19 Severe Accidents

Background

Federal regulations for the design, construction, licensing, and operation of commercial nuclear power plants are defined in Chapter 1 of Title 10 of the Code of Federal Regulations (CFR). The U.S. Nuclear Regulatory Commission (NRC) evaluated the design against these regulations, as documented in the various chapters of this report. Compliance with the Commission's regulations ensures adequate protection of the public health and safety regarding operating of a nuclear power plant. In previous applications, the final safety analysis report demonstrated compliance with these regulations and set forth the design basis of the plant. The Commission has developed guidance and goals for resolving safety issues related to reactor accidents more severe than design-basis accidents. These "severe accidents" are those in which substantial damage is done to the reactor core whether or not there are serious offsite consequences.

Following the accident at the Three Mile Island Nuclear Plant, Unit 2, in 1979, when it was recognized that severe accidents needed further attention, the NRC evaluated, generically, the capability of existing plants to tolerate a severe accident. It was found that the design-basis approach contained significant safety margins for the analyzed events. These margins permitted operating plants to accommodate a large spectrum of severe accidents. Based on this information, the Commission, in the Severe Accident Policy Statement, concluded that existing plants posed no undue risk to public health and safety, and that no basis existed for immediate action on generic rulemaking or other regulatory changes for these plants because of severe accident risk. For operating plants in the long term, the NRC developed the "Integration Plan for Closure of Severe Accident Issues" (SECY-88-147), in which the NRC identified the following necessary elements for closure of severe accidents:

- performance of an individual plant examination
- assessment of generic containment performance improvements (CPI)
- improved plant operations
- a severe accident research program
- an external events program
- an accident management program

Progress continues in these areas for operating plants.

The Commission expects that new designs, like the AP1000, will achieve a higher standard of severe accident safety performance than previous designs. In an effort to provide this additional level of safety in the design of advanced nuclear power plants, the NRC has developed guidance and goals for which designers should strive in accommodating events that are beyond what was previously known as the design basis of the plant.

For advanced nuclear power plants, including both the evolutionary and passive designs, the staff concluded that vendors should address severe accidents during the design stage. This will allow the designers to take full advantage of the insights gained from such input as probabilistic safety assessments, operating experience, severe accident research, and accident analysis by designing features to reduce the likelihood that severe accidents will occur and, in the unlikely occurrence of a severe accident, to mitigate the consequences of such an accident. Incorporating insights and design features during the design phase has been demonstrated to be much more cost effective than modifying existing plants.

Regulatory Guidance

The NRC has issued guidance for addressing severe accidents. This guidance is found in the following documents:

- NRC Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants (*Federal Register* (50 FR 32138) dated August 8, 1985)
- NRC Policy Statement on Safety Goals for the Operations of Nuclear Power Plants (*Federal Register* (51 FR 28044) dated August 4, 1986)
- NRC Policy Statement on Nuclear Power Plant Standardization (*Federal Register* (52 FR 34844) dated September 15, 1987)
- NRC Policy Statement on the Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities (*Federal Register* (60 FR 42622) dated August 16, 1995)
- 10 CFR Part 52, "Early Site Permits; Standard Design Certification; and Combined Licenses for Nuclear Power Plants"
- SECY-90-016 “Evolutionary Light Water Reactor Certification Issues and Their Relationship to Current Regulatory Requirements,” and the corresponding 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,” and the corresponding SRM dated July 21, 1993
- SECY-96-128 “Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design,” and the corresponding SRM dated January 15, 1997
- SECY-97-044 “Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design,” and the corresponding SRM dated June 30, 1997.

Whereas, the first four documents provide guidance as to the appropriate course for addressing severe accidents and the use of PRA, 10 CFR Part 52 contains general requirements for addressing severe accidents, and the SRMs relating to SECY-90-016, SECY-93-087, SECY-96-128, and SECY-97-044 give Commission-approved positions for implementing features in new designs for preventing severe accidents and mitigating their effects.

Severe Accident Policy Statement

The Commission issued the "Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants," on August 8, 1985. The focus of severe accident issues in this policy statement was prompted by the NRC's judgment that accidents of this class, which are beyond the traditional design-basis events, constitute the major remaining risk to the public associated with radioactive releases from nuclear power plant accidents. A fundamental objective of the Commission's severe accident policy was to take all reasonable steps to reduce the chances that a severe accident involving substantial damage to the reactor core will occur and to mitigate the consequences of such an accident, should one occur. This statement described the policy that the Commission intended to use to resolve safety issues related to reactor accidents more severe than design-basis accidents (DBAs). The main focus of the statement was on the criteria and procedures the Commission intended to use to certify new designs for nuclear power plants. Regarding the decision process for certifying a new standard plant design, an approach the Commission strongly encouraged for future plants, the policy statement affirmed the Commission's belief that a new design for a nuclear power plant could be shown to be acceptable for severe accident concerns if it met the following criteria and procedural requirements:

- demonstration of compliance with the procedural requirements and criteria of the current Commission regulations, including the Three Mile Island (TMI) requirements for new plants as reflected in the 10 CFR 50.34(f)

- demonstration of technical resolution of all applicable unresolved safety issues (USI) and the medium- and high-priority generic safety issues (GI), including a special focus on assuring the reliability of decay heat removal (DHR) systems and the reliability of both ac and dc electrical supply systems

- completion of a probabilistic risk assessment (PRA) and consideration of the severe accident vulnerabilities the PRA exposes along with the insights that it may add to providing assurance of no undue risk to public health and safety

- completion of a staff review of the design with a conclusion of safety acceptability using an approach that stresses deterministic engineering analyses and judgment complemented by PRA

The Commission believed that an adequate basis existed from which to establish an appropriate set of criteria. This belief was supported by the current operating reactor experience, ongoing severe accident research, and insights from a variety of risk analyses. The Commission recognized the need to strike a balance between accident prevention and

consequence mitigation and in doing so expected that vendors engaged in designing new standard plants will achieve a higher standard of severe accident safety performance than they achieved with their previous designs.

Safety Goals Policy Statement

The Commission issued the “Policy Statement on Safety Goals for the Operation of Nuclear Power Plants” on August 4, 1986. This policy statement focused on the risks to the public from nuclear power plant operations with the objective of establishing goals that broadly define an acceptable level of radiological risk that might be imposed on the public as a result of nuclear power plant operation. These are the risks from release of radioactive material from the reactor to the environment from normal operations as well as from accidents. The Commission established two qualitative safety goals that are supported by two quantitative objectives. The qualitative safety goals follow:

- Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.

- Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.

The following quantitative objectives were to be used in determining achievement of the above safety goals:

- The risk to an average individual in the vicinity of a nuclear power plant of a prompt fatality that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

- The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.

This statement of NRC safety policy expresses the Commission's views on the level of risks to public health and safety that the industry should strive for in its nuclear power plants. The Commission recognizes the importance of mitigating the consequences of a core-melt accident and continues to emphasize such features as the containment, siting in less populated areas, and emergency planning as integral parts of the defense-in-depth concept associated with its accident prevention and mitigation philosophy. The Commission approves the use of the qualitative safety goals, including use of the quantitative health effects objectives, in the regulatory decisionmaking process.

Standardization Policy Statement

The Commission issued the “Policy Statement on Nuclear Power Plant Standardization” on September 15, 1987. The policy statement encouraged the use of standard plant designs and contained information concerning the certification of plant designs that are essentially complete in scope and level of detail. The intent of these actions was to improve the licensing process and to reduce the complexity and uncertainty in the regulatory process for standardized plants. In relation to severe accidents, the policy statement expected applicants for a design certification to address the four licensing criteria for new plant designs as given in the Commission's Severe Accident Policy Statement.

Use of PRA Methods in Nuclear Regulatory Activities Policy Statement

The Commission issued the “Policy Statement on the Use of Nuclear Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities” on August 16, 1995. This statement presented the policy that the NRC will follow in the use of probabilistic risk assessment methods in nuclear regulatory matters. The Commission established the policy so that the many potential applications of PRA could be implemented in a consistent and predictable manner that would promote regulatory stability and efficiency. The Commission adopted the following policy statement regarding the expanded NRC use of PRA:

(1) The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.

(2) PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. Where appropriate, PRA should be used to support the proposal for additional regulatory requirements in accordance with 10 CFR 50.109 (Backfit Rule). Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.

(3) PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.

(4) The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.

10 CFR Part 52

The Commission issued 10 CFR Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," on April 18, 1989. This rule provides for issuing early site permits, standard design certifications, and combined licenses with conditions for nuclear power reactors. It states the review procedures and licensing requirements for applications for these new licenses and certifications, and was intended to achieve the early resolution of licensing issues and to enhance the safety and reliability of nuclear power plants. Relating to severe accidents, 10 CFR Part 52 codified some of the guidance in the Severe Accident Policy Statement and the Standardization Policy Statement. Specifically, 10 CFR 52.47 requires an application for design certification to include the following:

- demonstrate compliance with any technically relevant portions of the TMI requirements given in 10 CFR 50.34(f)

- propose technical resolutions of those unresolved safety issues and medium- and high-priority generic safety issues which are identified in the version of NUREG-0933 current on the date 6 months prior to application and which are technically relevant to the design

- contain a design-specific PRA

SECY-90-016

On January 12, 1990, the NRC staff issued SECY-90-016 which requested Commission approval for the staff's recommendations concerning proposed departures from current regulations for the evolutionary light water reactors (LWR). The issues in SECY-90-016 were significant to reactor safety and fundamental to the NRC decision on the acceptability of evolutionary LWR designs. The positions in SECY-90-016 were developed as a result of the following activities:

- NRC's reviews of current-generation reactor designs and evolutionary LWRs
- consideration of operating experience, including the TMI-2 accident
- results of PRAs of current-generation reactor designs and the evolutionary LWRs
- early efforts conducted in support of severe accident rulemaking
- research to address previously identified safety issues.

The Commission approved some of the staff positions stated in SECY-90-016 and provided additional guidance regarding others in an SRM dated June 26, 1990.

SECY-93-087

On April 2, 1993, the NRC staff issued SECY-93-087 which sought Commission approval for the staff's positions pertaining to evolutionary and passive LWR design certification policy

issues. This paper was an evolution of SECY-90-016. Preventive feature issues addressed in SECY-93-087 relating to the AP1000 include the following:

- anticipated transient without scram (ATWS)
- mid-loop operation
- station blackout
- fire protection
- intersystem loss-of-coolant accident

Mitigative feature issues addressed in SECY-93-087 relating to the AP1000 include the following:

- hydrogen control
- core debris coolability
- high-pressure core melt ejection
- containment performance
- dedicated containment vent penetration
- equipment survivability
- containment bypass potential resulting from steam generator tube ruptures

The Commission approved some of the staff positions from SECY-93-087 and provided additional guidance regarding others in an SRM dated July 21, 1993.

SECY-96-128

On June 12, 1996, the NRC staff issued SECY-96-128 which sought Commission approval for the staff's position pertaining to the AP600 reactor design. The issues involving severe accidents in this paper, which are also applicable to the AP1000, include the following:

- prevention and mitigation of severe accidents
- external reactor vessel cooling

The Commission provided additional guidance concerning prevention and mitigation of severe accidents, and approved the staff's position concerning external reactor vessel cooling in an SRM dated January 15, 1997.

SECY-97-044

On February 18, 1997, the NRC staff issued SECY-97-044 which provided the Commission with additional information regarding prevention and mitigation of severe accidents. This paper was in response to the Commission's SRM dated January 15, 1997. Specifically, this paper provided additional information regarding the type of non-safety-related system that would achieve an appropriate balance between prevention and mitigation of severe accidents for the AP600 reactor design, which are also applicable to the AP1000 design. The Commission approved the staff's position in an SRM dated June 30, 1997.

Severe Accident Resolution

The basis for resolution of severe accident issues for the AP1000 is 10 CFR Part 52, and SECY-93-087, SECY-96-128, and SECY-97-044, as approved by the Commission. In 10 CFR Part 52, the NRC requires the following criteria:

- compliance with the TMI requirements in 10 CFR 50.34(f)
- resolution of unresolved safety issues and generic safety issues
- completion of a design-specific PRA

The staff evaluates these criteria in Sections 20.6, 20.1 and 20.2, and 19.1 of this report, respectively.

The Commission-approved positions on the issues discussed in SECY-93-087, SECY 96-128, and SECY-97-044 form the basis for the staff's deterministic evaluation of severe accident performance for the AP1000. The staff evaluates the AP1000 relative to these criteria in Section 19.2 of this chapter.

19.1 Probabilistic Risk Assessment

19.1.1 Introduction

As part of the AP1000 advanced design certification application, Westinghouse submitted a Probabilistic Risk Assessment (PRA) in accordance with the requirements of 10 CFR 52.47 and the Commission's "Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants." The NRC staff's assessment of the AP1000 PRA consisted of the traditional evaluation of events that could lead to core damage and offsite consequences as well as an evaluation of what the PRA revealed about the AP1000 design.

19.1.1.1 Background and NRC Review Objectives

The general objectives of NRC staff's review of the AP1000 design PRA included the following:

- identify risk-informed safety insights based on systematic evaluations of risk associated with the design,
- support the process used to determine whether regulatory treatment of non-safety systems (RTNSS) was necessary,
- determine in a quantitative manner whether the design represents a reduction in risk over existing plants,
- assess the balance of preventive and mitigative features of the design,
- assess the reasonableness of the risk estimates documented in the PRA, and

- support design certification requirements, such as inspection, tests, analyses, and acceptance criteria (ITAACs), design reliability assurance program (D-RAP), technical specifications (TS), as well as combined license (COL) and interface requirements.

In addition, the staff used the AP1000 PRA to determine how the risk associated with the design relates to the Commission's goals of less than 1E-04/yr for core damage frequency (CDF) and less than 1E-06/yr for large release frequency (LRF). These goals are consistent with the Commission's safety goal policy statement (SECY-90-016). Also, the AP1000 PRA was used to uncover design and operational vulnerabilities.

The objectives are drawn from 10 CFR Part 52, the Commission's Severe Reactor Accident Policy Statement regarding future designs and existing plants, the Commission's Safety Goal Policy Statement, the Commission approved positions concerning the analyses of external events contained in SECY-93-087, and NRC interest in the use of PRA to help improve future reactor designs. In general, these objectives have been achieved by the AP1000 PRA and the NRC staff's review (pending the resolution of issues documented in Section 19.1.10 of this report).

During the construction stage, the COL applicant will be able to consider as-built information. The Commission believes that updated PRA insights, if properly evaluated and used, could strengthen programs and activities in areas such as training, emergency operating procedures development, reliability assurance, maintenance, and 10 CFR 50.59 evaluations. The design-specific PRA, developed as part of the design certification process, should be revised to account for site-specific information, as-built (plant-specific) information refinements in the level of design detail, technical specifications (TS), plant specific emergency operating procedures, and design changes. This is COL Action Item 19.1.1-1. These updates are the responsibility of the COL applicant. As plant experience data accumulates, failure rates (taken from generic data bases) and human errors assumed in the design PRA are to be updated and incorporated, as appropriate, into the operational reliability assurance program.

19.1.1.2 Evaluation of PRA Quality and Closure of Open Issues

In reviewing the AP1000 PRA, the NRC staff is relying significantly on the similarity between the AP1000 and the AP600 designs to reduce the review effort. This similarity (e.g., in system design and overall plant layout) allowed the use of the AP600 PRA as the starting point in the development of the AP1000 PRA. The NRC staff is interacting with the applicant to obtain the needed information to finalize its review of the quality and completeness of the AP1000 PRA. These attributes are essential in using the PRA to gain insights about how the design is robust and tolerant to severe accidents, and to provide risk-informed input to pre-and post-certification activities, thus achieving the objectives itemized above in Section 19.1.1.1 of this report. The staff has been reviewing the quality of the PRA submittal by evaluating the models, techniques, methodologies, assumptions, data, and calculational tools that were utilized by the applicant. In addition, the staff has been checking the AP1000 PRA for completeness by engaging in the following activities:

- comparing it with PRAs performed for current generation and advanced pressurized water reactor (PWR) designs to ensure that known safety significant PWR issues either do not apply to AP1000 design or they are appropriately modeled in the PRA

- ensuring that the final resolution of various deterministic issues, raised by the staff during the certification process, are appropriately incorporated into the PRA models.

As with the certification of previous advanced reactor designs (e.g., the AP600 design), the review of the quality and completeness of the AP1000 PRA submittal involves the issuance of requests for additional information (RAI) to the applicant followed by the evaluation of the applicant's responses to the RAI. Reported PRA results as well as results of sensitivity, uncertainty and importance analyses have been used to focus the review. A sharper focus has also been achieved by using PRA experience in the review process. The staff is using applicable insights from previous PRA studies about key parameters and design features controlling risk.

The staff has also been placing a special emphasis on PRA modeling of novel and passive features in the design as well as addressing issues related to these features, such as the issue of thermal-hydraulic (T-H) uncertainties. The issue of T-H uncertainties arises from the "passive" nature of the safety-related systems used for accident mitigation. Passive safety systems rely on natural forces, such as gravity, to perform their functions. Such driving forces are small compared to those of pumped systems and the uncertainty in their values, as predicted by a "best-estimate" T-H analysis, can be of comparable magnitude to the predicted values themselves. Therefore, some accident sequences with frequency high enough to impact results, which are not predicted to lead to core damage by a "best-estimate" T-H analysis, may actually lead to core damage when T-H uncertainties are considered in the PRA models. T-H uncertainties and their impact on PRA models are being considered in the certification of the AP1000 design using the same approach that was used in the AP600 design certification. This approach is discussed in Section 19.1.10 of this report.

Although the AP1000 PRA review is a continuous process, it involves two distinct stages. The first stage of the review ends with the issuance of this draft safety evaluation report (DSER). In the DSER, three classes of items are identified that the staff believes need additional attention by Westinghouse. These three classes are:

- Open items (i.e., areas where the staff disagrees with the submittal or requires additional supporting documentation)

- Confirmatory items (i.e., areas where resolution of previously open items has been reached but has not been incorporated into the PRA and/or DCD)

- COL action items (i.e., areas where the COL applicant should factor in plant or site-specific information at the COL stage).

