamic loads. The staff expects that even if the cavity were to fail, in the absence of direct communication between the cavity and the containment boundaries, the likelihood of containment failure is expected to be negligible; however, this conclusion needs to be verified. The staff issued RAI 349, Question 19-334, requesting that the applicant provide additional information that addresses this issue. In addition, the staff requested that the applicant revise the ex-vessel steam explosion analysis to address the potential impact of phenomenological uncertainties, and to discuss the

consequences of steam explosions from delayed relocation of core debris from the reactor vessel after failure of the melt plug. **RAI 349, Question 19-334, which is associated with the above request, is being tracked as an open item.**

19.2.4.3.2.6 *Containment Bypass*

In SECY-90-016, the staff concluded that a special effort should be made to eliminate or further reduce the likelihood of a sequence that could bypass the containment. In SECY-93-087, the staff stated that vendors should make reasonable efforts to minimize the possibility of bypass leakage and should account, in their containment designs, for a certain amount of bypass leakage. Two types of accident scenarios would lead to containment bypass: SGTR and ISLOCA.

Steam Generator Tube Rupture. In SECY-93-087, the staff recommended that the advanced plant designer consider design features to reduce or eliminate containment bypass leakage that could result from SGTR. The staff identified the following design features as able to mitigate the releases associated with a tube rupture:

- A highly reliable (closed-loop) SG shell-side heat removal system that relies on natural circulation and stored water sources
- A system that returns some of the discharge from the SG relief valve back to the primary containment
- Increased pressure capacity on the SG shell side with a corresponding increase in the safety valve setpoints

The U.S. EPR design strategy in reducing potential radioactive release in an SGTR is based on having the medium head safety injection pump shut off head at a pressure below the SG safety relief valve set point. As a consequence, the applicant states that the likelihood of a SGTR progressing to containment bypass due to secondary system pressure increasing enough to open a safety valve and fail to reseat has been significantly reduced. Automatic isolation of the affected SG on its high level signal coincident with the end of partial cooldown prevents overfilling and limits liquid release to the environment. The applicant states that the design is such that no operator actions are needed to mitigate the SGTR accident, and the secondary system remains sealed against releases to the environment after the relief valve or its block valve is closed. The subsequent plant cooldown is accomplished using the remaining three intact loops.

In addition, the applicant considered the following design options as part of the assessment of SAMDAs for the U.S. EPR:

- Install a highly reliable (closed loop) SG shell-side heat removal system that relies on natural circulation and stored water sources (CB-16). The applicant states that the SGs in the U.S. EPR are vertical shell natural circulation, u-tube heat exchangers. The secondary side is cooled with feedwater supplied from the IRWST. In a September 19, 2008, response to RAI 45, Question 19-190, the applicant stated that the supplied water for the feedwater is the deaerator/feedwater storage tank, and not the IRWST. This error was corrected in Revision 1 of the Environmental Report, and the intent of the SAMDA is already implemented in the design. The staff agrees with the applicant's assessment.

- Redirect the discharge flow from all main steam safety valves (SG safety and relief valves) through a structure where a water spray would condense the steam and remove most of fission products (CB-15). The applicant stated the estimated cost of a similar system at a conventional PWR unit at $9.5 million.

- Vent main steam safety valves in containment (Item CB-19). The applicant states that such design mitigation would pose drawbacks, such as increased pressure loading and water inventory within containment, which would exceed any intended benefit. Therefore, it was not considered for implementation for the U. S. EPR.

- Increase the pressure capacity of the SG secondary-side so that an SGTR would not cause the [secondary system safety] relief valve to open (CB-11). The applicant estimated the cost of a similar system at a conventional PWR unit at $1.0 million.

The applicant's evaluation of various SAMDAs is provided in Section 19.2.4.6 of this report. As indicated in Section 19.2.4.6, the applicant, on the basis of the estimated CDF and risk from internal events in the U.S. EPR design, concluded that any potential design modifications for accident mitigation that cost more than about $51,000 would not be cost effective, even if the modifications would eliminate all offsite consequences. The staff's review of the applicant's method, as detailed in Section 19.2.6.5 of this report, identified that if the design modifications could completely eliminate all severe accidents, the projected maximum value of the averted cost would be about $400,000. The review also generated RAI 6, Question 19-121 on the methods and assumptions that could alter the applicant's conclusions in regard to the third and fourth design options. For the third design item, it appears the applicant's interpretation of the design is in contradiction with the intent of the recommended system.

- As stated in Section 19.2.4.6.7 of this report, in a February 11, 2009, response to RAI 133, Question 19-238, the applicant shows that the SGTR mitigation strategy for SGTR-initiated events allows for venting into the three condenser shells through the main steam bypass valves, and this is a preferable strategy to venting into containment. Moreover, from a SAMDA perspective, the costs of making a design change outweigh the benefits. For these reasons the applicant has dismissed the second and third alternatives. The staff agrees with this approach. The fourth alternative also is not cost-beneficial.

The staff agrees that having the medium head safety injection pump shut off head at a pressure below the SG safety relief valve set point would reduce the likelihood of fission product releases from accidents initiated by a steam generator tube rupture.

On the other hand, high-RCS pressure severe accidents leading to induced tube ruptures would likely still result in large releases if MSSVs would not reseat, resulting in steam generator depressurization. In an August 8, 2008, response to RAI 6, Question 19-79, and a February 11, 2009, response to RAI 133, Question 19-240, the applicant has shown that the likelihood of induced tube ruptures with a depressurized steam generator is very low (the consequent contribution to LRF from RC 702 is stated by the applicant to be 4.6×10^{-9}/RY).

The staff concludes that, in line with the general SECY-93-087 guidance, the U.S. EPR design does include specific design features to minimize the release of radioactivity to the environment

following a SGTR. Further, the staff concludes that the general and specific intents of the guidance of SECY-93-087 have been met.

Interfacing Systems Loss of Coolant Accident. As stated above, the U.S. EPR conforms to the guidance associated with an ISLOCA as described in SECY-90-016 and SECY-93-087.

19.2.4.3.2.7 *Equipment Survivability*

SECY-90-016 and SECY-93-087 present the staff's position, which was approved by the Commission, that there will be reasonable assurance that the severe accident mitigation features should be designed with reasonable assurance that they will operate during credible severe accidents over the duration for which they would be needed. The regulation in 10 CFR 50.34(f)(2)(ix)(c) requires that equipment survivability should consider an accident with the release of hydrogen generated by the equivalent of a 100 percent fuel-cladding metal-water reaction.