The second stage of the review, which will follow the issuance of this report, will involve the resolution of all DSER open items, the inclusion of all identified confirmatory and COL action

items, and the preparation of the final safety evaluation report (FSER). The resolution (closure) of DSER open items is expected to involve close interaction between the staff and Westinghouse and may require Westinghouse's response to additional RAIs. The open, confirmatory and COL action items, along with the staff's evaluation of the quality and completeness of the current AP1000 PRA, are discussed in Section 19.1.10 of this report.

Even though there are still open items, safety insights about the AP1000 design and design certification requirements are documented in the following sections (19.1.2 to 19.1.9) of this report. Such insights and certification requirements are based on the results of the current PRA and the experience gained from the certification of the AP600 design. Depending on how the open issues (listed in Section 19.1.10) are resolved, both the safety insights and design certification requirements may change. Any such changes will be included in the applicable sections of the final safety evaluation report and the design control document (DCD).

The special advanced design features that were incorporated into the AP1000 design for the purpose of preventing and mitigating accidents are briefly presented in Section 19.1.2 below. Safety insights about the AP1000 design, drawn from the internal events risk analysis for operation at power, are presented in Section 19.1.3. Safety insights about the AP1000 design, drawn from the internal events risk analysis for low power and shutdown operation are reported in Section 19.1.4. Safety insights from the external events risk analysis (seismic, internal fires and internal floods), for both at-power and shutdown operation, are reported in Section 19.1.5. In Section 19.1.6, representative examples of how the applicant used PRA in the design process are discussed. In Section 19.1.7, the PRA input to the RTNSS process is summarized and evaluated. In Section 19.1.8 the PRA input, derived from PRA insights and assumptions, to the design certification process is documented. In Section 19.1.9, the staff's major conclusions and findings about the design are summarized. Finally, Section 19.1.10 documents the staff's evaluation of the AP1000 PRA quality and discusses open, confirmatory and COL action items.

19.1.2 Special Advanced Design Features

The AP1000 standard design, as the AP600 standard design, evolved from current PWR technology through incorporation of several passive design features and other design changes intended to make the plant safer, more available, and easier to operate. Insights from operating reactor PRAs helped in designing such passive features as well as in identifying other design changes. Therefore, the AP1000 design incorporates features intended to improve plant safety, and thus, reduce risk when compared to current generation nuclear power plants.

Some of these special advanced design features are preventive in nature while others are mitigative. Preventive features aim to accomplish the following objectives:

- minimize the initiation of plant transients,
- arrest the progression of plant transients once they start, and
- prevent severe accidents (core damage).

Mitigative features aim to arrest the progression of core damage and prevent breach of the reactor vessel and containment pressure boundary. The major preventive and mitigative special advanced design features of the AP1000 design are described in sections 19.1.2.1 and 19.1.2.2, respectively. In these descriptions, a brief qualitative discussion points out the effect that each of these features has on various elements involved in severe accident prevention and mitigation. More details about these features are found in the appropriate chapters of the AP1000 DCD.

19.1.2.1 Special Advanced Design Features for Preventing Core Damage

Major features incorporated into the AP1000 design for the purpose of limiting plant transients and preventing severe accidents include:

19.1.2.1.1 Passive Safety-Related Systems

The AP1000 design relies on passive safety-related systems for accident prevention and mitigation. The passive systems rely on natural forces, such as gravity and stored energy, to perform their safety functions (once actuated and started). In order for such systems to actuate and start, certain active components, such as air operated valves (AOVs) or check valves (CVs), must open. Such components do not require alternating current (ac) power for operation (to open) or for control and no support systems are needed after actuation. This reduces significantly, as compared to operating nuclear power plants, the risk contribution from loss of offsite power (LOOP) and station blackout (SBO) events. In addition, because of the passive systems, several important contributions to risk for operating nuclear power plants, have been eliminated in the AP1000 design. These risks are associated with failure of support systems (e.g., ac power and component cooling) and failure of active components (e.g., pumps and diesel generators) to start and run. Finally, the passive nature of the safety systems reduces, as compared to operating reactor designs, the reliance on operator actions to mitigate accidents. For a fair comparison to operating and evolutionary reactor designs, which use mostly active safety-related systems, the potential impact of T-H uncertainties on the performance of passive systems needs to be considered and appropriately included in the PRA models. Analyses performed by the applicant concluded that the AP1000 design is "robust" with respect to T-H uncertainties. The staff’s review is discussed in Section 19.1.10 of this report.

19.1.2.1.2 Defense-In-Depth Active Non-safety-Related Systems

The AP1000 design incorporates several active systems that are capable of performing some of the same functions performed by the safety-related passive systems. The availability of such redundant systems minimizes the challenge to the safety-related passive systems by providing core cooling during normal plant shutdowns and a first line of defense during accidents. Operation of the non-safety-related startup feedwater (SFW) system prevents challenging the passive residual heat removal (PRHR) heat exchanger during anticipated transients. For accidents occurring during power operation, the non-safety-related normal residual heat removal system (RNS) provides additional defense-in-depth to the "feed" portion of the "feed-and-bleed" core cooling function (provides an alternate "pumped" means of low pressure

injection from the in-containment refueling water storage tank (IRWST) and long-term recirculation from the containment sump). The diverse actuation system (DAS) provides an alternate means for initiating automatic and manual reactor trip and actuation of selected engineered safety features which is diverse from the safety-related protection and safety monitoring system (PMS).

19.1.2.1.3 In-Containment Refueling Water Storage Tank

Important characteristics and functions of the IRWST include the following:

- large capacity,
- acts as a heat sink for the PRHR,
- provides water for low pressure emergency core cooling (IRWST injection and RNS injection) after reactor coolant system depressurization,
- serves as the heat sink for the first three stages of the Automatic Depressurization System (ADS), and
- provides debris cooling following a severe accident.

The IRWST is a central feature in the AP1000 design that contributes to the simplicity and reliability of the passive safety systems. As the heat sink for the PRHR heat exchanger, it allows reliable core cooling at high reactor coolant system (RCS) pressures when cooling through the steam generators (SGs) fails during anticipated transients and steam generator tube rupture (SGTR) events (reduces the need for RCS depressurization and use of "feed-and-bleed" cooling). It is a reliable source of borated water for low pressure emergency core cooling and eliminates the need for switching over from the injection mode to the recirculation mode during emergency core cooling operations (a risk-important failure at operating PWRs).

19.1.2.1.4 Redundant Decay Heat Removal Systems

Redundant decay heat removal systems provide defense-in-depth during all possible scenarios of an accident. Alternative means for core cooling include the following:

- main feedwater (MFW) and condensate,
- startup feedwater,
- automatically actuated (with manual actuation backup capability) PRHR, and
- automatic with manual backup "feed & bleed" capability using systems with adequate redundancy and defense against common-cause failures throughout the RCS depressurization range for both the "feed" function (two core makeup tanks (CMTs), two accumulators, the two RNS pumps and the two IWRST gravity injection lines) and the

"bleed" function (four ADS stages with two paths in each of the first three stages and four paths in the forth stage).

19.1.2.1.5 Automatic Depressurization System

The function of the ADS is to provide a safety-related means of reducing RCS pressure in a controlled fashion during accidents to allow safety injection. This constitutes the "bleed" portion of the "feed-and-bleed" means of core cooling. ADS is actuated automatically, with manual backup actuation capability, and has incorporated redundancy (four ADS stages with two paths in each of the first three stages and four paths in the forth stage) and defense against common-cause failures (motor operated valves (MOVs) in the first three stages, explosive valves in the forth stage).

19.1.2.1.6 Redundant Safety Injection Systems

The AP1000 design includes redundant and diverse means of providing safety injection (i.e., the "feed" portion of the "feed-and-bleed" core cooling function) throughout the RCS depressurization range. Safety injection is provided by safety-related systems (two CMTs, two accumulators and two IWRST gravity injection lines) as well as by non-safety-related "defense-in-depth" systems (the two chemical and volume control pumps and the two normal residual heat removal pumps).

19.1.2.1.7 Redundant Long-Term Recirculation Systems

RCS recirculation is required for long-term core cooling during loss-of-coolant accidents (LOCAs) and whenever "feed-and-bleed" is used to cool the core during an accident. In the AP1000, recirculation can be either by gravity (through the safety-related IRWST injection lines) or pumped (through the non-safety-related normal residual heat removal system) with suction from the containment sump. There are two redundant recirculation lines (one for each of the two redundant IRWST injection lines). Furthermore, each recirculation line has two redundant paths.

19.1.2.1.8 Redundant Passive Containment Cooling Systems

Containment cooling, as the ultimate heat sink function for all accidents involving loss of feedwater (main and startup) to both SGs, is very important in the AP1000 design. The containment cooling function is performed by two highly reliable and redundant means that remove thermal energy from the containment atmosphere to the environment via the steel containment vessel by (1) natural external air circulation and (2) evaporation of water drained by gravity from an elevated tank.

19.1.2.1.9 Canned Reactor Coolant Pumps

The AP1000 uses canned reactor coolant pumps. A canned motor pump contains the motor and all rotating components inside a pressure vessel. The pressure vessel consists of the pump casing, thermal barrier, stator shell, and stator cap, which are designed for full RCS

pressure. Because the shaft for the impeller and rotor is contained within the pressure boundary, seals are not required to restrict leakage out of the pump into containment. Because of the canned motor reactor coolant pumps (RCPs), RCP seal LOCA (an important contributor to risk for operating nuclear power plants) has been eliminated in the AP1000 design.

19.1.2.1.10 Improved Control Room Design and Digital I&C Systems

The AP1000 Control Room design is an advanced design that is expected to provide more as well as more useful information to the operator than currently operating reactor designs. The AP1000 Control Room is still being designed. For this reason, no credit was taken in the PRA for the impact of the advanced control room on normal operations (e.g., initiating event frequency) and emergency response.

19.1.2.1.11 Large Pressurizer and Low Power Density

The larger pressurizer, as compared to operating plants, reduces the frequency of reactor scrams by increasing transient operation margins. This feature also moderates the pressure rise during certain transient events, such as loss of main feedwater, thus reducing the likelihood of challenging the primary safety valves. A larger pressurizer volume, as compared to operating plants, also helps lower the peak pressure that can be reached after a postulated anticipated transient without scram (ATWS) event.

19.1.2.1.12 Physical Separation of Safety System Redundant Trains

The design provides physical separation of safety systems or trains of systems that perform redundant safety-related functions. This increases the availability of systems due to their protection from failures associated with internal fires, internal floods, and similar common cause failures. Except for support systems, such as class 1E direct current (dc) power and instrumentation and control (I&C) systems, and the passive containment cooling system (PCS), all passive safety-related systems are located inside the containment where external events, such as fires, floods and tornadoes, are less likely to occur. This contributes to the reduction of risk as compared to current plant designs.

19.1.2.1.13 Highly Reliable dc Power Supply With 72-Hour Station Blackout Coping Capability

Each of the four independent and physically separated divisions of 125V dc Class 1E vital instrumentation and control power is provided with a separate and independent Class 1E 24-hour battery bank. In addition, two of the four divisions are provided with a Class 1E 72-hour battery bank. This permits operating instrumentation and control loads, associated with safety systems that may be required following the loss of ac power concurrent with a design basis accident, for 72 hours. This feature contributes to the large reduction of risk associated with SBO accidents as compared to current plant designs.

19.1.2.2 Special Advanced Design Features for Core Damage Consequence Mitigation

The following design features improve the ability of the containment to accommodate the challenges associated with severe core damage accidents. The impact of these features on severe accident mitigation and containment performance is modeled in the AP1000 PRA and/or supporting deterministic analyses. The staff's evaluation of these models and analyses is provided later in Section 19.1.10 and 19.2 of this report.

19.1.2.2.1 Automatic Depressurization System

In addition to providing a core damage prevention function, the ADS also serves a mitigative function. Specifically, in core damage events in which early depressurization is not successful, late actuation of ADS (before significant core damage and debris relocation into the lower plenum of the reactor vessel) can reduce or eliminate the potential for creep rupture of the SG tubes and the reactor vessel. Prevention of reactor vessel breach precludes severe accident phenomena associated with vessel failure -- direct containment heating (DCH), large hydrogen combustion events at vessel breach, ex-vessel steam explosions, and core concrete interactions -- thereby reducing the probability of early containment failure. The ADS also reduces the amount of fission products released to the containment atmosphere since a portion of the discharge flow (from ADS stages 1 through 3) is routed through a sparger network in the IRWST. However, in many sequences the RCS is vented to the containment airspace (via the 4th stage of ADS) at the time when most fission products are released, and the potential for fission product scrubbing is not fully realized. Finally, RCS depressurization can reduce or terminate fission product releases to the environment during SG tube rupture events.

19.1.2.2.2 Large Passively-Cooled Steel Containment

The AP1000 design includes a large, passively cooled steel containment. The containment building volume to reactor power ratio for AP1000 is similar to that for typical operating PWRs with large, dry containments. The large volume to power ratio reduces the potential for developing detonable concentrations of hydrogen under severe accident conditions and the potential for containment over-pressure from non-condensible gas buildup. The containment pressure capacity is sufficiently large that the pressure loads associated with early challenges, e.g., hydrogen combustion and direct containment heating, are at or below the applicant's Service Level C estimate (627.4KPa (91psig)) and pose an insignificant threat to containment integrity (a containment failure probability of less than one percent).

The PCS provides water to the external surface of the containment shell from the PCS water storage tanks or the post-72 hour water tank. Alternative water sources can be provided via separate connections outside containment in accordance with accident management guidelines to be developed by the COL applicant (see COL Action Item 19.2.5-1). Without operation of the PCS, air cooling alone is not sufficient to maintain containment pressure below the applicant's Service Level C estimate in the long term, and the containment will need to be vented after 24 hours in order to prevent over-pressure failure of containment.

19.1.2.2.3 In-Containment Refueling Water Storage Tank

The AP1000 design incorporates an IRWST. In addition to serving the typical function of the refueling water storage tank at operating plants, this system performs water collection, delivery, and heat sink functions inside the containment during accident conditions. The IRWST is important to the progression of a severe accident due to its ability to condense steam and scrub fission products for releases into the IRWST via stages 1 through 3 of ADS, and to reduce the likelihood of reactor vessel failure and core-concrete interaction (CCI) by enabling reactor cavity flooding via gravity draining. The potential for hydrogen-rich mixtures to form in the vicinity of the IRWST (as a result of steam condensation as the hydrogen-steam blowdown passes through the IRWST) represents a unique containment challenge for AP1000, but is minimized by locating the IRWST pipe vents in areas where diffusion flames will not impinge on the containment shell, and by equipping the IRWST vents along the containment wall with louvers that will reclose following an initial release into the IRWST.

19.1.2.2.4 External Reactor Vessel Cooling

The capability to fully flood the AP1000 reactor cavity and depressurize the RCS in the majority of core melt sequences minimizes the potential for reactor vessel breach by molten core debris. By maintaining reactor vessel integrity, the potential for large releases due to ex-vessel severe accident phenomena is substantially reduced, however, a residual threat from hydrogen combustion remains. The ability to flood the reactor cavity is enhanced in the AP1000 design by the following attributes:

- A containment and reactor cavity arrangement that permits breakflow from the RCS to drain to the cavity without significant holdup in containment.

- The inclusion of manually-actuated safety-grade valves which allow additional water from the IRWST to be drained to the cavity.

The operator action to flood the cavity is specified in energy response guideline (ERG) AFR.C-1, which instructs the operator to flood the reactor cavity if injection to the RCS cannot be recovered or containment radiation reaches levels that indicate fission product releases as determined by a core damage assessment guideline. The operator instructions to flood the cavity have been moved from the end of the procedure (in AP600) to the entry of the procedure (in AP1000) to achieve the higher water depths and earlier flooding times required for successful external reactor vessel cooling in AP1000. The following design features contribute to the effectiveness of external reactor vessel cooling in AP1000:

- a reactor vessel lower head that contains no in-core instrument or other penetrations,

- a reactor vessel insulation system that limits thermal losses during normal operations, but provides an engineered pathway for supplying water cooling to the vessel and venting steam from the reactor cavity during severe accidents, and

- refinements in the reactor vessel insulation system design (relative to AP600) to increase the heat transfer capability (critical heat flux) from the reactor pressure vessel to the surrounding water, and accommodate the higher decay heat level for AP1000.

19.1.2.2.5 Reactor Cavity Design

The AP1000 design relies primarily on safety grade RCS depressurization and reactor cavity flooding capabilities to prevent high pressure core melt events and reactor vessel breach. In the event that vessel breach occurs, the AP1000 reactor cavity design is sufficient to accommodate the loads associated with ex-vessel severe accident phenomena without early loss of containment integrity. These challenges include DCH, fuel-coolant interactions (FCI), and CCI. The specific reactor cavity features to deal with each challenge are summarized below.

DCH: The paths from the reactor cavity to the upper containment volume in AP1000 include the following:

- the area around the reactor vessel flange,

- the area where the coolant loops penetrate through the biological shield, and

- a ventilation shaft from the roof of the reactor coolant drain tank room that leads to the steam generator compartments.

These paths are convoluted, hence a portion of the corium will be de-entrained and removed from the atmosphere before reaching the upper containment region, thereby reducing the pressure rise associated with DCH. The peak containment pressure for a postulated DCH event is expected to be sufficiently small that the corresponding probability of containment failure is negligible (less than 0.1 percent).

FCI: The deterministic evaluation of ex-vessel FCIs (Section 19.2.3.3.5.2 of this report) indicates that the impulse loads from ex-vessel steam explosions may fail the reactor cavity floor and wall structures, but that the integrity of the embedded steel liner will be maintained. The evaluation also indicates that containment vessel integrity will not be compromised by the displacement of the reactor pressure vessel (RPV) as a result of the impulse loading.

CCI: The AP1000 reactor cavity design incorporates features generally consistent with the EPRI utility requirements document (URD) criteria, including the following:

- a cavity floor area and sump curb that provides for debris spreading without debris ingression into the reactor cavity sump,

- a manually-actuated reactor cavity flood system that would cover the core debris with water and maintain long-term debris coolability, and

- a minimum 0.85 m (2.8 ft) layer of concrete to protect the embedded containment shell, with an additional 1.8 m (6 ft) of concrete below the liner elevation.

The enhanced capability to retain a molten core in-vessel, in conjunction with these design features, result in a low expected frequency of basemat melt-through in the AP1000 PRA.