Equipment and Instrumentation Necessary to Survive. The U.S. EPR severe accident systems design is based on the conservative assumption that all severe accident scenarios result in RPV failure, and the recovery of failed equipment is not credited. That is, if equipment fails or becomes unavailable at any time during the accident, it will not be repaired or made available. Systems specifically designed for the environmental conditions anticipated during a severe accident within the RCS and the containment are:

- RCS and SADVs
- CMSS
- CGCS
- SAHRS

Only those components within the containment boundary are subject to a severe accident environment (e.g., pressure, temperature, humidity, radiation). Therefore, primary depressurization system, CMSS, and CGCS components are qualified for the expected containment ambient conditions. The main components of SAHRS, namely the pump, isolation valves, and the heat exchanger are located in the SB, and are therefore qualified for the expected conditions in that building.

Table 19.2-1 of this report summarizes the equipment and instrumentation that are required to carry out severe accident functions.

Table 19.2-1 Severe Accident Equipment and Instrumentation (from FSAR Tier 2, Table 19.2-3)

Function / Systems	Monitored Variables	
RCS depressurization/PDS	Valve status indications	RCS pressure RCS temperature
Debris cooling / CMSS	RPV wall temperature Flooding valve status Basemat cooling channel thermocouple status	Chimney area temperature Flooding flow rate
Hydrogen control / CGCS	Mixing dampers status indications PAR	Containment H2 concentration
Containment pressure control and heat removal / SAHRS	SAHRS Pump variables status SAHRS Valves status SAHRS Sump level SAHRS Ventilation flaps status	Containment pressure IRWST water level IRWST temperature Sump screen pressure drop SAHRS heat exchanger temperature
Containment heat removal (support)/CCWS-ESWS	CCWS Pump variables status CCWS sump level CCWS heat exchanger temperature CCWS water supply valve status	Surge tank variables status ESWS Pump status Sump screen pressure drop ESWS flow
Containment/Annulus radiation	MSIRV position Area radiation monitoring Stack radiation and flow rate Annulus pressure	SB ventilation flow rate SB Radiation monitoring Annulus radiation monitoring Annulus ventilation flow rate

Severe Accident Environmental Conditions. The applicant used a series of MAAP simulations as part of the uncertainty analysis to predict environmental conditions (pressure, temperature, and radiation) for equipment survivability in a severe accident. The results of the uncertainty analysis provide a range of minimum and maximum values for environmental conditions for credible severe accident scenarios. The following summarizes the environmental conditions for the severe accident mitigation equipment and instrumentation.

RCS and PDS Valves. The operability of the RCS temperature instruments during a severe accident must be ensured for temperatures and pressures of up to 1,000 °C (1,832 °F), and 299 bars (2,900 psia), respectively. A core outlet temperature of at least 1,250 °C (2,282 °F) is expected. As the severe accident progresses after the RCS depressurization, the temperature at the core outlet could exceed the thermocouple qualification range, and the thermocouple could fail before the RPV fails. Continuous RCS pressure monitoring until RPV failure should remain available, even if the hot leg and pressurizer gas temperature have exceeded 1,200 °C (2,192 °F).

For reliable opening of the PDS valves, which occurs when the core outlet temperature is 922 °K (1,200 °F), the valves are qualified for temperatures up to 873 K (1,112 °F). The PDS

capabilities are required until RPV failure; therefore, reliable valve position would be needed up to pressurizer gas temperature of 1,273 K (1,832 °F).

Inside Containment. The maximum containment temperature and pressure that the equipment and instrumentation may be exposed to during a progression of a severe accident are about 483 K (410 °F), and 0.524 MPa (77 psia), respectively. The maximum humidity for equipment operability is assumed to be 100 percent. The water in the IRWST is expected to reach 407 K (257 °F), and the SAHRS is designed for a maximum IRWST water temperature of 433 K (320 °F).

As indicated earlier in FSAR Tier 2, Section 19.2.3.3.2.2, localized hydrogen detonation and deflagration-detonation transition have been excluded. An evaluation of hydrogen combustion (slow deflagration) using AICC was performed to estimate maximum containment pressure. The AICC pressure is a purely theoretical value that cannot be reached in practice because combustion is neither adiabatic nor isochoric, and may not be complete. Nevertheless, the applicant indicated that since the highest AICC pressure and temperature of 0.714 MPa (105 psia) and 1,163 K (1,634 °F) were reached, equipment and instrumentation capabilities for this extended operational range need to be addressed.

The applicant performed a deterministic analysis of the direct dose radiation environment in the U.S. EPR buildings, as well as the submersion dose for accident conditions. Based on an assumption of complete core radioactive inventory release, realistic assumptions for partitioning of the fission product groups between sump water and containment atmosphere, and corresponding beta and gamma source strengths, radiation levels inside the containment were assessed. The calculated doses inside containment due to air-borne or deposited gamma radiation in a severe accident after 24 hours and 1 year, respectively, were conservatively estimated in FSAR Tier 2, Section 19.2.4.4.5.2 to be about 400 and 6,815 kilo-Grey (kGy). The gamma radiation from activities in the IRWST after one year was estimated to be 4,640 kGy.

Reactor Cavity. The applicant assessed the structural integrity of the reactor cavity walls and floor due to the mechanical and thermal loading caused by severe accidents. The assessment was performed to demonstrate analytically that an RPV failure does not cause impairment of the melt retention capability, a loss of structural integrity, or breach of the liner. The study considered the impact of a detached RPV lower head plus the contained melt, a 1.97 MPa (290 psia) reactor cavity overpressure, a temperature transient due to heat diffusion through the protective layer, thermal radiation, and convective heat transfer from gas during MCCI. The results indicated a post cracking regime in concrete and large deformation and plasticity in the impacted RPV shell and rebars, but with significant margin to failure. The crack patterns at 1.97 MPa (290 psia) overpressure indicated through-cracking but no concrete crushing, which would diminish the temporary retention and condition function of the reactor cavity.

Safeguard Building. SB 4, which houses SAHRS equipment with the exception of the spray system is not exposed to any severe accident-related conditions until the SAHRS is activated. After the SAHRS starts, contaminated IRWST water flows through the system. This water has a maximum temperature of 125 °C (257 °F). Calculations of gamma radiation from IRWST water indicate a dose of about 260 kGy, at 1 m (39 in.) from the pipes, after one year, and a dose of 334 kGy in the SAHRS compartment due to leaked fluid on the floor after 100 hours.

Reactor Building Annulus. The annulus is to withstand a maximum over-pressure of 10.34 kPa (1.5 psig), or a pressure of 0.11 MPa (16 psia), which is limited by the strength of the doors. The temperature within the annulus does not significantly exceed initial conditions as a result of

a severe accident. The cumulative dose inside the annulus is assessed to be 144 kGy after 24 hours and 3,168 kGy after 1 year.