Compared to other advanced light-water reactors (ALWRs), the AP1000 ex-vessel debris bed is deeper and the concrete basemat is thinner. The AP1000 design does not impose any restrictions on the type of concrete that can be used for the containment basemat and the reactor cavity walls. Although these factors tend to increase the severity of basemat erosion, analyses using the MELTSPREAD and MAAP codes indicate that in the event of unabated CCI, containment basemat penetration or containment over-pressurization will not occur until after 2 days, regardless of concrete composition.

For a limestone basemat (which maximizes non-condensible gas generation and minimizes concrete ablation), basemat penetration would occur after about 3 days following onset of core damage. Containment pressure will not reach Westinghouse's Service Level C estimate (627.4KPa (91 psig)) until even later. Use of basaltic concrete (which maximizes concrete ablation and minimizes non-condensible gas generation) would reduce the time of basemat melt-through to about 2 days, but containment pressure would not reach Service Level C until much later. Thus, in the event that core debris is not retained in vessel, the AP1000 design provides adequate protection against early containment failure and large releases due to CCIs.

19.1.2.2.6 Hydrogen Igniter System

The AP1000 design incorporates a distributed ignition system to promote combustion at lean hydrogen concentrations and minimize the potential for large deflagrations or detonations. The igniter system is non-safety-related but is subject to investment protection short-term availability controls as described in DCD Tier 2 Section 16.3. The system uses 64 glow plug igniters powered from the non-safety-related onsite ac power system and is manually actuated from the control room when core exit temperature exceeds 648.9°C (1200°F), as an initial step in the AP1000 (ERG) AFR.C-1. The hydrogen igniter system is capable of being powered by either offsite ac power or onsite non-essential diesel generators. In the event of a station blackout, which represents less than 1 percent of the core damage frequency, the system can be powered from the non Class 1E batteries via dc-to-ac inverters. However, this feature was not credited in the PRA. The AP1000 design also includes two non-safety-related PARs located within the containment. The PARs are provided for defense-in-depth protection against the buildup of hydrogen following a design basis loss of coolant accident. Although the PARs are expected to function to reduce combustible gas concentrations during severe accidents as well, they are not credited in the PRA. The proven design of the glow plug igniters and the diverse means of powering the system, in conjunction with the small fraction of core melt sequences involving loss of onsite power in the AP1000 design, significantly reduce the threat of containment failure due to hydrogen deflagrations or detonations. The use of PARs further reduces the threat from hydrogen burns in those events in which the igniters are unavailable.

19.1.2.2.7 Non-Safety Containment Spray System

The AP1000 includes a non-safety containment spray system for severe accident management. The system consists of two spray rings located above the containment polar crane, with flow supplied from the normal fire main header. The source of water is provided by either the primary or secondary fire protection system water tank (depending on tank and inventory availability) using either the motor-driven or diesel-driven fire protection system pump. The impact of the non-safety grade containment spray system on containment response and fission product releases is not credited in the Level 2 and 3 PRA. Containment sprays could significantly reduce the estimated risk in the baseline PRA since the sprays would be effective in reducing the source terms in the risk-dominant release categories.

19.1.2.2.8 Containment Vent

The AP1000 design configuration will include a containment vent path that can be used to control containment pressure in the unlikely event of long-term over-pressurization of containment. The COL applicant, as part of COL Action Item 19.2.5-1 regarding the severe accident management program, will identify the specific penetration(s) to be used for containment venting and develop and implement severe accident management guidance for venting containment using the framework provided in WCAP-13914, Revision 3. The impact of the containment vent on containment response is not credited in the PRA.

19.1.3 Safety Insights From the Internal Events Risk Analysis (Operation at Power)

These insights include:

- dominant accident sequences contributing to CDF,
- areas where certain AP1000 design "passive" and "defense-in-depth" features were the most effective in reducing risk as compared to operating reactor designs,
- major contributors to the estimated CDF from internal events, such as hardware failures, system unavailabilities, and human errors,
- major contributors to maintaining the "built-in" plant safety (to ensure that risk does not increase unacceptably),
- major contributors to the uncertainty associated with the estimated CDF,
- sensitivity of the estimated CDF from internal events to potential biases in numerical values, to assumptions made, to lack of modeling details in certain areas, and to previously raised safety issues,
- core damage sequences and accident classes contributing to containment failure,
- frequency and conditional probability of containment failure,

- leading contributors to containment failure and risk, and
- important insights and supporting sensitivity analyses from the levels 2 and 3 of the PRA.

19.1.3.1 Level 1 Internal Events PRA

The applicant estimated the mean CDF for the AP1000 design, from internal events during operation at power, to be about 2.4E-7 per year. In addition, CDFs for various initiating event categories were estimated and are summarized in Table 19.1.1 of this report. Ranges of mean CDFs, by initiating event category, for currently operating PWR reactor designs (NUREG-1560, 1996) are also shown for comparison. The total CDF of the AP1000 design, from internal events at power operation, was estimated by the applicant to be roughly two orders of magnitude smaller than the corresponding total CDF of an average operating PWR reactor.

For the AP1000 design, the various LOCA categories of initiating events essentially dominate the CDF profile (about 85 percent contribution) followed by reactor vessel rupture (about 4 percent) and "transient" events (about 4 percent). Contributions from SGTR events (about 3 percent), ATWS sequences (about 2 percent) and LOOP/SBO (less than 1 percent) are relatively small.

In Section 19.1.3.1.1 of this report, the dominant accident sequences and the major contributors to the CDF estimates for the AP1000 design, as assessed by the applicant and reviewed by the staff, are presented. The design features that contribute to the reduced CDFs, as compared to operating PWRs, are described in section 19.1.3.1.2 of this report. Finally, in Sections 19.1.3.1.3, 19.1.3.1.4 and 19.1.3.1.5 of this report, the insights drawn from the uncertainty analysis and the importance and sensitivity studies are discussed.

19.1.3.1.1 Dominant Accident Sequences Leading to Core Damage

The applicant's PRA results identify 100 sequences initiated by internal events that contribute almost 100 percent of the estimated CDF from internal events. The top 10 sequences, contributing about 80 percent of the total CDF from internal events, are summarized below.

Sequence #1, with a CDF of about 6.9E-8 per year and about 28.5 percent contribution, is initiated by a break in one of the two safety injection lines (a LOCA event) followed by failure of the IRWST injection line which is not affected by the break to remove decay heat from the core (CMT injection and RCS depressurization via the ADS system are successful). In addition to the initiating event, risk important failures appearing in this sequence are listed below:

- plugging of the IRWST discharge line strainer in the intact line,
- common cause failure (CCF) of the two check valves in the intact IRWST discharge line, and

- CCF of the two explosive (squib) valves in the intact IRWST discharge line.

Sequence #2, with a CDF of about 4.3E-8/yr and about 18 percent contribution, is initiated by a large LOCA event which is not due to spurious ADS actuation (equivalent break diameter greater than 9 inches but smaller than a vessel rupture) followed by failure of any one of the two accumulators to inject. In addition to the initiating event, risk important failures appearing in this sequence are listed below:

- failure of any check valve in the accumulator injection lines to open, and
- plugging of any flow tuning orifice in the accumulator injection lines.

Sequence #3, with a CDF of about 2.1E-8/yr and about 9 percent contribution, is initiated by a spurious ADS actuation event that results in a large LOCA. The RCS rapidly depressurizes and at least one of the accumulators injects, making up the RCS water loss in the short time frame. However, due to the failure of either the CMT injection or the ADS actuation, the automatic IRWST injection is not actuated. In addition to the initiating event, risk important failures appearing in this sequence are listed below:

- CCF of hardware in the PMS engineered safety feature (ESF) input logic groups (causes CMT injection actuation failure which results in failure of automatic IRWST injection actuation with no adequate time for manual actuation),
- CCF of CMT level sensors which prevents IRWST injection actuation,
- CCF of CMT injection air-operated valves to open,
- CCF of CMT injection check valves to open, and
- CCF of 2 or more fourth stage ADS explosive (squib) valves to operate.

Sequence #4, with a CDF of about 2E-8/yr and about 8 percent contribution, is initiated by a break in one of the two safety injection lines (a LOCA event) followed by successful CMT injection but failure of full RCS depressurization (to allow low pressure IRWST injection). The failure that dominates the risk associated with this sequence is the CCF of ADS stage #4 explosive (squib) valves.

Sequence #5, with CDF of 1E-8/yr and 5 percent contribution, is a reactor vessel rupture event which leads directly to core damage.

Sequence #6, with a CDF of about 8.5E-9/yr and over 3 percent contribution, is initiated by a small LOCA event (0.952cm to 5.08cm (0.375in. to 2in.) equivalent break diameter) followed by failure to establish recirculation from the containment sump when the IRWST inventory is depleted (high pressure injection by the CMTs, heat removal by the PRHR, containment isolation, depressurization and low pressure injection by either the RNS or the IRWST are

successful). Risk important failures, in addition to the initiating event, appearing in this sequence are listed below:

- CCF of both sump recirculation lines due to sump screen plugging,
- CCF of all IRWST level transmitters (causes failure of automatic actuation of sump recirculation), and
- operator failure to manually actuate sump recirculation (when automatic actuation fails).

Sequence #7 with a CDF of about 7.5E-9/yr and about 3 percent contribution, is initiated by a medium LOCA event (5.08cm to 22.9cm (2in. to 9in.) equivalent break diameter) followed by failure to establish recirculation from the containment sump when the IRWST inventory is depleted (high pressure injection by the CMTs, containment isolation, depressurization and low pressure injection are successful). With the exception of the initiating event, the risk important failures appearing in this sequence are the same as for Sequence #6.

Sequence #8, with a CDF of about 5E-9 per year and over 2 percent contribution, is initiated by a small LOCA event (0.952cm to 5.08cm (0.375in. to 2in.) equivalent break diameter) followed by failure of full depressurization (required for low pressure injection from the IRWST), by success of partial depressurization (below the point where injection by the RNS is possible) and by failure of the RNS. High pressure injection by the CMTs, RCP trip and heat removal by the PRHR are successful. Risk important failures, in addition to the initiating event, appearing in this sequence are listed below:

- CCF of 2 or more fourth stage ADS explosive (squib) valves to operate,
- failure of any of four RNS isolation valves (V055, V011, V022, V023) to open, and
- unavailability of the cask loading pit due to fueling unloading operations.

Sequence #9, with a CDF of about 4.5E-9 per year and about 2 percent contribution, is initiated by a medium LOCA event (5.08cm to 22.9cm (2in. to 9in.) equivalent break diameter) followed by failure of full depressurization (required for low pressure injection from the IRWST), by success of partial depressurization (below the point where injection by the RNS is possible) and by failure of the RNS to inject. High pressure injection by the CMTs, reactor coolant pump (RCP) trip and heat removal by the PRHR are successful. With the exception of the initiating event, the risk important failures appearing in this sequence are the same as for Sequence #8.

Sequence #10, with a CDF of about 3.7E-9/yr and about 1.5 percent contribution, is initiated by a spurious ADS actuation event that results in a large LOCA followed by failure of any one of the two accumulators to inject. In addition to the initiating event, the failure that dominates the risk associated with this sequence is the CCF of two accumulator check valves, one in each of the two accumulator injection lines.

19.1.3.1.2 Risk Important Design Features

Listed below are major features that contribute to the reduced CDF of the AP1000 design as compared to operating PWR designs, for each of the initiating event categories contributing the most to this reduction.

19.1.3.1.2.1 Loss of Offsite Power and Station Blackout Sequences

The following are the most important features of the AP1000 design that contribute to the reduction in the estimated CDF associated with loss of offsite power (LOOP, including SBO, sequences (CDF reduced to 1E-9/yr from the 7E-5/yr to 1E-8/yr range corresponding to CDFs associated with LOOP/SBO at operating PWR reactors):

- Safety-related passive systems that do not rely on ac power for operation. They rely on natural forces, such as gravity and stored energy, to perform their accident mitigation functions once actuated and started. When power is needed to actuate and start such passive systems, dc power provided by Class 1E batteries is used.

- The PRHR is automatically actuated, without the need for any electrical power, to provide core cooling upon LOOP (AOVs "fail safe" in the open position).

- Class 1E dc batteries with capability to support all front line passive safety-related systems for 72 hours.

- Defense-in-depth, which provides alternative means for removing decay heat from the RCS during a LOOP/SBO accident. Most current PWR plants rely on two alternative means for core cooling:

  – an Auxiliary Feedwater System, with at least one turbine driven pump for SBO events, in addition to motor driven pump(s), and

  – a manual "feed & bleed" capability when onsite ac power is available.

  The AP1000 design provides better and more reliable defense-in-depth by relying on the following alternative means for core cooling:

  – the automatically actuated non-safety-related Startup Feedwater (SFW) system when onsite ac power is available,

  – the automatically actuated safety-related PRHR system, and

  – an automatic with manual backup "feed & bleed" capability using systems with adequate redundancy and defense against common-cause failures throughout the RCS depressurization range for both the "feed" function (two CMTs, two accumulators, the two RNS pumps and the two IWRST gravity injection lines)

and the "bleed" function (four ADS stages with two paths in each of the first three stages and four paths in the fourth stage).

- The improved reliability of the PRHR system (as compared to the AFW system used in most current PWR plants) contributes significantly to the reduced risk associated with LOOP/SBO sequences (the function of the PRHR following a LOOP/SBO event is similar to the AFW system function in operating PWRs).

- Canned reactor coolant pumps eliminate seal LOCAs, which are likely in operating PWRs during an SBO accident.

19.1.3.1.2.2 "Transient" Sequences

The following are the most important features of the AP1000 design which contribute to the reduction in the estimated CDF associated with "transient" sequences (CDF reduced to 8E-9/yr from the 3E-4/yr to 5E-7/yr range corresponding to CDFs associated with "transients" at operating PWR reactors):

- Defense-in-depth which provides several alternative means for core cooling during all possible scenarios of the accident. Most current PWR plants rely on three alternative means for core cooling following a "transient" initiator (main feedwater and condensate, auxiliary feedwater, and manual "feed & bleed"). The AP1000 design provides better and more reliable defense-in-depth by relying on the following alternative means for core cooling:

  – main feedwater and condensate,

  – startup feedwater,

  – automatically actuated (with manual actuation backup capability) PRHR, and

  – automatic with manual backup "feed & bleed" capability using systems with adequate redundancy and defense against common-cause failures throughout the RCS depressurization range for both the "feed" function (two CMTs, two accumulators, the two RNS pumps and the two IWRST gravity injection lines) and the "bleed" function (four ADS stages with two paths in each of the first three stages and four paths in the fourth stage).

- A reliable PRHR system (which is needed only when the non-safety-related SFW system is unavailable) reduces significantly the need for RCS depressurization and reliance on "feed and bleed" cooling, as compared to operating PWRs, and contributes to the reduced risk associated with "transient" sequences (the functions of the SFW and PRHR following a "transient" event are redundant and similar to the function performed by the AFW system in operating PWRs).

- Use of two redundant and diverse ESF actuation systems with automatic and manual actuation capability (one is safety-related) minimizes the likelihood of actuation failures, including common-cause actuation failures.

- Use of passive safety-related systems which do not need several traditional support systems, such as component cooling water and ac power, to operate eliminates all failures associated with such support systems in operating PWRs and contributes significantly to the increased reliability of most AP1000 safety-related systems as compared to systems for operating plants performing similar functions.

- The use of a larger pressurizer than those at comparable operating PWR plants reduces the frequency of "transient" initiating events by increasing transient operation margins.

19.1.3.1.2.3 Steam Generator Tube Rupture Sequences

The following are the most important features of the AP1000 design which contribute to the reduction in the estimated CDF associated with SGTR sequences (CDF reduced to about 7E-9/yr from the 3E-5/yr to 9E-9/yr range corresponding to CDFs associated with SGTR at operating PWR reactors):

- Three lines of defense against core damage following an SGTR event:

  – use of non-safety-related systems (CVS and SFW) and manual SG isolation,

  – use of passive safety-related systems (PRHR, CMT and PCS) and automatic SG isolation, and

  – use of "feed and bleed" if the leak cannot be isolated (ADS, CMT, Accumulators, RNS, IRWST injection, PCS).

  For comparison, operating PWRs have two lines of defense: One is similar to AP1000 design's first line of defense but uses safety-related systems (high pressure safety-injection (HPSI), AFW) and the other is manual "feed and bleed" using the pressurizer PORVs.

- Redundant means for reactor coolant inventory control:

  – automatic chemical and volume control system (CVS) injection at the upper end of the RCS pressure range,

  – automatic CMT injection once an "S" signal is generated, and

  – manual ADS actuation to allow accumulator injection if CMT injection fails.

- The improved reliability of the PRHR, as compared to the AFW system used in operating PWR plants, reduces the reliance on "feed and bleed" cooling as the last defense against core damage.

- The ADS provides an alternative decay heat removal path through primary "feed and bleed" which is much more reliable and faster than the high-pressure manual "feed and bleed" cooling of currently operating PWRs.

- Good capability for long-term recovery from unisolable SG leaks, which bypass the containment, exists by venting the RCS into the containment through the large ADS stage #4 valves to allow low pressure core cooling by IRWST gravity injection and containment sump recirculation. The large IRWST capacity, combined with the capability to refill either the IRWST or the containment sump, prevents depletion of borated water through the open path that bypasses the containment and ensures the water level in the sump is adequate to establish recirculation by gravity.

- SGs have a secondary-side water inventory which is larger than comparable operating plants. This feature extends the time available to recover feedwater or other means of core heat removal.

19.1.3.1.2.4 LOCA Sequences

The following are the most important features of the AP1000 design that contribute to the reduction in the estimated CDF associated with LOCA sequences (CDF reduced to about 2.1E-7/yr from the 8E-5/yr to 1E-6/yr range corresponding to CDFs associated with LOCA at operating PWR reactors):

- Defense-in-depth, which provides several alternative means for coolant makeup at both high and low pressures using both safety and non-safety-related systems (CVS pumps, CMTs, Accumulators, RNS, and IRWST injection), increases the reliability of the coolant makeup function. For comparison, most operating PWRs use the chemical and volume control (CVCS) pumps and HPSI pumps for high pressure injection while for low pressure injection accumulators and low pressure safety injection (LPSI) pumps are provided.

- Defense-in-depth, which provides several alternative means for core cooling during all possible scenarios and sizes of a LOCA accident using both safety and non-safety related systems, increases the reliability of the core cooling function (both in the short and long term). Operating PWRs rely on fewer and less reliable alternative means for core cooling during LOCAs (e.g., manual “feed and bleed” as compared to automatic with manual backup “feed and bleed “ capability of the AP1000 design).

- The ADS provides an alternate decay heat removal path through primary "feed and bleed" which is much more reliable and faster than the high pressure manual "feed and bleed" cooling of currently operating PWRs.

- The AP1000 design is expected to have a reduced frequency of LOCA initiators (breaks) as compared to operating PWR plants because the number of welds in the AP1000 RCS pressure boundary was significantly reduced and "leak-before-break" was applied in the design of all piping larger than 7.62cm (3in.).

19.1.3.1.2.5 ATWS Sequences

The following are the most important features of the AP1000 design that contributes to the reduction in the estimated CDF associated with ATWS sequences (CDF reduced to 5E-9/yr from the 4E-5/yr to 1E-8/yr range corresponding to CDFs associated with ATWS at operating PWR reactors):

- The AP1000 design has two redundant and diverse reactor trip systems. The non-safety-related DAS is a reliable system capable of initiating automatic and manual reactor trip via the motor-generator sets when the reactor fails to trip via the PMS. At operating reactors the DAS is less reliable and cannot automatically initiate a reactor trip.

- The ADS allows use of the low-pressure injection systems (accumulators, RNS pumps, IRWST injection) for long-term reactivity control and core cooling when the charging pumps are unavailable. At operating reactors the less reliable PORVs must be used to allow low-pressure injection.

- The AP1000 design employs a “low-boron” core that contributes to a more negative moderator temperature coefficient (MTC) of reactivity than in conventional cores. This feature contributes to a significant reduction in the peak pressure established in the RCS during an ATWS event.

- Because the AP1000 reactor uses a larger pressurizer than those at comparable operating plants, the frequency of ATWS precursors is reduced by increasing transient operation margins.

In the following sections, insights from the uncertainty analysis (Section 19.1.3.1.3 of this report) and from risk importance (Section 19.1.3.1.4 of this report) and sensitivity (Section 19.1.3.1.5 of this report) studies are presented.

19.1.3.1.3 Insights from the Uncertainty Analysis

The applicant performed an uncertainty analysis to determine the magnitude of uncertainties that characterize the level 1 PRA results (CDF from internal events) as well as the major contributors to these uncertainties. The AP1000 CDF estimates, for internal events, are

reported in terms of a mean value and an associated error factor (EF). The EF[1] is a measure of uncertainty that expresses the spread of a fitted log-normal distribution. The total CDF from internal events, as estimated by the applicant, has a mean value of about 2.4E-7/yr and an EF of approximately 6. Thus, the 95th and 5th percentiles are about 1.4E-6/yr and 4E-8/yr, respectively. It should be emphasized that only uncertainties associated with reliability and availability data were considered. Uncertainties associated with modeling (or lack of modeling) of accident sequences, system failure modes and human errors, were not included.
The following conclusions can be reached from the results of the uncertainty analysis:

- The majority of the major contributors to the dominant accident sequences, and total CDF, have relatively small uncertainties associated with them.
- The following are major contributors to the uncertainty associated with the plant CDF estimate:
  - LOCA initiating event frequencies, such as safety injection line break, LOCA breaks of all sizes (large, intermedium, medium and small) and CMT line break
  - reactor vessel failure probability
  - containment sump screen plugging probability (both single and common cause failures)
  - IRWST discharge line strainer plugging probability (both single and common cause failures)
  - CCF probability of hardware in the PMS ESF input logic groups
  - CCF probabilities of several sensor groups, such as CMT level heat sensor resistance temperature detectors (RTDs), tank level transmitters, pressurizer level sensors, and sensors in high pressure environment
  - failure probability of the turbine impulse pressure transmitter (DAS trip permissive)
  - CCF probability of the reactor trip breakers to open (mechanical failure)
  - CCF of the reactor trip portion of PMS hardware or software (no signal to open the PMS reactor trip breakers)

[1]The "error factor" is the ratio between the 95th percentile and the median (50th percentile) of the assumed log-normal distribution (which is the same as the ratio between the median and the 5th percentile).

– failure probability of a motor-generator (M-G) set circuit breaker to open by DAS (mechanical failure)

– failure probability of the automatic DAS function (hardware or software)

As a result of the lack of adequate data, the probability distribution function parameters associated with some risk-important events (e.g., software failures, CCF of explosive valves to operate and CCF of IRWST injection line check valves to open under small differential pressures) are rather subjective point estimates. The low confidence level in the point estimates (especially mean values) of such events, was addressed by the performance of sensitivity studies. The insights from these studies are discussed, together with insights from other sensitivity studies, in Section 19.1.3.1.5 of this report.

19.1.3.1.4 Insights from the Risk Importance Studies

The applicant performed studies to determine important contributors to risk as well as to maintaining the existing "designed-in" risk level. The staff, when necessary, used the applicant's PRA results to perform additional risk importance studies to gain more complete insights. Such studies address the following two general objectives: (1) risk reduction, and (2) safety or reliability assurance. The first objective, i.e., risk reduction, was achieved by the identification and ranking of dominant contributors to risk in order to identify areas in which the plant risk can be reduced by design and/or operational changes. The second objective, i.e. reliability assurance, was achieved by the identification of dominant contributors to maintaining the "built-in" risk level (to ensure that risk does not increase and is as low as the PRA indicates it is). To meet these two objectives, the applicant used the following two risk importance measures to rank systems, structures, components (SSCs) and human actions:

- Risk reduction worth that gives the factor by which the CDF decreases when an SSC or human action is assumed to be perfectly reliable (perfect component or no error). Provides indication of existing margin for improvement.

- Risk achievement worth that gives the factor by which the CDF increases when an SSC or human action is assumed not to be there or to be failed (event probability is assumed to be 1). Provides indication of the importance of maintaining the existing reliability.

The "risk achievement worth" importance measure is useful in identifying SSCs for which it is particularly important to do good maintenance, since poor reliability and availability of this equipment would significantly increase the CDF estimate. The "risk reduction worth" importance measure is useful in identifying SSCs that would benefit the most from improved testing and maintenance by minimizing equipment unavailability and failures.

Risk importance studies were performed at both the system and component level. The major insights drawn from the importance analysis are summarized below:

- The most important systems for core damage prevention, or equivalently, the systems that are the most "worthy" in achieving the low CDF level assessed in the PRA (i.e.,

systems with the highest "risk achievement worth"), are the PMS, the Class 1E dc power, the ADS, IRWST recirculation, IRWST injection, the CMTs and the accumulators.

- Events that would decrease significantly the "built-in" reliability, i.e., those with highest "risk achievement worth," are hardware common-cause failures and software errors. This is attributable to the redundancy and diversity of the AP1000 safety systems, which ensure that single independent hardware faults are not among those events whose occurrence would have a large impact on the CDF from internal events.

- Common-cause failure of the following sets of components was found to have a large impact on the estimated CDF from internal events (i.e., sets of components with highest "risk achievement worth"):

  – Containment sump screen plugging. If both recirculation lines are unavailable due to a CCF and the plant keeps operating at power, the plant CDF would increase by almost four orders of magnitude.

  – IRWST gravity injection components, such as squib valves and check valves. If both IRWST injection lines are unavailable due to a CCF and the plant keeps operating at power, the plant CDF would increase by over three orders of magnitude.

  – ADS stage #4 explosive (squib) valves. If two or more of these valves become unavailable to open when demanded due to CCF and the plant keeps operating at power, the plant CDF would increase by over three orders of magnitude.

  – PMS ESF hardware components, such as output drivers and input logic groups (hardware). If such components are unavailable due to a CCF and the plant keeps operating at power, the plant CDF would increase by about three orders of magnitude.

  – IRWST discharge line strainers. If both stainers become unavailable (plugging) and the plant keeps operating at power, the plant CDF would increase by almost three orders of magnitude.

  – CMT sensors and sump level heated RTD sensors. If such components become unavailable to operate when demanded due to CCFs and the plant keeps operating at power, the plant CDF would increase by almost three orders of magnitude.

  – CMT and accumulator injection line components, such as CMT AOVs, CMT check valves, and accumulator check valves. If such components become unavailable to operate when demanded due to CCFs and the plant keeps operating at power, the plant CDF would increase by almost three orders of magnitude.

– Class 1E dc batteries. If the plant operates without Class 1E batteries, the plant CDF would increase by over two orders of magnitude.

– PRHR AOVs. If both such AOVs become unable to open and the plant keeps operating at power, the plant CDF would increase by almost two orders of magnitude.

– IRWST gutter AOVs. If both such AOVs become unable to open on demand and the plant keeps operating at power, the plant CDF would increase by almost two orders of magnitude.

– ADS stage 2 and stage 3 MOVs. If three or more such MOVs become unable to open on demand and the plant keeps operating at power, the plant CDF would increase by almost two orders of magnitude.

– RCP breakers. If the RCP breakers become unable to open to trip the RCPs and the plant keeps operating at power, the plant CDF would increase by almost two orders of magnitude.

– Tank level transmitters (IRWST, BAT), sensors in high pressure environment and pressurizer level sensors. If such components become unable to operate as designed when demanded due to CCFs and the plant keeps operating at power, the plant CDF would increase by over one order of magnitude.

– PMS reactor trip components, such as reactor trip breakers and reactor trip logic hardware. If such components become unavailable to operate when demanded due to CCFs and the plant keeps operating at power, the plant CDF would increase by almost one order of magnitude.

• The AP1000 relies on digital I&C systems which are complex combinations of hardware and software (i.e., computer programs) components. Although computer software does not wear out, as hardware does, it could fail because of the excitation of residual design errors when a particular combination of inputs occurs. If the same programs are executed in two or more channels (or divisions) in parallel, a software fault would lead to a common mode software failure in all channels (or divisions) at the same time, i.e., it would be a CCF of redundant channels or divisions. The following types of software error were found to have a large impact on the estimated CDF (i.e., highest "risk achievement worth"):

– Software for the PMS and plant control system (PLS) logic cards. This type of CCF accounts for potential design errors in "common functions" software (i.e., software controlling fundamental processor functions, such as I/O, processing and communications). Because such functions, and its associated software, are repeated across all major subsystems of PMS and PLS, such software design errors could impact the reactor trip and ESF portions of PMS as well as all the PLS functions (and fail both their automatic and manual functions). If a software

fault of this kind existed and showed up every time an accident occurred without being detected, the plant CDF would increase by about four orders of magnitude. (In reality residual software faults do not show up, and thus they do not cause a software failure, unless the program is exposed to an environment for which it was not designed or tested).

– PMS ESF software components, such as input logic software, output logic software and actuation logic software. This type of CCF accounts for potential design errors in "application" software (i.e., software controlling the actual algorithms, protective and actuating functions that the PMS is designed to provide). Because a different application software controls each major PMS subsystem, this type of software CCF is contained within subsystems performing same or similar functions. If a software fault of this kind existed and showed up every time an accident occurred without being detected, the plant CDF would increase by almost three orders of magnitude.

– PMS ESF manual input multiplexer software. If the plant is operated with a fault in the multiplexer software which is assumed to fail the function of the multiplexer during an accident, the plant CDF would increase by over one order of magnitude.

- The AP1000 design is significantly less dependent on human actions for safety than operating reactors. If operators always failed to perform the human actions modeled in the PRA, the plant CDF would increase by almost two orders of magnitude (from about 2E-7/yr to about 2E-5/yr). Operator failure to perform the following actions was found to have the largest impact on the estimated CDF from internal events (i.e., operator actions with highest "risk achievement worth"):

  – diagnose a SGTR event,

  – manually actuate containment sump recirculation when automatic actuation fails,

  – manually actuate ADS for "feed and bleed" cooling when automatic actuation fails, and

  – perform a controlled shutdown to control and mitigate a RCS leak event.

- Failure of the following single components was found to have a significant impact on the estimated CDF from internal events (i.e., single components with highest "risk achievement worth"):

  – plugging of one IRWST discharge line strainer (important for a safety injection line break which disables one of the two redundant IRWST injection lines),

  – plugging or leak in the PRHR heat exchanger,

  - plugging or rupture of a flow tuning orifice in an accumulator injection or CMT injection line,
  - accumulator injection and CMT injection check valves,
  - non-class 1E dc distribution panel EDS3 EA 1 (supplies power to DAS which is important for ATWS sequences), and
  - Class 1E dc switchboard DS1 and distribution panel DD1.

- Failures of components associated with the following events were found to be major contributors to the estimated CDF from internal events (i.e., they have the highest "risk reduction worth"):
  - initiating events (dominated by safety injection line break, large LOCA and ADS spurious actuation),
  - plugging of one IRWST discharge line strainer (important for a safety injection line break which disables one of the two redundant IRWST injection lines),
  - CCF of both recirculation lines due to sump screen plugging,
  - CCF of two or more ADS stage #4 explosive (squib) valves to open on demand,
  - CCF of the four check valves in the two IRWST discharge lines,
  - CCF of the four explosive (squib) valves in the two IRWST discharge lines,
  - failure of one check valve in one accumulator injection line to open on demand (important for a large LOCA break which requires injection by both accumulators),
  - CCF of the IRWST level transmitters,
  - CCF of PMS ESF input logic groups (hardware),
  - CCF of the 4.16KV ac reactor coolant pump trip breakers to open , and
  - CCF of CMT AOVs to open.

- Operator failure to perform the following actions were found to be significant contributors to the estimated CDF from internal events; (i.e., these actions have the highest "risk reduction worth"):

- manually actuate safety systems through DAS, given failure to do so through PMS,
- manually actuate containment sump recirculation (when automatic actuation fails), and
- manually trip the reactor via PMS or DAS within one minute (given automatic trip failed).

The risk importance of non-safety-related "defense-in-depth" systems, credited in the AP1000 PRA, was also assessed. The major insights gained from such studies are summarized below:

- If the DAS becomes unavailable and the plant continues operating at power, the plant CDF would increase about 20 times.
- If the RNS becomes unavailable and the plant continues operating at power, the plant CDF would increase about two times.
- If the SFW system becomes unavailable and the plant continues operating at power, the plant CDF would increase less than two times.
- If both diesel generators become unavailable and the plant continues operating at power, the plant CDF would increase less than two times.
- If all non-safety-related "defense-in-depth" systems become unavailable and the plant continues operating at power, the plant CDF would increase by about two orders of magnitude (from about 2E-7/yr to about 1E-5/yr). Most of the contribution to such an increase in CDF is associated with transient and ATWS sequences.
- The DAS is very important in reducing the CDF associated with transient initiators (such as loss of main feedwater, loss of condenser and loss of component cooling water) and ATWS events. If all non-safety-related "defense-in-depth" systems with the exception of DAS become unavailable and the plant continues operating at power, the plant CDF would increase by less than one order of magnitude (from about 2E-7/yr to about 1E-6/yr).

As mentioned above, details on SSCs and human actions that were found to be risk significant by the applicant are documented in Chapter 50 of the AP1000 design PRA (for internal events at power operation). This information should be integrated with similar information from external events and shutdown risk analyses as well as information from the containment and offsite consequences analyses (levels 2 &3 of PRA) to form the basis for the following two lists:

- a list of important SSCs which the COL applicant should incorporate in the D-RAP program. This is identified as COL Action Item 19.1.3.1-1. The applicant should include such a list of important SSCs in DCD Tier 2 Chapter 17.4. This is part of Open Item 19.1.10.1-2 (see Section 19.1.10.1 of this report)

- a list of risk-important operator tasks that should be taken into account in the control room design as well as for implementing procedures and developing training programs. This is identified as COL Action Item 19.1.3.1-2. This list should be taken into account by the COL applicant in developing and implementing procedures, training and other human reliability related programs. DCD Tier 2 Chapter 18 discusses the use of such information in developing and implementing procedures, training and other human reliability related programs for the plant.

The applicant, in performing the level 1 PRA for internal events at power operation, identified the following risk-important tasks (with their PRA designators inside the parentheses), which must be performed by the operator to prevent or mitigate severe accidents. These tasks should be taken into account in the control room design. The process for inclusion of these tasks is addressed in Section 18.7 of this report.

- Operator fails to manually actuate ADS (AND-MAN01)
- Operator fails to manually trip reactor via PMS within one minute (ATW-MAN03)
- Operator fails to manually trip reactor via DAS (ATW-MAN04C)
- Operator fails to manually trip reactor via PMS within five minutes (ATW-MAN05)
- Operator fails to diagnose a SGTR event (CIB-MAN00)
- Operator fails to isolate failed SG (CIB-MAN01)
- Operator fails to recognize need for manual depressurization during a small LOCA or transient event (LPM-MAN01)
- Operator fails to recognize need for manual depressurization during a medium LOCA (LPM-MAN02)
- Operator fails to actuate a system using DAS only (REC-MANDAS)
- Operator fails to actuate containment sump recirculation when automatic actuation fails due to IRWST level signal failure (REN-MAN04)
- Operator fails to perform controlled shutdown (OTH-SDMAN)

Additional risk-important operator tasks related to shutdown operation and to containment performance (Level 2 PRA) are reported in Section 19.1.4.5 and Section 19.1.3.2 of this report, respectively.

In designing the AP1000 control room, it is important that no new significant human errors be introduced. To this end, during the main control room validation process, the COL applicant should qualitatively confirm that the "findings" from the integrated system validation do not lead to a risk-significant increase in error potential over that represented in the AP1000 PRA HRA. If this is not confirmed, the COL applicant should model the additional risk-significant errors in an updated HRA. This is COL Action Item 19.1.3.1-3 and part of Open Item 19.1.10.1-2 (see Section 19.1.10.1 of this report).

19.1.3.1.5 Insights from the Sensitivity Studies

The applicant performed several sensitivity studies to gain insights about the impact of uncertainties (and potential lack of detailed models) on the estimated CDF. The staff used the

applicant's PRA results to perform additional sensitivity studies to gain more complete insights when it was necessary. The sensitivity studies performed by the applicant and the staff, have the following objectives:

- determine the sensitivity of the estimated CDF from internal events to potential biases in numerical values, such as initiating event frequencies, failure probabilities, and equipment unavailabilities,

- determine the impact of potential lack of modeling details, such as long-term cooling with the PRHR following a transient or a LOOP/SBO event, on the estimated CDF from internal events, and

- determine the sensitivity of the estimated CDF to previously raised issues, such as passive system check valve reliability.