Staff Evaluation. The environmental conditions inside the RCS, containment, SAHRS compartments, and annulus in a severe accident event can be harsher than those during a design-basis accident. The instrumentation and equipment identified herein are relied upon to mitigate the consequences of a severe accident during these beyond design-basis accidents. The environmental conditions are used to specify the conditions in which the equipment operates. By using equipment that is qualified for use in these beyond-design-basis accident conditions, the staff agrees that the U.S. EPR reliably minimizes the consequences of a severe accident and prevents containment failure.

The applicant carried out a systematic evaluation to evaluate the capability of the equipment necessary to survive in a severe accident environment in the U.S. EPR and to demonstrate reasonable assurance of operability. In doing so, the applicant considered: physical location, design or qualification in comparison to the severe accident environment, timing of the required equipment function, nature of the equipment function, duration of the severe accident condition, and material properties. The severe accident environment was established by evaluating credible representative severe accident scenarios, as well as a non-mechanistic 100 percent fuel-clad metal-water reaction. The evaluation identified the equipment, instrumentation, and environmental conditions for qualification to achieve a controlled, stable plant condition over the required time span, both during and after the accident.

The staff requested that the applicant provide the details of its severe accident equipment evaluation in RAI 6, Question 19-113. In a July 7, 2008, response, the applicant provided a very instructive time line in Figure 19-113-2 for bounding containment temperatures and pressures during the various severe accidents analyzed. The staff reviewed the response and concludes that Figure 19-113-2 can be used to derive valuable insights for severe accident management activities. Moreover, the bounding temperatures and pressures are such that equipment such as PARs, hydrogen monitors, hydrogen dampers and foils, valves and their position sensors, temperature sensors, IRWST level and temperature indicators, and containment radiation level measuring devices would withstand the severe accident environmental conditions.

19.2.4.3.2.8 *Containment Venting*

The U.S. EPR design does not include a dedicated severe accident containment venting system. Containment over-pressure protection is provided through the U.S. EPR large, high-strength containment along with the passive autocatalytic hydrogen recombiners, and a severe accident heat removal system to remove hydrogen and steam, the primary sources of containment pressurization. The functions of these systems are described in FSAR Tier 2, Sections 19.2.3.3.2 and 19.2.3.3.3.

19.2.4.4 *FSAR Tier 2, Section 19.2.4: Containment Performance Capability*

The staff has reviewed the structural performance of the U.S. EPR containment to withstand the internal pressure and temperature loads induced by postulated severe containment phenomena. The containment structural performance and capacity to withstand pressure loads induced by internal initiated events are described in FSAR Tier 2, Sections 19.2.4 and 19.2.4.2.1.3. The containment ultimate pressure capacity evaluations are documented in FSAR Tier 2, Section 3.8.1.4.11. The U.S. EPR containment design and structural characteristics are described in FSAR Tier 2, Sections 3.8.1 and 3.8.2.

FSAR Tier 2, Section 3.8 describes the physical characteristics of the containment design for the U.S. EPR design certification. The RCB is a post-tensioned concrete pressure vessel and is located inside the RSB which is of a steel-lined reinforced concrete structure. The RSB protects the RCB from severe accident loads initiated from external events such as winds, tornados, etc. An annulus space between the RSB and the RCB is afforded to provide access for inspections and prevents any contact between the two structures.

The RCB structure is designed to resist various combinations of dead loads; live loads; environmental loads (including earthquakes), and loads generated by a postulated LOCA. The primary function of the RCB structure is to provide the principal barrier to control potential fission product releases to the environment (refer to GDC 16) and GDC 50, described under "Regulatory Criteria"). A leaktight steel liner plate covers the entire inner surface of the RCB and the basemat. The containment houses the RCS, IRWST, and parts of the main steam and feedwater lines. The EPR containment is designed to withstand a maximum pressure of 0.427 MPa (62 psig) and a maximum design temperature of 201.7 °C (395 °F). The RCB is also designed for a negative pressure of – 0.02 MPa (-3.0 psig).

This section describes the staff's assessment of the U.S. EPR containment structural performance based on the information provided in the FSAR. The staff used the review criteria as described below to perform the review and evaluation of the FSAR and to determine the adequacy of the applicant's assessment of the containment structural performance.

19.2.4.4.1 Containment Performance Evaluation

19.2.4.4.1.1 *10 CFR 50.44 Requirement*

10 CFR 50.44, "Combustible Gas Control for Nuclear Power Reactors," provides the requirement for combustible gas control within the containment for light-water cooled reactors. Section 50.44(c)(5) requires that an analysis be performed to demonstrate the containment structural integrity and the analysis must address loads generated in an accident that releases hydrogen from 100 percent fuel clad-coolant reaction accompanied by hydrogen burning. RG 1.70, Revision 3 provides a method that the NRC staff considers acceptable for meeting the 10 CFR 50.44(c)(5) requirement for containment structural performance under the internal pressurization from hydrogen concentration and burning.

FSAR Tier 2, Section 19.2 provides an evaluation of the ability of the U.S. EPR containment to withstand system-related containment challenges associated with potential in-containment hydrogen generation. The U.S. EPR does not employ an inerted containment. The U.S. EPR containment design relies on the CGCS and HMS for hydrogen control and mitigation.

The hydrogen initiated combustion process can be classified into two regimes: Deflagration and detonation. A deflagration is a laminar combustion process where the flame speed or the combustion front is sub-sonic, while a detonation is a combustion process where the flame speed is sonic or supersonic. The deflagration is further divided into slow deflagration [speed less than 100.6 m/sec (330 ft/sec)] and fast deflagration [speed greater than 100.6 m/sec (330 ft/sec).The latter is produced as a result of flame acceleration which is also the driving mechanism for detonation. To provide reasonable assurance that structural integrity is not compromised, the U.S. EPR assesses containment structural integrity with respect to two phenomena: (1) global hydrogen deflagration and (2) flame acceleration.

For global deflagration, the AICC analysis was performed by the applicant for the EPR containment. The applicant's AICC analysis assumes that any hydrogen in containment would

undergo complete combustion in a constant volume and there would be no heat transfer to the outside volume. Therefore, the applicant concluded that the containment pressure load generated by the AICC analysis represents a bounding analysis for global deflagration. The applicant's calculated AICC pressure for the containment to be 0.724 MPa (105 psia) (0.6 MPa or 90.5 psig).

According to the applicant, the pressure loads from a detonation or flame acceleration are the result of dynamic pressure caused by the combustion front. Loads resulting from flame acceleration may not be bounded by the calculated AICC pressure. The applicant stated that, to eliminate the possibility of flame acceleration, the sigma index was used for the assessment of flame acceleration for all compartments, except for the reactor cavity and the corium spreading room, due to the presence of corium, which will auto-ignite hydrogen.