In addition, sensitivity studies were performed to investigate the impact of uncertainties on PRA results under the assumption of plant operation at power without credit for the non-safety-related "defense-in-depth" systems ("focused" PRA model). These studies provided additional insights about the risk importance of the "defense-in-depth" systems which were taken into account in selecting non-safety-related systems for "regulatory treatment" according to the RTNSS process. Insights related to CDF are reported in this section while similar insights related to large release frequency and conditional containment failure probability (CCFP) are reported in Section 19.1.3.2 of this report.

19.1.3.1.5.1 Sensitivity to Potential Biases in Numerical Values

Results of studies to determine the sensitivity of the estimated CDF from internal events to potential biases in numerical values, such as failure probabilities, are summarized below.

19.1.3.1.5.1.1 Explosive (Squib) Valve Reliability

Squib valves are used in all ADS stage 4 lines, all IRWST injection lines and all containment sump recirculation lines. Because of the lack of adequate data for the AP1000 squib valves and uncertainties in the extrapolation of data from other designs and sizes to AP1000 operating conditions, there is uncertainty in the mean value of the failure probability of a squib valve to operate. A sensitivity study was performed to assess the impact of this uncertainty on PRA results and insights.

- Increasing the failure probability by a factor of five (i.e., the value recommended in EPRI's "Advanced Light Water Reactor Utility Requirements Document", Volume III, ALWR Passive Plan), the CDF would increase by less than a factor of two.

- Increasing all CCF probabilities of squib valves by a factor of ten, the CDF would increase by about a factor of three.

These results indicate some sensitivity of the CDF to reasonable increases of the mean value of the failure probability of squib valves used in the PRA but not large enough, by itself, to impact PRA conclusions and insights about the design.

19.1.3.1.5.1.3 Circuit Breaker Reliability

The most important circuit breakers (CBs) modeled in the AP1000 PRA are the reactor trip, the M-G set trip and the RCP trip CBs. Failure to open any of several sets of four reactor trip CBs causes failure of reactor trip through the PMS. Failure to open both M-G set trip CBs causes failure of the alternate means of tripping the reactor through DAS. Failure of any of several sets of RCP CBs causes failure of one or more RCPs to trip following an accident initiating event and potential failure of CMT injection and ADS automatic actuation. There is uncertainty in the mean values of the failure probabilities of CBs to open used in the AP1000 PRA. This uncertainty is the result of the use of failure rates for CBs to open on demand that are lower than generic failure rates, the linear extrapolation of failure rates to longer testing intervals and potential approximations in calculating CCF probabilities. A sensitivity study was performed to assess the impact of this uncertainty on PRA results and insights.

- Increasing the CB failure to open probabilities used in the AP1000 PRA by an order of magnitude, the CDF would increase by less than a factor of two. This indicates a small sensitivity of the CDF to reasonable increases in the mean value of the failure probabilities of CBs to open on demand.

- Increasing the CB failure to open probabilities used in the AP1000 PRA by an order of magnitude and at the same time assuming that all non-safety-related "defense-in-depth" systems become unavailable and the plant continues operating at power, the plant CDF would increase about 50 times from 2.4E-7/yr to about 1.2E-5/yr (based on risk importance study results, unavailability of the non-safety-related systems alone would increase the plant CDF about 30 times). This indicates that if the plant is operating without the non-safety-related "defense-in-depth" systems, the CDF is sensitive enough to reasonable increases in the mean values of CB failure to open probabilities used in the PRA to impact PRA conclusions and insights about the design (e.g., the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process).

- Increasing the CB failure to open probabilities used in the AP1000 PRA by an order of magnitude and at the same time assuming that all non-safety-related "defense-in-depth" systems, with the exception of DAS, become unavailable and the plant continues operating at power, the plant CDF would increase by less than one order of magnitude (from 2.4E-7/yr to about 2E-6/yr). Since the unavailability of the non-safety-related systems alone would increase the plant CDF by about a factor of five (based on risk importance study results), the plant CDF is not as sensitive to reasonable increases in the mean values of CB failure to open probabilities used in the PRA when the plant is operating without all non-safety-related "defense-in-depth" systems but DAS. This underlines the importance of the reactor trip function of DAS in reducing the impact of uncertainties associated with CB failure probabilities on PRA conclusions and insights

about the design (e.g., on the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process).

19.1.3.1.5.1.3 Digital I&C System Software Reliability

Digital I&C systems are designed as complex combinations of hardware and software (i.e., computer programs) components. Although computer software does not wear out, as hardware does, it can fail as a result of the excitation of residual design errors when a particular combination of inputs occurs. If one could eliminate all the design errors before a software product is put in operation, it would work perfectly forever. However, it is impossible to be certain that a software product is error free. On the contrary, experience shows that there are always residual faults which do not manifest themselves, and thus, they do not cause a software failure unless the program is exposed to an environment for which it was not designed or tested. Exposure to such an environment is possible because, as a result of the large number of possible states and inputs in most software programs, it is extremely difficult to perfectly comprehend program requirements and implementation and it is virtually impossible to test more than a small subset of all possible input combinations during development. Thus, software reliability is essentially a measure of the confidence one has in the design of the software and its ability to function properly in its expected environment.

Quantification of software reliability may be too difficult, especially for software that must meet high reliability requirements such as those used in the AP1000 design. This difficulty results from the random nature of a large number of possible inputs, the unknown mechanisms of human failure that creates errors during the development process, and the randomness of the testing process used to detect errors. However, regardless of whether the reliability of software can be accurately quantified, the design goal must be to minimize the number of residual errors, their frequency of occurrence, and their effect on system performance. This can be achieved by following formal and disciplined methods during the development process combined with an expected use-based testing program. For these reasons, each software product is unique and extrapolation of statistical data for other products is meaningless.

From the basic properties of software it follows that commonly used hardware redundancy techniques do not improve software reliability. The several defense mechanisms against hardware CCFs that are incorporated in the design (such as redundancy, separation, operational testing, maintenance, and immediate detectability of failure provided by the on-line diagnostics) cannot be relied upon to prevent software CCFs. If the same programs are executed in two or more channels (or divisions) in parallel, a software fault would lead to a common mode software failure in all channels (or divisions) at the same time, i.e., it would be a CCF of redundant channels or divisions. Thus, a highly reliable software product is needed whenever the same program is executed in two or more channels (or divisions) in parallel. Since the reliability of a software product is basically determined during development and testing, the importance of the software development process in achieving high reliability cannot be overestimated.

Although it is not easy to quantify software reliability, it is generally accepted that high reliability can be achieved by following formal and disciplined methods during the development process

combined with an expected use-based testing program. The AP1000 design PRA assumes high reliability for all software used in the digital I&C systems. The applicant expects to develop highly reliable software for the AP1000 I&C systems by setting reliability goals and design requirements and by incorporating features in the software design which act as "defenses" against CCFs. Such requirements and design features include the following four items:

- requirements for formalized design phases, for following design standards and for performing formal design reviews,

- requirement for an expected use-based software testing and verification program,

- incorporation of "fail safe" capability in the design, i.e., incorporation of mechanisms (independent of the source of error) for detecting errors at the module or intermediate level and producing a well defined output which results in an application specific safe action, and

- incorporation of "functional diversity" which allows initiation of automatic protection functions even when errors associated with some plant parameters are present (different plant parameters initiate same automatic protection function independently).

A sensitivity study was performed by the staff, using the applicant's PRA models and results, to assess the impact of uncertainty in the mean value of software failure probabilities used in the AP1000 PRA on PRA results and insights. The major findings of this study are summarized below:

- Increasing software failure probability by an order of magnitude, the CDF would increase by about 20 percent (from 2.4E-07/yr to about 3.0E-07/yr). This indicates a rather small sensitivity of the plant CDF to reasonable increases in the mean values of software failure probabilities used in the PRA.

- Increasing software failure probability by an order of magnitude and at the same time assuming that all non-safety-related "defense-in-depth" systems become unavailable and the plant continues operating at power, the plant CDF would increase by almost three orders of magnitude from 2.4E-07/yr to almost 1E-04/yr. (Based on risk importance study results, unavailability of the non-safety-related systems alone would increase the plant CDF by about two orders of magnitude). This indicates that if the plant is operating without the non-safety-related "defense-in-depth" systems, the CDF is sensitive enough to reasonable increases in the mean values of software failure probabilities used in the PRA to impact PRA conclusions and insights about the design (e.g., the selection of nonsafety-related SSCs for regulatory oversight according to the RTNSS process).

- Increasing software failure probability by an order of magnitude and at the same time assuming that all non-safety-related "defense-in-depth" systems, with the exception of DAS, become unavailable and the plant continues operating at power, the plant CDF would increase by almost one order of magnitude (from 2.4E-07/yr to about 2E-06/yr).

Since the unavailability of the non-safety-related systems alone would increase the plant CDF by about a factor of five (based on risk importance study results), the plant CDF is not as sensitive to reasonable increases in the mean values of software failure probabilities used in the PRA when the plant is operating without all non-safety-related "defense-in-depth" systems but DAS. This underlines the importance of the engineered safety features (ESF) actuation function of DAS in reducing the impact of uncertainties associated with software failure probabilities on PRA conclusions and insights about the design (e.g., on the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process).

19.1.3.1.5.2 Sensitivity to Potential Lack of Modeling Details

Results of sensitivity studies performed to determine the impact of potential lack of modeling details on the estimated CDF from internal events are summarized below.

19.1.3.1.5.2.1 Modeling Spurious Actuation of Squib Valves

The applicant assessed contributions of spurious ADS valve actuation, caused by faults in I&C systems (PMS and DAS), to the various LOCA initiating event frequencies. This assessment, however, did not include faults in I&C copper cables (e.g., hot shorts) from the protection logic cabinets (PLCs) to the squib valve operators. A hot short in one of these cables could increase the current to the value that causes detonation of the squib valve operator. It was assumed in the AP1000 PRA that the frequency and impact on PRA results of this spurious actuation mechanism is very small, except in the presence of a fire. According to the applicant, spurious actuation of squib valves due to hot shorts, caused by cable insulation degradation or mechanical damage and the presence of humidity, is expected to be a very low frequency event for nuclear plant safety-grade cabling.

A study performed by the staff, using the applicant's PRA models and results, underlined the importance of incorporating features in the design of ADS cabling that will minimize the probability of hot shorts actuating an ADS squib valve. The applicant responded by incorporating additional features in the AP1000 design which further reduce the likelihood of spurious actuation of a squib valve, such as using a valve controller circuit which requires multiple hot shorts for actuation and physical separation of potential hot short locations.

19.1.3.1.5.2.2 Success Criteria for Containment Cooling by Air

A sensitivity study was performed by the applicant to investigate the impact of potential uncertainties in the success criteria for passive containment cooling. There is some uncertainty about adequate long-term containment cooling by air flow for some accidents. Late containment failure, and consequent loss of core cooling, cannot be ruled out for sequences involving release of steam inside the containment and unavailability of the water cooling mode of the PCS. In the sensitivity study it was assumed that all sequences requiring containment cooling would lead to core damage if the water cooling mode of the PCS is unavailable. This resulted in a rather small increase (about 30 percent) in the plant CDF. This finding indicates that the plant CDF is not sensitive to uncertainties in the success criteria for containment

cooling by air used in the AP1000 baseline PRA. However, a similar conclusion cannot be reached without taking credit for non-safety-related “defense-in-depth” systems, such as SFW and RNS (see discussion in Section 19.1.10.1 of this report).

19.1.3.1.5.2.3 Mission Times for Systems Providing Long-Term Cooling

The applicant assumes, in the PRA, a mission time of 24 hours for long-term cooling independent of plant condition. The staff identified the following two categories of accident sequences that require long-term (beyond 24 hours) operator actions and/or system operation, and which could impact PRA results and insights about the design:

- LOCA sequences with impaired containment (no long-term recovery actions to replenish lost inventory were modeled).

- sequences with an open path outside containment (the potential need to replenish the lost IRWST or sump inventory was not modeled).

A sensitivity study performed by the staff has shown that the impact of this issue on the estimated CDF is rather small (the plant CDF from internal events would increase by less than 5 percent if long-term operator and/or system failures were included in the PRA models). In addition, the sensitivity study indicated that this issue does not have a significant impact on PRA conclusions and insights about the design. Furthermore, these concerns are addressed by the applcant through the development of ERGs for long-term operator actions.

19.1.3.1.5.3 Sensitivity to Previously Raised Issues

Results of studies performed to determine the sensitivity of the estimated CDF to previously raised issues are summarized below.

19.1.3.1.5.3.1 Check Valve Reliability

The applicability of generic failure data to CVs, present in several passive safety systems of the AP1000 design, has been an issue in the AP1000 PRA review. While CVs are not unique to the AP1000, the conditions under which they will be operating in the plant are different from those in current generation nuclear plants. Such CVs will have to open under very low differential pressures (created by the gravity driving head only) after long periods of being held closed (testing every 2 years at refueling) in the presence of stagnant borated water. To account for "less than ideal conditions" which may exist at the time the valves are demanded, the Electric Power Research Institute (EPRI) has recommended (“Advanced Light Water Reactor Utility Requirements Document”, Volume III, ALWR Passive Plant) increasing the standby failure rate of check valves in passive systems by a factor of five as compared to CVs in "pumped" systems used in operating reactor designs. The applicant, however, did not use the higher failure rate recommended by EPRI in the AP1000 PRA. This is justified, according to the applicant, because the CVs used in the IRWST injection lines, which are the most risk-important check valves in the AP1000 design, have two important features which compensate for the above-mentioned adverse conditions. First, contrary to most CVs at operating nuclear

power plants, the gate and seat design of these CVs allows for small leaks and makes them less susceptible to binding or sticking when they are closed. Second, because of the presence of the squib valves, there is no pressure holding the IRWST injection CVs closed which could force the disk to stick in the seat. The staff agrees that these features most likely improve CV reliability. However, the applicant did not submit data or analyses that could be used to show to what degree such features "compensate" for the adverse operating conditions of the AP1000 CVs (i.e., having to open under very low differential pressures after long periods of being held closed in the presence of stagnant borated water). As discussed below, the staff performed a sensitivity analysis to address the uncertainty due to the lack of data to support the reliability of these CVs assumed by Westinghouse in the PRA.

Another issue concerning CVs, which became apparent during the AP1000 PRA review, involves CCF histories at operating reactors and their applicability to AP1000 CVs. The CCF probabilities of check valves, assumed in the AP1000 PRA, are based on information provided in Revision 6 of the EPRI URD. The information on CCF of check valves, as revised in the last revision of EPRI's URD, leads to a decrease by about an order of magnitude in the value of CCF probability recommended in previous URD revisions which was used in previous PRAs for evolutionary designs and operating reactors. According to the applicant this is due to better understanding of individual events involving failure of check valves at nuclear power plants and that "EPRI found no common cause failures to open of check valves (other than failure modes unique to testable check valves)." An NRC-sponsored evaluation of LER and NPRDS events (see Common-Cause Failure data Collection and Analysis System, INEL-94/0064, December 1995), which occurred between 1980 and 1993 at operating nuclear power plants, has found about 20 events involving CCF of check valves. Although it can be argued that only a portion of such events are applicable to the AP1000 design, the staff believes that there is still significant uncertainty in the data used to calculate CCF probabilities of CVs in the AP1000 PRA.

A sensitivity study was performed by the staff, using the applicant's PRA models and results. The study assessed the impact of uncertainties associated with the CV failure rate and the CCF data, assumed in the AP1000 PRA, on PRA results and insights. The major findings of this study are summarized below:

- increasing both the CV failure rate by a factor of 5 (as recommended by EPRI) and the CV CCF multiplier by an order of magnitude (as in previous PRAs), would increase the CDF by about a factor of 5 (from 2.4E-07/yr to about 1E-06/yr)

- increasing both the CV failure rate by a factor of 5 (as recommended by EPRI) and the CV CCF multiplier by an order of magnitude (as in previous PRAs), and at the same time assuming that all non-safety-related "defense-in-depth" systems become unavailable and the plant continues operating at power, the plant CDF would increase almost two orders of magnitude (from 2.4E-07/yr to about 2E-05/yr)

- increasing both the CV failure rate by a factor of 5 (as recommended by EPRI) and the CV CCF multiplier by an order of magnitude (as in previous PRAs) and at the same time assuming that all non-safety-related "defense-in-depth" systems with the exception of DAS become unavailable and the plant continues operating at power, the plant CDF

would increase about 10 times (from 2.4E-07/yr to about 3E-06/yr). If, in addition to the above changes, the explosive valve failure rate is also increased by a factor of 10 (as explained in above mentioned study), the CDF would increase about 15 times (from 2.4E-07/yr to about 3.5E-06/yr).

- increasing both the CV failure rate by a factor of 5 (as recommended by EPRI) and the CV CCF multiplier by an order of magnitude (as in previous PRAs) and at the same time assuming that all non-safety-related "defense-in-depth" systems with the exception of DAS and the normal residual heat removal system (RNS) become unavailable and the plant continues operating at power, the plant CDF would increase by almost one order of magnitude (from 2.4E-07/yr to almost 2E-06/yr). Such an increase in CDF is not affected significantly when the failure rate for the explosive valves is also increased by a factor of five. This indicates that the availability of RNS significantly reduces the impact of uncertainties associated with failure probabilities of check valves and explosive (squib) valves on PRA conclusions and insights about the design (e.g., on the selection of nonsafety-related SSCs for regulatory oversight according to the RTNSS process).

19.1.3.1.5.3.2 MOV Reliability

A sensitivity study, performed by the staff based on Westinghouse PRA models and results, indicated that the AP1000 CDF from internal events is not very sensitive to reasonable increases in MOV failure rates. This result shows that the AP1000 design is not very sensitive to the concern that generic MOV failure rates may have been underestimated.

19.1.3.1.5.3.3 Frequency of Large LOCAs

A sensitivity study was performed by the staff to investigate the impact of potential uncertainty associated with the large break LOCA initiating event frequency assumed in the AP1000 PRA. In the AP1000 PRA, the applicant used “experience data” reported in NUREG/CR-5750, “Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995," for pipe breaks as opposed to the more conservative data from pipe break analysis used in the AP600 PRA. This resulted in a large break LOCA frequency of 5E-06/yr as opposed to the 1E-04/yr frequency used in the AP600 PRA. However, the large break frequency reported in NUREG/CR-5750 is based on expert opinion and includes significant uncertainty. This investigation has shown a significant sensitivity to the assumed frequency of large breaks (the plant CDF would increase over four times, from 2.4E-07/yr to about 1.1E-06/yr, had the higher frequency of 1E-04/yr been used for large breaks). The staff’s review has identified the large LOCA frequency assumed in the AP1000 PRA as one of several areas of uncertainty which, individually or collectively, have the potential to affect PRA results and conclusions. This is part of Open Item 19.1.10.1-3 (see discussion in Section 19.1.10.1 of this report).

19.1.3.1.5.4 Summary of Major Insights from the Sensitivity Studies

The most important insights from the sensitivity studies are summarized below:

- The estimated CDF from internal events is very sensitive to several CCF probabilities. This underlines the importance of those design features and operational requirements which aim at preventing CCFs, namely divisional separation, diversity of redundant components, as well as appropriate maintenance and training programs.

- The AP1000 CDF from internal events is not very sensitive to reasonable changes in single component failure probabilities or initiating event frequencies.

- The estimated CDF is not sensitive to further reductions in safety system outage times for test and maintenance during power operation or to further reductions in human error probabilities.

- Uncertainties associated with failure probabilities of reactor trip components, such as circuit breakers, could have a significant impact on PRA conclusions and insights about the design (e.g., on the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process). Availability control of the reactor trip (RT) function of DAS provides an efficient means for minimizing the impact of such uncertainties on PRA conclusions and insights about the design.

- Uncertainties associated with failure probabilities of ESF actuation components, such as software, could have a significant impact on PRA conclusions and insights about the design (e.g., on the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process). Availability control of the ESF actuation function of DAS provides an efficient means for minimizing the impact of such uncertainties on PRA conclusions and insights about the design.

- Uncertainties associated with failure probabilities of passive system check valves and explosive (squib) valves could have a significant impact on PRA conclusions and insights about the design (e.g., on the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process). Availability control of the RNS reduces significantly the impact of such uncertainties on PRA conclusions and insights about the design.

- A reduction in the effectiveness of features incorporated into the design of ADS cabling to minimize the probability of hot shorts actuating an ADS squib valve could have a significant impact on PRA insights and conclusions.

- PRA conclusions and insights about the AP1000 design are not very sensitive to the concern that generic MOV failure rates may have been underestimated.

The insights from the sensitivity studies were integrated with insights from the uncertainty analysis and the risk importance studies and were used, in conjunction with the assumptions made in the PRA, to identify the design certification requirements reported in Section 19.1.8 of this report.

19.1.3.2 Results and Insights from the Level 2 PRA (Containment Analysis)

In the sections that follow, results and insights from the Level 2 portion of the PRA are presented. This includes the frequency of the various accident classes considered in the Level 2 analysis, the frequency and conditional probability of containment failure, 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 supporting sensitivity analyses.

19.1.3.2.1 Core Damage Sequences and Accident Classes Contributing to Containment Failure

In the AP1000 PRA, the end states of the Level 1 system event trees (core damage sequences) are binned into 11 accident classes on the basis of initiating event and RCS conditions at the onset of core damage. The definition of each accident class is provided in Table 19.1-2 of this report, along with the representative RCS pressure at the onset of core damage, and the CDF assigned to the class in the baseline PRA for internal events at power.

The majority of Level 1 sequences (about 90 percent) involve events with at least partially successful RCS depressurization, and relatively low RCS pressure (less than 1.03MPa (150 psig)) at the time of core uncovery. For high pressure core melt sequences, the potential to depressurize the RCS in the time period between the onset of core damage and challenge of the RCS pressure boundary is further evaluated in the Level 2 event tree. Thus, an even larger fraction of the core melt sequences (about 95 percent) is estimated to involve a depressurized RCS at the time of RCS pressure boundary challenge.

Accident class frequencies are propagated through the containment event tree (CET) to evaluate the potential for operator actions, safety system response, and the containment structure to mitigate the release. The CET includes top events/nodes that address the following:

- RCS depressurization after core uncovery
- containment isolation
- reactor cavity flooding (by gravity draining or manual actuation)
- reactor vessel reflooding and associated hydrogen production
- reactor vessel integrity
- passive containment cooling
- containment venting
- intermediate containment failure
- hydrogen igniter system availability
- diffusion flames at IRWST and valve vault exits
- early hydrogen detonation (during hydrogen release to containment)
- global deflagration
- intermediate hydrogen detonation (after hydrogen is mixed in containment)

The CET is quantified separately for each accident class. For system related top events, split fractions are quantified by linking to the system fault trees (i.e., top events for RCS depressurization, containment isolation, reactor cavity flooding, and hydrogen igniter system).

For the balance of the top events, split fractions are assigned scalar values based on a characterization of the underlying processes/phenomena.

Each end state of the CET is assigned to one of six containment release categories (RC). The applicant considered all containment release/failure categories except intact containment (IC) to constitute a large release, which is conservative. As such, the LRF reported in the PRA is equivalent to the CDF less the frequency of the IC RC. The conditional containment failure frequency for each accident class is presented in Table 19.1-3 of this report for the baseline PRA for internal events at power. The conditional containment failure probability for accident classes 1A, 1AP, 3A, and 6 (40 to 92 percent) is considerably higher than other classes because of failure of late depressurization in these sequences, which leads directly to containment bypass. The conditional containment failure probability for accident classes 3BL and 3BR is lower than other classes (e.g., 3BE and 3D/1D) because reactor cavity flooding occurs as a consequence of accident progression in these accident classes. In contrast, 3BE and 3D/1D sequences require manual actuation of the cavity flooding system, with a typical failure probability of about 0.05.

The frequencies of the various containment release categories and the fractional contributions by release category to the total large release frequency are presented in Figure 19.1-1 of this report and Table 19.1-4 of this report. The leading contributors to the various release classes are discussed further in Section 19.1.3.2.2 of this report.

19.1.3.2.2 Leading Contributors to Containment Failure from the Level 2 PRA

The breakdown of results from the PRA reveals that about 8 percent of the core damage events result in large release/containment failure. The bulk of these releases (about 54 percent) involve containment bypass. Early containment failures account for about 38 percent of the containment failure frequency. Containment isolation failure contributes about 7 percent. Intermediate containment failure (as a result of hydrogen detonation) and late containment failures (attributable to containment pressurization as a result of PCS failure) together contribute about 1 percent. Basemat melt-through is not treated as a separate failure mode in the updated PRA. Rather, all events that result in reactor vessel melt-through are considered to result in early containment failure, as discussed below.

Important contributors to each of these release categories are identified in Figure 19.1-2, and discussed further in the sections that follow.

19.1.3.2.2.1 Containment Bypass (BP)

Accident sequences in which fission products are released directly from the RCS to the environment via the secondary system or other interfacing system are classified as containment bypass. The total frequency of containment bypass failure in the baseline PRA is 1.1E-08/y, or about 54 percent of the containment failure frequency.

As shown in Figure 19.1-2 of this report, pressure and temperature-induced SGTR sequences account for 64 percent of the containment bypass frequency. High-pressure core melt

sequences are conservatively assumed to result in failure of the SG tubes as a result of either of the two following conditions:

- high differential pressures in ATWS sequences (accident class 3A) with failure of RCP trip, CMT injection, or PRHR
- thermally induced creep rupture in high pressure core melt sequences (accident classes 1A and 1AP) in which late depressurization is unsuccessful

Hot-leg creep rupture is not credited to prevent SG tube failure or high pressure vessel failure. Conservatively assuming that these events result in containment bypass obviates the need for additional thermal-hydraulic and probabilistic analyses of the following:

- the likelihood of RCS piping versus SG tube over-pressure failures in ATWS events
- the likelihood of containment failure from DCH pressure loads in high pressure core melt accidents
- the relative threat and timing of creep-rupture failures in RCS piping and SG tubes in high pressure core melt accidents

SGTR-initiated core melt sequences with failure to depressurize the RCS prior or subsequent to core uncovery (accident class 6) account for the balance of the bypass frequency (approximately 36 percent). The potential for RCS depressurization is evaluated in the Level 2 analysis. Depressurization is credited in sequences in which the following occurs:

- PRHR is successful and ADS fails by operator error initially but is successfully recovered before extensive core damage
- PRHR and ADS are successful (core melt occurs in these sequences as the result of failure of sump recirculation).

RCS depressurization is successful in approximately half of the Level 1 SGTR sequences in the baseline PRA. SGTR sequences with successful depressurization are not considered to result in containment bypass due to low RCS pressure and high water level in the faulted SG, and therefore, are not reflected in the 36 percent contribution from SGTR events in Figure 19.1-2 of this report. Instead, these events are further evaluated in the CET, where they generally result in an intact containment and a benign source term. The assumption that the SG level will be maintained above the break in such sequences is important to LRF and dose results, and will be further assured by inclusion of appropriate guidance on SGTR response within the severe accident management guidance to be developed by the COL applicant.

In previous PRAs, interfacing system LOCA sequences are typically a major concern for containment bypass. However, as a result of piping system upgrades discussed previously, the frequency for ISLOCA sequences is very low for AP1000 (5E-11/y). As such, the contribution

of interfacing-systems loss-of-coolant accident (ISLOCA) sequences to CDF and risk is negligible.

The containment bypass release category is characterized in the PRA by a loss of feedwater transient with subsequent creep rupture of five SG tubes and the failure of a SG safety valve to reseat (Case 1A-2). The fission product release to the environment begins approximately at the onset of fuel damage. In the AP600 PRA, the applicant applied a decontamination factor (DF) of 100 to the aerosol release fractions calculated from the MAAP code to account for impaction on the SG tubes, which was not modeled in MAAP. The sequence description provided by the applicant does not indicate whether additional attenuation of the source term beyond that which is explicitly modeled in MAAP is credited in this calculation. This will be confirmed as part of the Open Item 19.1.10.3-1 related to the selection of representative sequences for assigning source terms.

19.1.3.2.2.2 Early Containment Failure (CFE)

Accident sequences in which containment failure occurs within the period between onset of core damage and the end of core relocation are classified as early containment failure. In the baseline PRA, containment failures in this time period are caused by events involving RPV failure or hydrogen detonation. The total frequency of CFE in the baseline PRA is 7.5E-09/y, or about 38 percent of the containment failure frequency.

The majority of the early failure frequency in the baseline PRA is associated with failure of the RPV. About 66 percent of the CFEs involve 3BE and 3D sequences with failure of reactor cavity flooding and subsequent reactor vessel failure. An additional 13 percent is attributed to spontaneous reactor pressure vessel failure events (3C) in which the vessel is not able to be reflooded to prevent debris relocation. The major cause of cavity flooding failure in AP600 was:

- common cause failure of strainers in IRWST tank,
- common cause failure of actuation software and hardware,
- common cause failure of recirculation MOVs to open, and
- operator failure to open the IRWST valves to flood the reactor cavity.

Similar information has not been provided for AP1000. Such information is useful for identifying major contributors to system failure and confirming that reasonable measures have been taken to reduce risk. The staff will request that the applicant provide this information for AP1000. This is Open Item 19.1.10.3-2 (see Section 19.1.10.3 of this report).

CFE is assumed to occur as a result of ex-vessel phenomena associated with debris relocation into the reactor cavity in low pressure core melt sequences. This assumption conservatively bounds uncertainties related to ex-vessel FCI, CCI, and impingement of corium on the containment shell. High pressure core melt sequences, which could potentially challenge the containment from DCH, are assumed to result in containment bypass and do not contribute to

early containment failure. The assumption that RPV failure leads to CFE was made in view of the following:

- the high probability that the reactor cavity will be flooded in a core melt accident,
- high confidence that molten core debris would be retained in-vessel due to the incorporation of external reactor vessel cooling features in the AP1000 design, and
- the large uncertainties associated with ex-vessel debris spreading and fuel coolant interactions.

Deterministic calculations performed by the applicant and documented in DCD Tier 2 Appendix 19B indicate that containment integrity would be maintained despite localized structural failures predicted for an ex-vessel FCI (interaction of molten fuel with residual break flow expected to be present in the cavity with failure of reactor cavity flooding), and core concrete interactions. Although many of the events contributing to CFE frequency could be expected to result in later or no containment failure on the basis of these calculations, the bounding assumption was made in view of the uncertainties in the resulting endstates. This assumption dominates the probability of early containment failure in the AP1000 PRA.

CFE as a result of hydrogen combustion account for 21 percent of the CFE frequency. The majority (13 percent) is attributed to creep rupture of the containment shell due to diffusion flames at adjacent, failed-open, IRWST louvered-vents. The threat from diffusion flames was found to be important for AP600, and is significantly reduced in AP1000 by addition of the louvered-vent feature. The remaining hydrogen-related failures (8 percent) involve early hydrogen detonation because of failure of the hydrogen igniter system. The major causes of igniter failure in AP600 were found to be:

- common cause failure of igniters
- failure of the 12 volt distribution panel
- operator failure to actuate the hydrogen control system
- station blackout

Similar information has not been provided for AP1000. Such information is useful for identifying major contributors to system failure and confirming that reasonable measures have been taken to reduce risk. The staff requests that the applicant provide this information for AP1000. This is Open Item 19.1.10.3-2.

The actual frequency of early containment failure from hydrogen combustion is small due to the high reliability of the hydrogen igniter system, the small fraction of core damage sequences involving station blackout sequences in the AP1000 design, and the addition of the IRWST louvered-vents.

The applicant evaluated the potential for early containment failure from deflagrations in the development of the Level 2 event trees, but judged the contribution to be insignificant. Deflagrations were not considered to contribute to early containment failure because of the

limited quantities of combustible gases produced when core debris is successfully retained in-vessel, and are not modeled as a contributor to early containment failure in the containment event tree (Failure to retain the core debris in-vessel would result in larger amounts of combustible gases, but such sequences are already assumed to result in early containment failure as discussed above).

A non-safety grade containment spray system is included in the AP1000, but its impact on containment response is not reflected in the Level 2 and 3 PRA results. The use of sprays is generally considered to be beneficial in terms of reducing containment pressure and enhancing fission product removal. In view of the potential for the sprays to adversely impact containment response by increasing the likelihood and magnitude of hydrogen combustion events, the staff requested the applicant to evaluate the impact of spray operation on hydrogen combustion modeling and assumptions in the Level 2 analysis, and to confirm that containment performance (and containment failure frequency) will not be adversely impacted. The applicant assessed the effect of sprays on the evaluation of containment failure for each combustion mode treated in the PRA, and determined that the operation of the non-safety-related spray system has no significant impact on the containment failure probability determined in the AP1000 hydrogen assessment. Given the very low frequency of sequences involving failure of PCS (in which use of sprays could result in deinerting of the containment atmosphere), the staff agrees that the potential for containment sprays to adversely impact containment performance would be insignificant.

Additional mechanisms that contribute to early containment failure in other PRAs include in-vessel FCI (alpha mode failure), rocket mode failure, and corium impingement as a result of high pressure melt ejection. The applicant evaluated these mechanisms and found them to be insignificant based on deterministic and probabilistic considerations. The potential for containment failure from in-vessel FCI was addressed for AP600 using ROAAM, and judged to be physically unreasonable. This analysis and conclusion has been extended to AP1000 (see Section 19.2.3.3.5.1 of this report). Even if NUREG-1150 mean values are used to quantify the conditional containment failure probability from this containment failure mode, the absolute value of containment failure frequency as a result of alpha mode would be very small. Reactor vessel displacements associated with postulated ex-vessel steam explosions were also considered and determined to not affect the integrity of the containment and associated equipment. Corium impingement on the containment shell is precluded by the AP1000 containment layout and the inclusion of a protective layer of concrete in the reactor cavity, as described in Section 19.2.3.3.3 of this report.

The CFE release category is represented in the PRA by a spurious actuation of two ADS Stage 4 valves with failure of IRWST injection, successful cavity flooding and in-vessel retention, and successful operation of hydrogen igniters (Case 3D-4). A diffusion flame is assumed to occur due to hydrogen release from the IRWST, and result in containment failure. The fission product release to the environment begins approximately at the time of containment failure. The staff notes that the sequence description is inconsistent in that releases from the ADS Stage 4 valves enter directly into containment rather than into the IRWST, and given the location of the valves relative to the containment shell, would not result in diffusion flames that can challenge containment. If the sequence were defined in a consistent manner (e.g., failure of Stage 3

rather than Stage 4 valves) the resulting source terms could be significantly different. Westinghouse needs to justify the selection of this sequence as representative of early containment failures given this inconsistency. This is Open Item 19.1.10.3-1 (see Section 19.1.10.3 of this report).

19.1.3.2.2.3 Intermediate Containment Failure (CFI)

CFIs are defined as events in which containment failure occurs in the time period between the end of core relocation and 24 hours after the onset of core damage. Risk significant contributors to CFI involve failure of the hydrogen igniter system and containment failure due to hydrogen detonation in the intermediate time frame. Sequences with containment over-pressurization due to failure of both PCS and containment venting also contribute, but this contribution is negligible. The total frequency of CFI in the baseline PRA is 1.9E-10/y, or about 1 percent of the containment failure frequency.

Within the containment event tree, global hydrogen deflagrations are modeled as a potential contributor to CFI for events in which igniters are failed. However, the containment failure probability from deflagration was judged to be negligible and assigned a value of zero. Quantification was based on combining a probability distribution of the peak adiabatic isochoric complete combustion (AICC) hydrogen burn pressure (developed from separate probability distributions for hydrogen generation and pre-burn containment pressure) with the conditional containment failure probability distribution. Scenarios with no reflooding, early reflooding, and late reflooding of the RPV were separately evaluated and limited sensitivity analyses were performed. In all cases, the containment failure probability from deflagration was determined to be negligible and therefore assigned a value of zero. Deflagrations do not contribute to CFI because of the limited quantities of combustible gases produced when core debris is successfully retained in-vessel (Failure to retain the core debris in-vessel would result in larger amounts of combustible gases, but such sequences are already assumed to result in early containment failure as discussed above).