The sigma index is the ratio of the expansion sigma (density of the gas before combustion divided by the density of the gas after non-isochoric combustion) to an experimentally established sigma limit. As long as the sigma index remains less than 1.0, flame acceleration does not exist. For situations where the sigma index is greater that 1.0, flame acceleration cannot be excluded. FSAR Tier 2, Figure 19.2-8, "Tolerance Limit Plot of Sigma Index for the Pump/SG Compartment," shows the sigma index for the pump/SG compartment (representative of the worst location for all cases) to be less than 1.0. Therefore, the risk for flame acceleration is negligible.

FSAR Tier 2, Section 19.2, concluded that the containment is designed with adequate capacity to withstand pressure loads induced by a 100 percent fuel-clad coolant reaction, therefore meeting the requirement of 10 CFR 50.44.

The staff has determined that the AICC methodology is conservative because it assumes detonation or deflagration is complete, takes place in a constant volume, and is adiabatic, all of which maximize the calculated pressure, nonetheless, the review by the staff has identified two major issues.

First, the AICC analysis, was relied on for estimating the U.S. EPR containment pressure from global deflagration; however, there is no discussion regarding how the accident scenario assuming 100 percent fuel clad-fuel reaction followed by hydrogen burning was presented in the AICC analysis.

Second, 10 CFR 50.44(c)(5) requires a structural analysis of the containment under an internal pressurization resulting from 100 percent fuel clad-fuel reaction followed by hydrogen burning. RG 1.70 provides guidance for meeting 10 CFR 50.44(c)(5) by demonstrating that the resulting containment structural demands do not exceed the Service Level C (Factored Loads for concrete containments) allowable limits specified in the ASME B&PV Code Section III. Since the applicant has not provided the Service Level C analysis for the containment, the staff issued RAI 234, Question 19-305, requesting that the applicant provide the following information:

- An analysis which estimates the containment internal pressure load time history due to the hydrogen released by assuming 100 percent fuel clad-fuel reaction followed by hydrogen burning.

- A structural analysis of the containment subject to the pressure load as determined in Step 1 plus the dead load (guidance is provided in RG 1.70, Rev 3); the Code specified minimum material properties at the accident temperature

should be used in the analysis (however, the temperature load should not be included).

- Demonstrate that the containment response in terms of the liner strain determined from the Step 2 analysis remains below the ASME Service Level C limit.

On October 30, 2009, the applicant provided a response to RAI 234, Question 19-305. The response is currently under staff review. **RAI 234, Question 19-305, which is associated with the above request, is being tracked as an open item.**

Due to the open item that remains to be resolved for this section, the staff was unable to finalize its conclusion regarding acceptability.

19.2.4.4.1.2 *SECY-93-087 Deterministic Containment Performance*

FSAR Tier 2, Section 19.2.4, addresses the SECY-93-087, Section I.J, guidance regarding the deterministic assessment of containment performance under the pressure and temperature loads generated for the more likely accident scenarios. The more likely accident scenarios were examined using the results from Level 1 PRA. The criterion for screening the accident scenarios is to identify the associated initiating events whose contribution to CDF exceeds 1.0E-08/yr. Since this 1.0E-8/yr threshold captured categories of events covering over 95 percent of the CDF, the sequences identified should encompass the events most likely to challenge containment structural integrity, which is consistent with SECY-93-087 guidance.

However, SECY-93-087 recommends that the analysis demonstrate that the containment response to the more likely internal challenges is limited to within the ASME Service Level C (factored load) limits. Such an analysis was not provided in the application. Instead, the applicant made a statement that the maximum pressure induced by these accident scenarios is about 0.62 MPa (90 psia) (0.52 MPa or 75.5 psig), which is less than the containment ultimate pressure capacity of 0.82 MPa (119 psig), which the applicant estimated based on a much less stringent criterion than the ASME Service Level C (Factored load). Therefore, to demonstrate that the U.S. EPR containment meets the SECY-93-087 guidance, the staff, in RAI 234, Question 19-306, requested the following information:

- Provide the controlling containment pressure demand in terms of pressure time history and the corresponding temperature time history derived from the more likely accident scenarios.

- Provide a structural analysis of the containment under the pressure load as determined in Step 1 plus the dead load; the Code specified minimum material properties at the accident temperature should be used in the analysis (however, the temperature load should not be included in the containment structural analysis).

- Demonstrate that for the initial 24 hours following the onset of core damage, the containment response in terms of the stresses or strains for containment structural elements as determined from the Step 2 analysis remains below the ASME Service Level C (or Factored Load) limit.

- For the period following 24 hours after the onset of core damage, either demonstrate that the pressure and temperature time histories are not greater than

those during the initial 24-hour period, or perform additional nonlinear containment structural analysis to demonstrate that the containment still provides a barrier against the uncontrolled release of fission products.

- On October 30, 2009, the applicant provided a response to RAI 234, Question 19-306. The response is currently under staff review. **RAI 234, Question 19-306, which is associated with the above request, is being tracked as an open item.**

Due to the open item that remains to be resolved for this section, the staff was unable to finalize its conclusion regarding acceptability.

19.2.4.4.1.3 *Containment Pressure Fragility*

The estimate for containment pressure fragility for the U.S. EPR is described in FSAR Tier 2, Section 19.1.4.2.1.3. The containment pressure fragility is used in the Level 2 PRA to quantify the containment performance as a barrier to releases of fission products. The fragility is expressed as a cumulative probability of containment failure given an internal pressure induced by a postulated severe accident scenario. To develop an estimate of containment pressure fragility, knowledge of the containment structural capacity to withstand pressure loads is necessary.

FSAR Tier 2, Section 19.1.4.2.1.3, provides a high-level description of the development of the containment pressure fragility estimate. It includes a best estimate structural assessment of the containment to identify important failure modes and calculated failure pressures, as well as uncertainty from material properties, construction practices, and analytical methods. FSAR Tier 2, Table 19.1-21 presents the containment failure probability distributions for six dominant containment failure modes. A logarithmic normal probability model was used in these calculations. Based on the review of this table, it appears that only failure locations, but not the failure modes, were provided.

The applicant established a composite fragility curve, which is presented in FSAR Tier 2, Figure 19.1-8. The applicant determined the fragility for a containment temperature of 170 °C (338 °F), as opposed to the maximum design temperature of 201.7 °C (395 °F). No discussion was provided in the FSAR regarding how the failure probability for the six failure modes was used to develop the composite containment fragility.