The CFI release category is represented in the PRA by a DVI line break in the PXS compartment with: failure of IRWST injection; successful cavity flooding, reactor vessel reflood, and in-vessel retention; and failure of hydrogen igniters (Case 3BE-3). The hydrogen generated in the primary system is released into the SG compartments, IRWST and the valve vault room. A detonation to deflagration transition is assumed to occur in the CMT room in the intermediate timeframe (after reflood), causing containment failure. Containment failure occurs after the majority of the fission products have been released from the RCS, thus some time is available for fission product deposition within the containment.

19.1.3.2.2.4 Late Containment Failure (CFL)

CFL is defined in the AP1000 PRA as a failure occurring later than 24 hours after the onset of core damage. All contributors to late containment failure involve failure of the passive containment cooling system, and containment failure as a result of late over-pressurization. The total frequency of CFL in the baseline PRA is about 3E-13/y, or less than 0.1 percent of the containment failure frequency.

Unlike AP600, in which air cooling of the containment alone is sufficient to maintain containment pressure less than Service Level C (627.4KPa (91 psig)), failure to deliver PCS water to the containment shell is considered a containment failure mode in the AP1000 PRA. This is due to the inability to remove the higher decay heat levels in AP1000 by air cooling only. Based on MAAP calculations performed for both nominal and bounding representations of decay heat, ambient air temperature, and containment shell temperature, the majority (98 percent) of events involving failure of PCS water delivery are considered to result in a CFL. The remainder (2 percent) are considered CFIs. The actual frequency of CFL is quite small due to the high reliability of PCS water delivery. The reliability of PCS water delivery in AP1000 has been improved over AP600 by addition of a third, parallel water supply line for PCS, controlled by a diverse valve (a MOV in contrast to an air-operated valve (AOV) in each of the other two lines).

In the AP600 PRA, PCS failure was dominated by blockage of the PCS annulus drain lines, which was estimated to have a probability of 1E-04. This failure mechanism is not modelled in the AP1000 PRA, but at that same failure probability would have a corresponding containment failure frequency of about 2E-11/y. Containment pressurization will initially be limited by PCS water delivered to the containment shell. However, following depletion of PCS water inventory (at approximately 72 hours) containment pressure will increase and eventually exceed Service Level C due to blockage of the air cooling path. Inclusion of this failure mode would substantially increase the frequency of late containment failures in AP1000. However, the frequency of CFL would remain less than 0.1 percent of the total containment failure frequency. Although not a key failure mode, the availability of the PCS annulus drains will be confirmed every two years in accordance with the AP1000 TS.

The following additional CFL modes were evaluated in other ALWR PRAs, but were not explicitly modeled in the AP1000 PRA for the reasons discussed below:

- containment basemat melt-through
- containment over-pressurization failure non-condensible gas generation, or late hydrogen burn
- containment over-temperature failure (other than diffusion flames)

Sequences that proceed to RPV failure could lead to basemat melt-through or over-pressurization from non-condensible gas generation, but are conservatively treated as CFEs in the AP1000 PRA. Hydrogen combustion would have a negligible contribution to CFLs given the high availability of igniters, the limited amount of hydrogen that can be produced in-vessel, and the likelihood that this hydrogen would be burned in the early and intermediate time frames. Hydrogen combustion was therefore not modeled as contributing to late containment failure. Late containment over-temperature failure would be a viable threat only if the reactor cavity is dry and the containment heat removal is lost. Such events are of low frequency, given the high probability of a flooded reactor cavity and the high reliability and independent nature of PCS in the AP1000 design, and they are conservatively assumed to lead

to early containment failure in the PRA. The over-temperature challenge would be further reduced by use of the non-safety containment sprays.

The CFL release category is represented in the PRA by a 5.1-cm (2-in.) hot-leg break in the steam generator compartment with failure of IRWST injection, failure of cavity flooding and in-vessel retention, and successful operation of hydrogen igniters (Case 3BE-7). Containment failure was assumed to occur coincident with RPV failure. The staff notes that containment failure occurs at 3 hours in this case, which is inconsistent with the time frame for late containment failure. Sequences in this release category would typically involve containment failure many hours after core damage and fission product release from the RCS, and significant opportunity for fission product deposition prior to containment failure. Thus, the resulting source terms could be significantly different. The applicant needs to justify the selection of this sequence as representative of late containment failures given this inconsistency. This is Open Item 19.1.10.3-1 (see Section 19.1.10.3 of this report).

19.1.3.2.2.5 Containment Isolation Failure (CI)

CIs are events involving failure of the system of valves that close the penetrations between the containment and the environment. The containment isolation analysis in the AP1000 PRA consists of a screening of all penetrations to identify those penetrations whose failure would result in a failure of the containment isolation function, and a fault tree analysis on the remaining penetrations to determine the probability of failure to isolate. Penetrations retained in the analysis (i.e., not screened out) are limited to the following lines:

- instrument air in normal containment sump
- containment air filter supply and exhaust
- main steam lines and feedwater lines
- startup feedwater lines
- steam generator blowdown lines

Failure of steam generator isolation following a SGTR, and steamline isolation following a main steamline break event are considered in the Level 1 event tree analysis, but do not contribute to the containment isolation frequency reported in the Level 2 PRA. The frequency of containment isolation failure in the baseline PRA is 1.9E-09/yr, or about 7 percent of the containment failure frequency. The probability of a pre-existing opening in containment large enough to constitute an isolation failure (1.2E-04) is included in the Level 1 fault tree model for LOCA, but was omitted in the containment isolation fault trees. The inclusion of this contributor would not noticeably impact the CI frequency. Nevertheless, for completeness of the PRA model, the staff believes that Westinghouse should include this failure mechanism within the AP1000 PRA. This is Open Item 19.1.3.2-1.

The CI release category is represented in the PRA by a large LOCA at the reactor vessel belt-line with successful IRWST injection, successful cavity flooding and in-vessel retention, and successful operation of hydrogen igniters (Case 3C-2). It is the staff's understanding that the containment isolation failure is represented in the PRA by a failure to close the largest containment penetration, an 45.7cm (18 in.) diameter purge line, at the onset of the accident.

Thus, fission product releases from the RCS can pass from the containment to the environment with reduced potential for attenuation. This will be confirmed as part of Open Item 19.1.10.3-1 related to the selection of representative sequences for assigning source terms.

19.1.3.2.3 Important Insights from Level 2 PRA and Supporting Sensitivity Analyses

Insights from the Level 2 PRA are summarized below. These are organized in terms of equipment/design features, severe accident phenomena/challenges, and human actions.

19.1.3.2.3.1 Equipment/Design Features

External reactor vessel cooling (ERVC) is effective in the majority of sequences. The AP1000 design incorporates several features that enhance ERVC relative to operating plants, including the following:

- safety grade systems for RCS depressurization and reactor cavity flooding
- a unique RPV thermal insulation system that improves coolant access to the RPV during severe accidents and is not subject to clogging or structural failure by ERVC-related loads
- a "clean" lower head that is unobstructed by penetrations

Credit for ERVC in the Level 2 analysis results in the majority (~97 percent) of core melt accidents (that do not involve containment bypass or containment isolation) being arrested in-vessel in the baseline PRA. As such, containment challenges from ex-vessel FCI and CCI are avoided and the quantity of hydrogen generated is limited in most core melt accidents.

High reliability of RCS depressurization and reactor cavity flooding contribute to the success of ERVC. Credit for ERVC in the PRA is based on a deterministic analysis of ERVC using the Risk Oriented Accident Analysis Methodology (ROAAM), which concludes that thermally-induced failure of an externally flooded AP1000-like reactor vessel is "physically unreasonable", AP1000-specific testing and analyses to extend this work to the AP1000 design, and a probabilistic assessment of the likelihood of achieving the necessary conditions for successful ERVC. Requisite conditions are:

- depressurization of the RCS to below 1.03 mpa (150 psi) before RCS pressure boundary challenge
- flooding of the reactor cavity to a level above the reactor vessel nozzle gallery (Elevation 98') prior to the time at which core debris would relocate to the lower head, vaporize the water in the lower head, and reheat to the point of melting additional structures. A value of 70 minutes after core exit temperatures exceed 648.9°C (1200°F) is used to define this criteria.

Sufficient depressurization (as the result of successful operation of Stages 1-3 of ADS or large LOCA break flow) is achieved in about 95 percent of the core melt sequences. Adequate reactor cavity flooding is achieved in about 98 percent of the sequences. About half of the core damage events require operator actuation of the cavity flooding system to ensure successful cavity flooding, but the remaining half would adequately flood as a direct consequence of the accident progression, even without manual actions. If the operator always fails to manually flood the reactor cavity, the containment failure frequency would increase from 1.9E-08/yr to 1.6E-07/yr, and the CCFP would increase from 8.1 to 66 percent. Common cause failure of IRWST discharge line strainers is a dominant contributor to failure of reactor cavity flooding and early containment failure in the PRA. IRWST strainer plugging will be controlled by inclusion in D-RAP, and by a TS requiring verification that the screens are not restricted by debris.

Reflooding of the RPV through postulated RCS pipe breaks has a significant effect on hydrogen production. If the initiating event is a LOCA in the loop compartment, RPV reflooding occurs after significant core damage and cladding oxidation have already occurred, and does not significantly impact hydrogen production. However, if the initiating event is a DVI line break in the valve vault room and the gravity injection valves in the broken DVI line open, RPV reflooding occurs while cladding oxidation is just beginning, and substantially enhances hydrogen production in the supporting MAAP calculations. Although RPV reflooding is addressed as a separate top event in the CET, the outcome of reflooding has no appreciable impact on containment performance because the igniter system and cavity flooding system function in the majority of sequences to mitigate the effect of additional hydrogen produced by reflood and to retain the core debris in-vessel.

Diversity between injection and recirculation squib valves is important to Level 2 results. An important modeling assumption for 3BE sequences is that the IRWST injection squib valves are diverse from the containment recirculation squib valves. As such, when IRWST injection is failed as a result of CCF of squib valves in the injection line, credit is taken for diverse squib valves in the recirculation lines used for reactor cavity flooding. Diversity is derived from the difference in operating conditions and design pressures for these valves, and is not considered to be compromised by maintenance errors or environmental/aging effects.

A specific reactor cavity concrete type is not required to meet the Commission's goals regarding large release frequency and conditional containment failure probability. Compared to other ALWRs, the AP1000 ex-vessel debris bed is deeper, and the concrete basemat is thinner. Although these factors tend to increase the severity of basemat erosion, deterministic analyses indicate that in the event of unabated CCI, containment basemat penetration or containment over-pressurization will not occur until after 2 days, regardless of concrete composition. Based on these results, the AP1000 design does not impose any restrictions on the type of concrete that can be used for the containment basemat and the reactor cavity walls. The impact of basemat concrete composition on overall plant risk is not readily apparent from the PRA since all events that lead to reactor vessel breach are assumed to result in CFE from other mechanisms. The staff expects the risk contribution from CCI to be small however, since the consequences associated with basemat melt-through or late containment over-pressure at the earliest projected times would be benign relative to other failure modes. Operation of the

non-safety-related containment spray system would further reduce the risk from over-pressure failure.

PCS water delivery is required to assure containment integrity. Failure of PCS water delivery to the containment shell is considered a containment failure mechanism in the PRA, since containment cooling by air alone is sufficient to limit containment pressure to values below the applicant's Service Level C estimate. The majority (98 percent) of events involving failure of PCS water delivery are considered to result in a CFL (after to 24 hours). The remainder (2 percent) are considered CFIs (prior 24 hours). The actual frequency of CFL is quite small due to the high reliability of PCS water delivery. The reliability of PCS water delivery in AP1000 has been improved over AP600 by addition of a third, parallel water supply line for PCS, controlled by a diverse valve (a MOV in contrast to an AOV in each of the other two lines).

An additional PCS-related failure mode is plugging of the drains near the floor of the annulus around the containment shell. Drain plugging can lead to accumulation of PCS water in the annulus, eventually reaching the baffle plate in the annulus and interrupting the air circulation. The availability of the PCS annulus drains will be confirmed every two years in accordance with the TSs. In the AP600 PRA, PCS failure was dominated by blockage of the PCS annulus drain lines, which was estimated to have a probability of 1E-04. This failure mechanism is not modeled in the AP1000 PRA, but at that same failure probability would have a corresponding containment failure frequency of about 2E-11/yr. Inclusion of this failure mode would substantially increase the frequency of CFLs in the AP1000. However, the frequency of CFL would remain less than 0.1 percent of the total containment failure frequency. Although not a key failure mode, for completeness of the PRA model, the staff believes that Westinghouse should include this failure mechanism within the AP1000 PRA. This is Open Item 19.1.3.2-2.

A subset of the containment isolation valves are important in limiting offsite releases during core melt accidents, and are therefore actuated by DAS in addition to PMS. These include the isolation valves in the containment purge supply and exhaust lines, and the normal containment sump line. The 45.7 cm (18 in.) containment purge supply and exhaust valves are assumed to be open 12 percent of the time during normal operation in the PRA, and are key release pathways in the event of failure to isolate.

AC power is available in the majority of core melt accidents. Core melt sequences involving loss of offsite power contribute less than 1 percent of the CDF in the baseline PRA. Thus, ac power would be available in the majority of internally initiated severe accidents. As a result, non-safety-related systems provided specifically to deal with severe accidents, such as containment sprays, can be supplied by normal ac power and still serve their function in the large majority of core melt events.

The non-safety containment spray system provides additional fission product removal. The AP1000 design includes a containment spray system for long term accident management, as discussed in Section 19.2.3.3.9 of this report. In the event of a severe accident involving failure or ineffective operation of PCS, containment sprays would reduce containment pressurization and enhance fission product removal. However, the spray system is not needed to meet the Commission's containment performance goals or quantitative health objectives. The

containment spray system is not modeled in the PRA, but would not significantly impact the estimated containment failure frequency since containment over-pressurization is not a dominant failure mode in the PRA. The greater impact would be on offsite risk, as discussed in Section 19.1.3.3.3 of this report.

The AP1000 design includes a capability to manually vent the containment as a long term accident management measure. Venting provides for a controlled release of fission products in lieu of a catastrophic, over-pressure failure of containment in events involving failure of PCS or unmitigated CCI. However, the vent is not needed in order to meet the Commission's containment performance goals or quantitative health objectives. Venting is not credited in the PRA, but would not significantly impact the estimated containment failure frequency, since containment over-pressurization is not a dominant failure mode in the PRA. Venting capabilities are discussed further in Section 19.2.3.3.8 of this report.

19.1.3.2.3.2 Phenomena/Challenges

Failure of RCS depressurization or ERVC is conservatively assumed to lead to containment failure. The majority of containment failures in the baseline PRA are a result of conservative treatment of severe accident phenomena associated with events in which the RCS is not successfully depressurized or the reactor cavity is not flooded. High pressure core melts (which could lead to RPV breach and DCH, thermally-induced SGTR, or a more benign creep-rupture failure of RCS piping) are assumed in the PRA to always result in thermally-induced SGTR. Events with failure of cavity flooding (which could lead to early containment failure by ex-vessel FCI, late containment failure by basemat melt-through, or no containment failure) are assumed in the PRA to always result in early containment failure. In contrast, deterministic analyses indicate that DCH and ex-vessel FCI will not result in early containment failure, and that CCI will not lead to containment over-pressure or basemat penetration until after 2 days. Accordingly, the containment failure frequency and dominant contributors could be substantially different than reported in the PRA if a more realistic, less conservative treatment of these issues were performed, but the risk would remain low as discussed below.

Eliminating credit for ERVC would increase CCFP, but the large release frequency goal would still be met. For the "final bounding state" core debris configuration that forms the centerpiece of the related ROAAM analysis (DOE/ID-10460), the staff's review of ERVC supports the Westinghouse contention that RPV integrity will be maintained. However, uncertainties in the likelihood of retaining a molten core in-vessel are large. If credit for successful ERVC is reduced or eliminated, containment failure frequency would increase proportionally since all RPV breaches are assumed to lead to early containment failure in the baseline PRA. Under the most limiting assumption of no credit for ERVC, the containment failure frequency would approach the core melt frequency given the pessimistic characterization of containment response to an RPV breach. Even then, however, the containment failure frequency would remain below the 1E-06/y goal because of the low estimated CDF. The actual containment failure frequency is expected to be much lower based on deterministic analyses that indicate that the containment is capable of sustaining ex-vessel loads.

Diffusion flames represented a unique containment challenge for AP600. In that design, diffusion flames could occur at the IRWST exit in events with successful operation of ADS stages 1-3 but failure of 4th stage ADS. If the flames remain anchored to the vent the resulting radiative and convective heat loads would not challenge the integrity of the containment shell. However, if the flames become attached to the containment shell the thermal loads could produce sufficient heating of the containment shell to result in localized creep rupture. The containment layout has several provisions to minimize the threat of diffusion flames that can challenge the integrity of the containment shell, specifically:

- the openings from the accumulator rooms and CVS compartments that can vent hydrogen to the CMT room are either located away from the containment wall and electrical penetration junction boxes or are covered by a secure hatch,

- IRWST vents near the containment wall are oriented to direct releases away from the containment shell, and

- IRWST vents near the containment wall are equipped with louvers that are normally closed, and designed to open at higher differential pressures than the IRWST pipe vents, and then reclose under their own weight when the differential pressure is reduced.

The latter feature was added to the AP1000 design to reduce the potential for diffusion flames at the containment shell. Operation of the IRWST louvered vents will preferentially direct the hydrogen releases to the IRWST pipe vents (located along the steam generator doghouse wall), where diffusion flames would not adversely impact the containment. Failure of the louvered vents to reclose is assumed to result in early containment failure due to diffusion flames, and accounts for about 5 percent of the containment failure frequency for AP1000.

Hydrogen deflagrations do not contribute to containment failure in the baseline PRA because of the following:

- the relatively limited amount of hydrogen that is produced in events that are successfully arrested in-vessel

- the availability of the hydrogen igniter system in the majority of core melt sequences

- the capability of the containment to withstand the AICC peak pressures associated with large deflagrations when igniters are unavailable.

With the exception of diffusion flames, deflagration-to-detonation transitions are the only combustion-related contributor to containment failure in the PRA, but the contribution is small as a result of the high availability of the igniter system. If the igniter system failure probability is increased to 0.1, the containment failure frequency increase is small (from 1.9E-08/yr to 2.3E-08/yr). If the system is assumed to be unavailable in all sequences, the containment failure frequency increases from 1.9E-08/yr to 6.3E-08/yr and the CCFP increases from 8.1 to 26 percent in the baseline PRA. This shows that the operation of igniters is important to

maintaining a low release frequency, but that system reliability can be reduced and not substantially impact risk.