Since the FSAR lacks a description of a specific analytical process used to determine the containment pressure fragility and associated failure modes, the staff issued RAI 234, Question 19-307, requesting that the applicant provide the following information:

- An analytical approach to determining containment fragility which considers both aleatoric and epistemic (data and model) uncertainties

- Failure criteria

- Various accident conditions that could lead to containment over-pressurization. Specifically, the degradation effect of elevated temperatures on material properties.

In a July 13, 2009, response, the applicant provided a detailed description of the methodology fragility for determining and identified critical locations for U.S. EPR containment response to over-pressurization.

According to the applicant's response, the U.S. EPR containment is sub-divided into six areas, which, when assembled together, can be represented by a continuous model of the entire containment structure. These areas are the cylindrical wall, spherical dome, dome belt, gusset (the connection from the wall to the foundation), and the equipment hatch (horizontal and vertical sections). Major penetrations, and personnel and emergency airlocks are not currently modeled, because design details for these will be developed later in the design process. The applicant selected boundaries of the six areas modeled so that each area covers a pressure boundary location in the containment, and for each such location, the most limiting failure mode is analyzed.

The applicant calculated containment fragility based on the composite fragility representing the sum of the probabilities of failure of the six critical areas identified for the containment. The applicant used a Monte Carlo sampling to select the highest probability of failure from the six critical areas to construct the composite fragility for the containment. Using this approach, the failure dependencies among these critical areas will not affect the containment fragility, because the containment fragility will always reflect the weakest of the six critical areas. Accordingly, the staff concludes that the applicant addressed the uncertainties identified in RAI 234, Question 19-307.

The applicant established failure criteria based on the material strain limits. Material properties and associated uncertainty estimates were provided for an ambient temperature of 21.1 °C (70 °F) and a LOCA condition corresponding to a containment inner surface temperature of 153.9 °C (309 °F). In addition, the applicant indicated that NUREG/CR-6906 observes that temperature up to 204.4 °C (400 °F) has only a small effect on the ultimate pressure capacity of the containment since cracked concrete carries no tension regardless of temperature, and temperature up to 204.4 °C (400 °F) has only a minor effect on typical rebar properties. The staff has reviewed the failure criteria and material properties, and has determined that they were reasonably established in view of the conclusions in NUREG/CR-6906, and since the material properties are comparable to those typically used in current containment fragility analysis.

Based on the above discussion, the staff concluded that the issues raised by the staff have been adequately addressed by the applicant, and the staff considers RAI 234, Question 19-307 resolved.

19.2.4.4.2 Summary

Section 19.2.4 of this report provides the staff's review and evaluation of the applicant's assessment of the U.S. EPR containment structural performance. The staff focused its review on the ability of the structural components comprising the containment pressure boundary to meet: (1) 10 CFR 50.44 requirements, and (2) SECY-93-087 guidance for deterministic containment performance. The staff's review also focused on evaluating the adequacy of the applicant's assessment of containment pressure fragility.

On the basis of its review, the staff identified a number of safety issues and issued RAIs requesting additional information from the applicant. The staff concludes that the acceptance of the applicant's containment structural performance evaluation will be contingent upon the successful resolution of the issues identified in the sections above.

19.2.4.5 *FSAR Tier 2, Section 19.2.5: Accident Management*

Accident management consists of the actions taken by the plant's emergency response organization (including plant operations, technical support, and management staff), to prevent core damage, terminate core damage once it begins, maintain containment integrity, and minimize offsite radiation releases. Severe accident management refers to those actions that would mitigate the consequences of accidents that result in core damage. The objectives of a severe accident management program are to arrest core melt progression by cooling the molten core material, either in-vessel if possible, or ex-vessel if the debris has entered the containment building, and to ensure that fission products are not released to the environment. The ultimate objective is to achieve a safe, stable state. To accomplish these objectives, the emergency response organization should make full use of the plant's design features, including both standard and non-standard use of plant systems and equipment.

The nuclear power industry initiated a coordinated program on accident management in 1990 (Section 5 of NEI 91-04, Revision 1, "Severe Accident Closure Guidelines," lays out the elements of the industry's severe accident management closure actions that have been accepted by the NRC). This program involves the development of (1) a structured method by which utilities may systematically evaluate and enhance their abilities to deal with potential severe accidents, (2) vendor-specific accident management guidelines for use by individual utilities in establishing plant-specific accident management procedures and guidance, and (3) guidance and material to support utility activities related to training in severe accidents. Using the guidance developed through this program, each operating plant has implemented a plant-specific accident management plan as part of an industry initiative.

Based on the staff's review of these efforts, severe accident evaluations in Individual Plant Examinations (IPEs), and industry PRAs, the staff has concluded that improvements to utility accident management capabilities could further reduce the risk associated with severe accidents. Although future reactor designs such as the U.S. EPR will have enhanced capabilities for the prevention and mitigation of severe accidents, accident management will remain an important element of defense-in-depth for these designs. However, the increased attention on accident prevention and mitigation in these designs can be expected to alter the scope and focus of accident management relative to that for operating reactors. For example, increased attention on accident prevention and the development of error-tolerant designs can be expected to decrease the need for operator intervention, while increasing the time available for such action if necessary. This will tend to make it less likely for the emergency response organization to make rapid decisions and permit a greater reliance on support from outside sources. For longer times after an accident (several hours to several days), the need for human intervention and accident management will continue.

For both operating and advanced reactors, the overall responsibility for accident management, including development, implementation, and maintenance of the accident management plan, lies with the nuclear plant operator, because the plant operator bears ultimate responsibility for the safety of the plant and for establishing and maintaining an emergency response organization capable of effectively responding to potential accident situations. For operating plants, vendors have played key roles in providing essential severe accident management guidance and strategies for implementation. This guidance has served as the basis for severe accident management procedures and for training personnel in carrying out the procedures. Computational aids for technical support have been developed, information needed to respond to a spectrum of severe accidents has been provided, decision-making responsibilities have been delineated, and utility self-evaluation methodologies have been developed and utilized.

Severe accident management in the U.S. EPR begins with several design elements specifically addressing the stated objectives of maintaining fuel, RPV, and containment integrity while minimizing radiological releases. These design elements are described in FSAR Tier 2, Sections 19.2.2 and 19.2.3. Severe accident management encompasses those actions taken during the course of an accident by the plant operating and technical staff to:

- Prevent core damage
- Terminate the progress of core damage if it begins and retain the core within the reactor vessel
- Maintain containment integrity as long as possible
- Minimize offsite releases

The applicant has developed a new approach to severe accident management guidance in a project called Operating Strategies for Severe Accidents. The OSSA framework makes maximum use of the lessons learned to date in the field of severe accidents and incorporates a number of new features, which simplify and streamline the guidance material while maintaining comprehensive guidance for response to any severe accident. The ultimate goal for the OSSA is to provide mitigation strategies to cover all potential events that lead to core melt and to stop or reduce the releases of fission products to the environment.

The prevention of core damage is considered to be within the domain of emergency operating procedures. Once a specified set of plant conditions [i.e., core exit temperature greater than 922 K (1,200 °F)] is met, use of EOPs is abandoned and control switches to the OSSA. The OSSA is developed based on a list of possible challenges to severe accident mitigation and the corresponding instrumentation used to assess safety margins. Based on the challenges that may be present, appropriate actions are derived based on the deterministic process studies using MAAP4.07.

The U.S. EPR employs an ex-vessel severe accident mitigation strategy. The severe accident features addressing ex-vessel behavior are passive in nature for 12 hours following the onset of a severe accident and consequent operator response to initiate RCS depressurization. By the end of the 12-hour period, the melt is expected to have been transferred into the spreading room where water passively delivered from the IRWST will reside in a pool above the spread melt.

Beyond this 12-hour period, the event enters the long-term cooling phase, which involves active operator response, beginning with actuation of the SAHRS. During this event phase, the spreading compartment, adjoining chimney vent, and reactor cavity are flooded. The flooding response serves to both remove decay heat and contain fission products. The SAHRS also controls containment pressure through condensation of resident water vapor.

As discussed below, a COL applicant referencing the U.S. EPR certified design will review final plant-specific EOPs and SAMGs to confirm that the assumptions used in the severe accident analyses remain valid. The staff determined that the applicant should provide to the COL applicant the technical basis for the U.S. EPR severe accident management program, including emergency operating guidelines, to ensure core damage prevention and mitigation, and meeting the offsite dose limits. To further clarify the exact nature of the information transfer, RAI 45, Question 19-192 was issued to the applicant to identify a COL action item that would call for a

COL applicant to provide documentation of the severe accident management technical basis for NRC review. This information should include the following:

- A discussion of the various sequences considered, and the range of possible challenges to accident mitigation
- The results of MAAP 4.0.7 analyses that support the development of the SAMGs
- The sets of high level and in-depth mitigation strategies to be used by the technical support center during a postulated severe accident

The applicant's September 19, 2008, response to RAI 45, Question 19-192, contained insufficient information, and follow-up RAI 133, Question 19-243, was issued, requesting the applicant to provide additional information for severe accident mitigation strategies including:

- Recommendations for the various accident scenarios being considered, regarding how best to prevent the accidents from progressing to core damage, terminate core damage once it begins, maintain the capability of the containment as long as possible, and minimize on-site and off-site releases and their effects
- Identification of a COL action item that would require each COL applicant to provide documentation of the severe accident technical basis

In a June 19, 2009, response, the applicant provided a detailed description of the AREVA OSSA methodology technical basis and its application to the U.S. EPR design. The applicant emphasized that both the in-vessel and ex-vessel strategies will be developed. The ex-vessel strategy will only be used after in-vessel strategies have been exhausted. The applicant claimed that the information provided in this response, coupled with the information in FSAR Tier 2, Chapter 19, was sufficient to support the development and implementation of SAMG. The applicant also committed to provide a COL information item to complete the development and implementation of SAMG. The following COL information item will be added to FSAR Tier 2, Section 19.2.5 and Table 1.8-2:

> A COL applicant that references the U.S. EPR design certification will develop and implement severe accident management guidelines prior to fuel loading using the Operating Strategies for Severe Accidents methodology described in FSAR Tier 2, Section 19.2.5.

The response to RAI 133, Question 19-243 is still under review and is being tracked as an open item.

The staff will review the accident management plan at the COL stage and audit each COL applicant to assure that the evaluation process and commitments proposed by the COL applicant provide an acceptable means of systematically assessing, enhancing, and maintaining accident management capabilities, consistent with NRC guidance. The COL applicant should develop this plan based on the final, as-built plant, the accident management-related information developed by the plant designer, and the accident management program guidance developed for the current generation of operating reactors.

19.2.4.6 *FSAR Tier 2, Section 19.2.6: Consideration of Potential Design Improvements*

19.2.4.6.1 Introduction and Regulatory Criteria

In 10 CFR 52.47(b)(2), the NRC requires applicants for standard design certification to perform an environmental report required by 10 CFR 51.55, "Environmental report—standard design certification." Section 51.55(a) requires the design certification applicant to "address the cost and benefit of severe accident mitigation design alternatives, and the bases for not incorporating severe accident mitigation design alternatives in the design to be certified."

In 10 CFR 50.34(f)(1)(i), the NRC requires an applicant to "perform a plant/site specific PRA, the aim of which is to seek such improvements in the reliability of core and containment heat removal systems as are significant and practical and do not impact excessively on the plant." The applicant provided a brief evaluation of potential design improvements (SAMDA) for the U.S. EPR in FSAR Tier 2, Section 19.2.6, and a detailed evaluation in, "AREVA NP Environmental Report Standard Design Certification," ANP-10290 Revision 1, September 2009.

Based on this evaluation, the applicant has concluded that because of the small risk associated with the U.S. EPR design, the majority of the design improvements beyond those that already exist as part of the design either were of procedural and administrative nature, or were not considered to be cost beneficial. The staff's review of the evaluation is presented below.

The initial staff review determined that the applicant's evaluation did not contain sufficient information on addressing uncertainties in the estimated benefits from potential SAMDA implementation. In an August 8, 2008, response to RAI 6, Question 19-121, the applicant provided additional information justifying the method used and conclusion reached. The review identified additional shortcomings in that response, which resulted in follow-up questions (RAI 22, Question 19-160, RAI 45 Question 19-190, and RAI 133, Questions 19-236 through 19-238), as discussed below.

19.2.4.6.2 Estimate of Risk for the U.S. EPR

As stated earlier in Section 19.1.4.3, the applicant did not perform a Level 3 PRA as part of design certification process. Therefore, the applicant used core damage frequency and large release frequency as surrogate risk measures for meeting the Commission's safety goals. The risk measure results for CDF, LRF, and CCFP are summarized in Section 19.1.4.13 of this report. 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 is 0.05.

The staff found some discrepancies in the inputs to the off-site consequence calculations, and requested, in RAI 236, Question 19-313, dated June 12, 2009, that the applicant provide corrected core radionuclide inventories and release category frequencies. In a September 11, 2009, response, the applicant provided the requested information. The staff accepted the response and considers the issue closed.

19.2.4.6.3 Identification of Potential Design Improvements

The applicant identified 167 candidate design alternatives based on a review of the design alternatives for other plant designs, including the License Renewal Environmental Reports, as provided in NEI 05-01 [Nuclear Energy Institute, "Severe Accident Mitigation Alternatives

(SAMA) Analysis Guidance Document," NEI 05-01, Revision A, November 2005.]. Cutsets from the U.S. EPR Level 1 and Level 2 PRA were evaluated to identify plant-specific modifications for inclusion in the comprehensive list of SAMDA candidates. The top 100 Level 1 cutsets were examined – these encompass about 50 percent of the total CDF. This evaluation produced the comprehensive list of SAMDA candidates. Then, in response to RAI 22, Question 19-160, dated September 5, 2008, the top 100 Level 2 cutsets that contribute to LRF were evaluated to identify modifications that would reduce the likelihood of significant containment challenges. Evaluating these cutsets did not identify any additional SAMDA candidates.

The SAMDA candidates were characterized as both hardware (i.e., modifications to plant components, systems, and structures), and non-hardware (i.e., modification to operation and maintenance procedures and programs) changes. The applicant excluded non-hardware modifications, because they cannot be considered until the COL process for actual plants. The applicant also eliminated certain design improvements from further consideration because they either are not applicable to the U.S. EPR design, have very low benefits, have excessive implementation costs, or have already been incorporated into the design. Examples of design enhancement features already included in the design are the following:

- Primary Depressurization System
- Core Melt Stabilization System
- Enhanced DC power reliability
- In-containment Refueling Water Storage Tank
- Increased maximum design pressure
- 12-hour battery coping period
- Digital controls and instrumentation

Based on the applicant's screening process, 21 potential alternatives were eliminated as being not applicable, 69 design alternatives were considered to be similar to those already included in U.S. EPR design, 46 items were identified as procedural or administrative as opposed to design features (whose benefits are beyond the scope of the design certification application), 26 items were eliminated on the basis of their high cost relative to potential benefits. Finally, five training- and procedure-related items were considered to be not required for design certification.

19.2.4.6.4 Risk Reduction Potential of Design Improvements

The applicant assumed that each design alternative would work perfectly to completely eliminate all severe accident risk from evaluated internal events. This assumption is conservative, as it maximizes the benefit of each design alternative.

The applicant used the cost-benefit methodology of NUREG/BR-0184 [U.S. Nuclear Regulatory Commission, "Regulatory Analysis Technical Evaluation Handbook," NUREG/BR-0184, January 1997] to calculate the maximum attainable benefit associated with completely eliminating all risks. This methodology includes consideration of averted onsite and replacement power costs. The applicant used values related to the point estimate CDF in its evaluations.

The staff issued RAI 133, Question 19-236, requesting the basis for not using mean CDF values. In a February 11, 2009, response to RAI 133, Question 19-236, the applicant stated that point estimate values were used, because point estimate value is stable and the mean CDF value could vary significantly from one Monte-Carlo run to another. This response put in question the validity of various CDF quintiles (e.g., 5th, 50th, 95th, etc.) reported in the FSAR. The staff issued RAI 236, Question 19-311, requesting that the applicant confirm the reported mean values as well as the uncertainty distributions are numerically reasonable representations of uncertainty bands and are not significantly affected by the Monte-Carlo sampling process. In a July 13, 2009, response to RAI 236, Question 19-311, the applicant stated that a series of Monte-Carlo runs was performed, showing that the variation in mean CDF values would not exceed 15 percent, and variations in 5, 50, and 95 percentiles are less than five percent. In addition, the applicant considered mean CDF values for the evaluation of the estimated averted cost, as a sensitivity analysis, and concluded that no additional plant modifications are cost beneficial. The applicant's response was determined to be satisfactory, and fluctuations introduced by the applicant's Monte-Carlo simulations, which are typical, would not be expected to impact any conclusions.

The applicant then estimated the present worth of eliminating all severe accident risk to be about $53,063 (using the point estimate CDF) and $71,040 (using the mean value CDF). The applicant estimated the maximum benefit including seismic to be $70,574 (using the point estimate CDF) and $90,931 (using the mean value CDF), based on an assumption that the seismic risk contribution would be proportional to its core damage frequency contribution (assumed to be equal to that of the internal/fire risk).

The applicant's risk reduction estimates did not consider uncertainties in either the CDF or the offsite consequences. Even though this approach is consistent with that used in previous design alternative evaluations, further consideration of these factors could lead to significantly higher risk reduction values, given the extremely small CDF and risk estimates in the baseline PRA. On the other hand, the staff has based its evaluation of the risk reduction potential of design improvements for the U.S. EPR on the applicant's risk reduction estimates for the various design alternatives, in conjunction with an evaluation of the potential impact of uncertainties on the results. This staff evaluation is discussed further below.

19.2.4.6.5 Cost Impacts of Candidate Design Improvements

The applicant did not explicitly assess the capital costs associated with the various design alternatives evaluated. Instead, the applicant used the estimated costs of back fitting of similar SAMDA as provided by applicants for license renewal. This approach has a potential to overestimate the actual costs, since the cost of implementing a modification after the design has already been built is always greater than that for a design that has yet to be built. Nevertheless, based on the analyses performed by the applicant, the staff believes that potential costs for the U.S. EPR are reasonable. The staff also notes that the cost estimate determination conformed to the guidelines of NUREG/BR-0184.

19.2.4.6.6 Cost-Benefit Comparison

The methodology used by the applicant was based primarily on NRC guidance in NUREG/BR-0184 for performing the cost-benefit analysis. The guidance involves determining the net value for each SAMDA according to the following formula:

Net Value = (APE + AOC + AOE + AOSC) - COE

Where:

APE = Present value of averted public exposure ($).

AOC = Present value of averted offsite property damage costs ($).

AOE = Present value of averted occupational exposure costs ($)

AOSC = Present value of averted onsite costs ($). This includes cleanup and decontamination, and long-term replacement power costs.

COE = Cost of enhancement ($).

If the net value of a SAMDA is negative, the cost of implementing the SAMDA is larger than the benefit associated with the SAMDA and it is not considered cost-beneficial. The applicant's estimates of each of the associated cost elements are summarized in Table 19.2-2. The provided results are based on the approach, parameters, and data listed in NUREG/BR-0184. As indicated above, the applicant's estimates are based on the point-estimate core damage frequency (i.e., 5.3E-7 /yr). The staff has adjusted the estimated present value using the mean value for CDF for all internal, fire, and flood events (a value of 7.4E-7 /yr).

Table 19.2-2 Summary of Estimated Averted Costs

Quantitative Attributes		Present Value Estimate ($)		
		Point Estimate CDF[a]	Mean Value CDF [b]	Maximum[c]
Health	**Public (APE)**	5,094	11,017	110,170[d]
	Occupational (AOE)	264	607	1,644
Property	**Offsite (AOC)**	2,603	5,063	50,630[d]
	Onsite	NA[e]	NA[e]	NA[e]
Cleanup and Decontamination	**Onsite (AOSC-1)[f]**	TBD	TBD	30,858
Replacement Power	**(AOSC-2)[f]**	TBD Total AOSC is $45,102	TBD Total AOSC is $62,974	117,804
Total (Internal, fire and flood events)		53.063	71,040	311,106
Total (including seismic events)		70,574[g]	90,931[g]	399,393[h]

[a] Based on point estimate core damage frequency, seven percent discount rate, and best estimate parameter values in NUREG/BR-0184.

[b] Based on mean value core damage frequency, seven percent discount rate, and high estimate parameter values in NUREG/BR-0184.

[c] Reviewer-derived maximum is based on mean core damage frequency, three percent discount rate, and high estimate parameter values in NUREG/BR-0184.

[d] Estimate is based on a factor 10 increase in estimated dose risk, or public property risk, to account for potential uncertainties.

[e] Not analyzed by the applicant.

[f] Averted On-site Costs were divided into the cleanup and decontamination costs (AOSC-1) and Replacement power costs (AOSC-2). The applicant provided a lump sum cost for this item. This cost was reallocated using the values given in Reference [19-9].

[g] The applicant increased the benefit by 33 percent, (1+ ratio of internal fire core damage [as a surrogate for the seismic risk] over the total core damage frequency).

[h] The reviewer used similar approach as that used by the applicant, but considered the mean fire core damage frequency of 2.1E-7 per year as given in Figure 19.1-18 of the FSAR. This increases the benefits by about 28 percent.

The applicant provided present value estimates using both three and seven percent discount rates. The applicant presented the estimates using the three percent discount rate as the upper bound value.

It is important to note that the monetary present value estimate for each risk attribute does not represent the expected reduction in risk resulting from a single accident. Rather, it is the present value of a stream of potential losses extending over the projected lifetime of the facility (in this case, 60 years). Therefore, it reflects the expected annual loss resulting from a single accident, the possibility that such an accident could occur at any time over the licensed life, and the effect of discounting these potential future losses to present value.

As indicated above, the applicant estimated the total present dollar value equivalent associated with complete elimination of severe accidents at a single U.S. EPR unit site to range between $70,574 (point estimate CDF) and $90.931 (mean value CDF). The estimated cost of replacement power has the largest effect on the averted cost. In order for any SAMDA to be cost-beneficial, the enhancement cost must be less than $90,931. Using either the point estimate or mean CDF values, the applicant concluded that none of the SAMDA candidates are cost beneficial.

The applicant performed a sensitivity analysis to assess the uncertainty in the maximum benefit calculations, using upper estimates for onsite dose and cleanup costs, and increases in replacement power costs using inflation rates of 3.66 and 10.41 to adjust the 1993 dollar values provided in the NUREG/BR-0184. The calculations were performed on a segregated basis, without consideration of true effects of combination of uncertain inputs. These calculations resulted in an estimated range of benefits between $70,633 and $218,358 using point estimate CDF values, and from $91,009 to $285,697 using mean value CDF values. These results still are lower than maximum value provided in Table 19.2-2. The applicant stated that the minimum

cost of any design change is about $1 million and, therefore, no additional plant modifications are cost beneficial.

The staff analyses of the total present value using the mean CDF and three percent discount rate along with upper bound parameters indicate a maximum value of about $400,000. Even though this value is higher than the range evaluated by the applicant, the staff agrees with the applicant's conclusion that no additional modifications would be cost-beneficial and considers this issue closed.

19.2.4.6.7 Staff Evaluation

In 10 CFR 50.34(f)(1)(i), the NRC requires an applicant to perform a plant-/site-specific PRA. The aim of this PRA is to seek such improvements in the reliability of core and containment heat removal systems that are significant and practical and do not impact excessively on the plant. For the reasons stated above, the staff finds that the U.S. EPR design-specific PRA and the applicant's use of the insights of this study to improve the design of the U.S. EPR meet this requirement.

The set of potential design improvements considered for the U.S. EPR includes improvements from generic PWR SAMA reports. Several design enhancements relative to severe accident mitigation have already been incorporated into the design. These design improvements have resulted in a CDF that is about one to two orders of magnitude less than that of existing PWR designs.

The staff's analyses of the total present value using the mean CDF and a three percent discount rate indicate a maximum value of about $400,000. As indicated in Table 19.2-2, the estimated cost of replacement power has a very large effect on the averted cost. This cost is currently driven based on an estimate of potential replacement power costs in 1993-dollars. If one were to adjust annual replacement power cost, for future energy cost increase, the total present dollar value would be even higher. Using the staff's estimate of maximum benefits and the applicant's provided costs, a number of the SAMDA items could become marginally cost beneficial (i.e., CP-23, CW-22, and FW-03). Nonetheless, given the uncertainties in these estimates and the conservative assumptions necessary for these SAMDA items to be considered even marginally cost beneficial, the staff concludes that they need not be included in the design.

The applicant's review of the potential SAMDA and their impacts on the U.S. EPR design is considered acceptable, except for those items identified in the outstanding RAIs identified above. The staff review did not reveal any additional design alternatives that should have been given consideration by the applicant.

19.2.5 Combined License Information Items

Table 19.2-3 of this report lists the combined license information items applicable to FSAR Tier 2, Section 19.2. The item numbers and descriptions are taken from FSAR Tier 2, Table 1.8-2.

Table 19.2-3 Combined License Information Items

Item No.	Description	FSAR Tier 2 Section	Action Required by COL Applicant	Action Required by COL Holder
19.1-9	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 SAMDA) remain valid with respect to internal events, internal flood and fire events (routings and locations of pipe, cable and conduit), and HRA analyses (development of operating procedures, emergency operating procedures and severe accident management guidelines and training), external events including PRA-based seismic margins HCLPF fragilities, and LPSD procedures.	19.1.2.2 (also referred to in 19.2.6.3)		Y
19.2-1	A COL applicant that references the U.S. EPR design certification will develop and implement severe accident management guidelines prior to fuel loading using the Operating Strategies for Severe Accidents methodology described in FSAR Tier 2, Section 19.2.5.	19.2.5		Y

19.2.6 Conclusions

Based on the technical evaluation of the U.S. EPR PRA documented in the sections above, the NRC staff concludes that the regulatory requirements and SRP acceptance criteria summarized in Section 19.2.3 above have been adequately addressed by the applicant, except for the open items identified in the text.

19.2.7 Design Features for Protection Against a Malicious Aircraft Impact

The applicant submitted, “Supplement to U.S. EPR Final Safety Analysis Report to Add the Beyond Design Basis Large Commercial Aircraft Impact Assessment,” on December 11, 2009. The staff is currently developing a schedule to review this supplement.