19.1.3.2.3.3 Human Actions

A limited number of human actions in the Level 2 PRA are risk-important. The applicant identified the following operator actions in the Level 2 analysis as important to large release frequency based on sensitivity/importance analyses. These risk-important actions will be taken into account in control room design and the development of implementing procedures and training programs, as discussed in Chapter 18 of this report:

- diagnose and actuate the ADS after core damage to prevent RPV failure or temperature-induced SGTR (LPM-REC01 and AND-REC01)
- diagnose and actuate the ADS after core damage in SGTR events to terminate releases from containment (PDS6-MANADS)
- open recirculation valves to flood the reactor cavity (REN-MAN03)
- actuate the hydrogen igniter system (VLN-MAN01)

Guidance for certain human actions will be developed as part of accident management. Late RCS depressurization, hydrogen igniter system actuation, and reactor cavity flooding system actuation are credited in the Level 2 analysis and included within the Emergency Operating Procedures. Several other actions not modeled in the Level 2 analysis are also manual, including actuation of the containment spray system and the containment vent system, and energizing the igniter system from either the non-essential diesel generators or the non-Class 1E batteries. Detailed procedures for these latter actions will be developed by the COL applicant as part of COL Action Item 19.2.5-1 regarding accident management.

Operator actions to depressurize the RCS are credited for terminating SGTR. Operator actions to depressurize the RCS and maintain a water level covering the SG tubes are important in mitigating fission product releases from a SGTR accident. In approximately half of the Level 1 SGTR sequences, late RCS depressurization is successful. SGTR sequences with successful late depressurization are not considered to result in containment bypass in the PRA because of low RCS pressure and high water level in the faulted steam generator. Instead, these events are further evaluated in the CET, where they generally result in an intact containment and a benign source term. Eliminating credit for late depressurization during SGTR events increases the frequency of containment failure from 1.9E-08/yr to 2.9E-08/yr, and the CCFP from 8.1 to 12 percent. The assumption that the RCS will be depressurized and the SG level will be maintained above the break in such sequences will be further assured by inclusion of appropriate guidance on SGTR response within the severe accident management guidance to be developed by the COL applicant, as discussed in Section 19.2.5 of this report.

19.1.3.2.4 Frequency and Conditional Probability of Containment Failure

In assessing the probability of containment failure, the staff considered two alternative definitions of failure:

- Loss of containment structural or leak-tight integrity (i.e., the containment integrity definition). Containment failure frequency under this definition is the total frequency of all containment release modes/categories except those in which the containment remains intact, and is equivalent to the "large release frequency" used by the applicant.

- Releases which result in whole body doses of 0.25 Sv (25 rem) or greater at 0.80 km (0.5 miles) from the reactor (i.e., the dose definition). Containment failure frequency under this definition is the total frequency of events which result in a relatively large release at the site boundary. Rather than attempt to define a "large release", the staff used the EPRI criterion of 0.25 Sv (25 rem) at 0.80 km (0.5 miles) from the reactor as the dose definition of containment failure.

Based on the AP1000 source terms and offsite consequence analysis discussed in Section 19.1.3.3 of this report, the dose definition and containment integrity definition of containment failure are equivalent (i.e., yield approximately the same containment failure frequency) since the conditional probability of exceeding 0.25 SV (25 rem) at the boundary is close to unity for all release categories (except intact containment). Discussions below are based on the containment integrity definition of containment failure.

The containment failure frequency for internal events is 1.9E-08/yr in the baseline PRA. The corresponding CCFP is approximately 8.1 percent for the baseline PRA. The PRA analysis includes the following major features:

- stand-alone assessments of external reactor vessel cooling and in-vessel steam explosions using the ROAAM in lieu of including these issues in the CET

- explicit treatment of reactor cavity flooding, reactor vessel reflooding, and hydrogen combustion challenges within the CET

- simplifications to the CET that provide a bounding treatment of temperature-induced SGTR, DCH, and ex-vessel phenomena associated with reactor vessel melt-through

In the applicant’s analysis, most of the containment failure frequency is associated with early containment failure or containment bypass. This is an artifact of two major simplifying assumptions in the Level 2 PRA as follows:

- all accidents that proceed to core damage without successful depressurization are assumed to result in containment bypass due to creep rupture of SG tubes

- all accidents in which external reactor vessel cooling is unsuccessful are assumed to result in early containment failure as a result of ex-vessel phenomena.

These assumptions conservatively bound the significant uncertainties in both core melt progression at high RCS pressure, and containment response to ex-vessel sever accident phenomena.

Sensitivity studies reported in Chapter 43 of the AP1000 PRA provide insights into the importance of various additional assumptions on the containment failure frequency for the baseline PRA. These studies indicate that for reasonable variations in Level 2 input assumptions and CET split fractions, increases in the containment failure frequency are limited to about a factor of 3, and the containment failure frequency remains below 1E-07/yr. It is interesting to note that modest changes in the containment failure probability distribution used in the analysis would not noticeably impact the containment failure frequency or CCFP since the bulk of the containment failures in the existing analyses are driven by the frequency of events with failure of RCS depressurization or reactor cavity flooding, rather than the frequency at which containment pressure loads exceed the containment pressure capability.

The staff concludes that the AP1000 containment design satisfies the Commission's containment performance goal, and is therefore, acceptable. Specifically, the estimated containment failure frequency in the baseline PRA is well below the general plant performance guideline of 1E-06/yr for a large release of radioactive material, as proposed in the safety goal policy statement. The conditional containment failure probability is less than the CCFP goal of 0.1. The CCFP goal was proposed by the staff for evolutionary LWR designs in SECY-90-016, and approved by the Commission in its SRM of June 26, 1990. Although CCFP is exceeded in several sensitivity cases, these increases are modest and the corresponding containment failure frequencies remain well below 1E-06/yr. In view of the approximate nature of the containment performance goal, the recognition that PRA results contain considerable uncertainties, and the fact that a large fraction of the containment failures reflected in the calculated CCFP in the baseline PRA would actually involve late basemat melt-throughs (or no containment failures) rather than early releases to the atmosphere, the staff concludes that the AP1000 design satisfies the Commission's goals for both large release frequency and CCFP.

19.1.3.3 Results and Insights from the Level 3 PRA (Offsite Consequences)

In the updated AP1000 PRA, the end-states of the containment event trees were grouped into 6 individual release categories. For each release category, the timing, energy, isotopic content, and magnitude of release were established based on plant-specific thermal-hydraulic calculations using the MAAP code. The NRC-developed MACCS2 code, Version 1.12, was then used to calculate offsite consequences for each of the release categories, specifically, the effective dose equivalent (EDE) whole-body dose complementary cumulative distribution function (CCDF) at 0.5 miles from the reactor site, and the total person-rem exposure over a 50-mile radius from the plant. These analyses were supplemented by sensitivity analyses to assess the impact of uncertainties in key parameters. The staff finds this overall approach and the use of the above codes to be consistent with the present state of knowledge regarding severe accident modeling and, therefore, acceptable.

In the sections that follow, results and insights from the Level 3 portion of the PRA are presented. This includes the estimated probability of exceeding selected dose criteria, a

breakdown of the total risk in terms of important release classes, and finally, a summary of the risk-significant insights from the Level 3 PRA and supporting sensitivity analyses.

19.1.3.3.1 Risk Results for AP1000

Based on the updated PRA, the probability of exceeding a whole-body dose of 0.25 Sv (25 rem) at 0.8 km (0.5 mile) is about 1.9E-08/yr for internal events. This value is about a factor of 50 lower than the Commission's large release frequency goal of 1E-06/yr and, is therefore, acceptable. The design also meets the Public Safety Requirement goal established by EPRI in the ALWR URD (1E-06 probability of exceeding a dose of 25 rem at a distance of 0.5 miles). It should be noted, however, that the EPRI goal applies to both internal and external events, and that the results for AP1000 do not include the contribution from seismic and fire events.

Based on the Level 3 PRA, the estimated total risk to the public for AP1000 is quite small. The applicant's analysis indicates a total dose of about 0.01 person-rem/yr, based on the use of population and weather data developed by EPRI to bound 80 percent of the reactor sites in the United States (Ref: Revisions 5 and 6 of the URD), and site land use and crop data based on representative data from the Surry site (NUREG/CR-6613). Those site sectors that are ocean were treated as land in this assessment. Offsite risk is very low compared to the current generation of operating plants because of a combination of three factors: (1) a very low estimated CDF for AP1000, (2) a low conditional containment failure probability, and (3) a relatively benign source term associated with the frequency-dominant release category.

19.1.3.3.2 Leading Contributors to Risk from Level 3 PRA

The contribution to risk from each of the release categories is presented in Table 19.1-5 and Figure 19.1-3 of this report. The following can be noted:

- Based on Figure 19.1-3, the probability of exceeding 0.25 Sv (25 rem) at the site boundary (0.8 km (0.5 miles)) is essentially flat and close to unity for all release categories except intact containment (IC). Thus, the probability of exceeding 0.25 Sv (25 rem) is equivalent to the probability of containment failure, or about 1.9E-8/yr.

- Events in which the containment remains intact (IC) account for 92 percent of core damage events, but are negligible contributors to risk because of the insignificant consequences associated with normal containment leakage. Late containment failures also have a negligible contribution to risk due to the very low frequency of these events in the PRA.

- CFE contribute 38 percent of the containment failure frequency, and account for 52 percent of the risk. The large risk contribution is the result of the significant consequences (about 1E6 person-rem/event) associated with this release.

- Containment bypass events (BP) contribute 54 percent of the containment failure frequency, and account for 24 percent of the risk. This small contribution to risk is the result of the relatively small consequences (about 3E5 person-rem/event) for this release compared to other release categories.

- Releases from CI contribute 7 percent of the containment failure frequency, and account for only 21 percent of the total risk. This relatively large risk contribution is the result of the severe consequences (about 2E6 person-rem/event) associated with this release.

Selection of different representative sequences for the various release categories could alter the consequences by perhaps a factor of 3 and result in a re-ranking of the relative contribution to risk from each of the three risk-significant release categories. However, the major insights regarding the level of risk associated with the AP1000 design, and the risk-significant systems and features would not be impacted.

19.1.3.3.3 Important Insights from Level 3 PRA and Supporting Sensitivity Analyses

Insights from the Level 3 PRA are summarized below on the basis of the Level 3 PRA results and supporting sensitivity analyses.

- On the basis of the PRA, the probability of exceeding a whole-body dose of 0.25 SV (25 rem) at 0.8 km (0.5 mile) is about 1.9E-08/yr, and is equivalent to the containment failure frequency (CDF less the frequency of events with intact containment). The release frequency is a factor of 50 lower than the Commission's large release frequency goal and EPRI's Public Safety Requirement. It should be noted that the EPRI goal applies to both internal and external events, and that the results for AP1000 do not include the contribution from seismic and fire events. However, based on the estimated core damage and containment failure frequencies for externally-initiated events and events at shutdown, the large release frequency goals would also be met when these additional contributors are considered.

- The AP1000 risk profile is shaped by several major assumptions regarding containment failure modes and release characteristics including the following: (1) conservative assumptions regarding early containment failure from ex-vessel phenomena, and (2) optimistic assumptions that external reactor vessel cooling will always prevent reactor pressure vessel breach. Their impact on risk results is described below.

  In the baseline PRA, risk is dominated by events in which early containment failure is conservatively assumed to occur as a result of ex-vessel phenomena associated with RPV melt-through. However, deterministic calculations performed by the applicant indicate that the containment is likely to withstand these phenomena without loss of integrity. If early containment failure is avoided and reactor pressure vessel breach results instead in a more benign release (e.g., a containment failure in the intermediate time frame), overall risk for internal events would be reduced by less than a factor of 2.

In the baseline PRA, successful RCS depressurization and reactor cavity flooding (achieved in over 90 percent of the core damage events) are assumed to always prevent reactor vessel breach and associated ex-vessel phenomena. However, in view of the considerable uncertainties associated with core melt progression and lower head debris bed behavior, RPV failure cannot be ruled out for all possible core melt scenarios. If credit for ERVC is reduced or eliminated, containment failure frequency would increase proportionally since all RPV breaches are assumed to lead to early containment failure in the baseline PRA. Under the most limiting assumption that ERVC always fails and leads to early containment failure, the containment failure frequency would approach the core melt frequency and risk would increase by about a factor of 15 (from 0.013 to about 0.2 person-rem/yr). Even then, however, the containment failure/large release frequency would remain below the Commission's large release frequency goal of 1E-06/yr and the absolute level of risk would remain low. The actual containment failure frequency and risk is expected to be much lower based on deterministic analyses that indicate that the containment is capable of sustaining ex-vessel loads, as discussed above.

- The impact of the containment spray system on fission product releases was not credited in the PRA. Containment sprays could significantly reduce the estimated risk in the baseline PRA (by perhaps a factor of 2) since the sprays would be effective in reducing the source terms in the risk-dominant release categories (i.e., CFE and CI).

- Containment failures in the intermediate and late time frames are insignificant contributors to risk because of the small frequency associated with these release categories.

- Interfacing system LOCAs do not contribute to overall plant risk, primarily because of a piping upgrade that led to a low estimated frequency of these events.

19.1.4 Safety Insights from the Internal Events Risk Analysis for Shutdown Operation

Safety insights from the level 1 PRA are reported in Sections 19.1.4.1 through 19.1.4.5 while Section 19.1.4.6 reports safety insights from levels 2 and 3 of the PRA.

19.1.4.1 Level 1 Shutdown Internal Events PRA

The staff's review of the AP1000 shutdown PRA is based on the results reported in Chapter 54 of the AP1000 PRA. The AP600 shutdown PRA , specifically the analyses contained in the AP600 Shutdown PRA Attachment 54B and Attachment 54C, provide the basis for the AP1000 shutdown PRA. Attachment 54B is a re-quantification of the shutdown PRA results using revised success criteria for injection and recirculation during reduced inventory conditions with loss of the normal residual heat removal function. The revised success criteria state that (1) at least one of the four 4th stage ADS valves must open during reduced inventory conditions for successful gravity injection from the IRWST and (2) containment sump recirculation is needed for long term cooling following ADS operation during reduced inventory conditions. Attachment 54C documents the bases for these two success criteria.

The applicant estimated the mean AP1000 shutdown CDF from internal events to be 1.2E-07 per year (about 50 percent of the corresponding AP1000 CDF for power operation). This estimate assumes that no maintenance activities will be scheduled during reduced inventory conditions on the gravity injection lines from the IRWST, the 4th stage ADS valves and the containment sump recirculation trains, even though such outages are allowed by the AP1000 TSs. The AP1000 internal shutdown CDF estimate can increase to 2E-06/year if a COL applicant were to always choose minimal compliance with the AP1000 TS. These insights are discussed further in Section 19.1.4.5 of this report.

The reported CDF from internal events during shutdown operation (1.2E-07/year) covers two plant operational states:

- safe shutdown/cold shutdown with the RCS filled and intact, and
- mid-loop/vessel flange operations with the RCS vented and drained.

Mid-loop/vessel flange operations include: (1) draining to mid-loop, and (2) drained maintenance, and post-refueling maintenance.

Vacuum refill of the RCS from drained conditions (mid-loop) was mentioned in the PRA. However, no risk assessment was performed for this configuration. Vacuum refill of the RCS helps to reduce non-condensible gas pockets in the RCS, eliminating the need for dynamic venting of the RCS and the multiple reactor coolant pump start and stop operations that it requires.

The applicant stated that the shutdown risk due to vacuum refill operations is included in the calculation of shutdown risk during vented drained conditions. The staff is reviewing the applicant's response to RAI 720.99 to determine if the shutdown risk due to vacuum refill operations is included in the calculation of shutdown risk during vented drained conditions. The staff noted during their review of the applicant's response to RAI 720.99 that Investment Protection Short term Availability Controls do not include RNS and its support systems such as Component Cooling Water System, Service Water system, and ac power supplies during vacuum refill operations. Assuming an extended loss of RNS during vacuum refill operations, the staff questions using the RNS suction relief valve to relief RCS pressure should the operators not open the ADS valves. The operators may instead isolate the RNS suction relief valve to isolate RCS leakage. As discussed in Section 19.1.10.2 of this report, this vacuum refill issue is considered to be Open Item 19.1.10.2-1.

The reported internal AP1000 shutdown CDF estimate can be directly added to the full power estimate. The AP1000 shutdown PRA CDF estimate is based on the fraction of time per year that the plant is expected to be in safe/hot shutdown operation, cold shutdown operation, and refueling operations until the refueling cavity is flooded. Over ninety percent of AP1000 internal event shutdown risk occurs during drained operations with a vented RCS.

Operation in Mode 2 (startup) and Mode 3 (hot standby) were not quantitatively evaluated because the plant response to a loss of core cooling during these conditions is the same as

during power operation. Since the safety related systems (with the exception of the accumulators below 6.89 MPa (1000 psig)) and most actuation signals (both automatic and manual) are required to be available during Modes 2 and 3, the CDF contribution from events during these modes of plant operation is expected to be insignificant compared to at-power conditions (due to the smaller decay heat and the longer times for operator intervention).

Section 19.1.4.2 of this report presents the dominant accident cutsets and the major contributors to the shutdown CDF estimates. The AP1000 design features that reduce AP1000 shutdown risk compared to operating PWRs are described in Section 19.1.4.3 of this report. In Sections 19.1.4.4 and 19.1.4.5 of this report, insights drawn from the importance and sensitivity studies are discussed.

19.1.4.2 Dominant Accident Sequences Leading to Core Damage

As discussed above, over ninety percent of AP1000 shutdown risk occurs during vented, drained conditions. This plant configuration occurs during cold shutdown when the RCS boundary is open (via stages 1,2, and 3 of ADS), and the RCS is drained to reach mid-loop conditions so that nozzle dams can be installed in the hot and cold legs to perform steam generator maintenance. When the RCS boundary is open, emergency core cooling using PRHR is not viable; therefore, gravity injection from the IRWST and 4th stage ADS actuation must be initiated. Given that 4th stage ADS must open during reduced inventory conditions following an extended loss of RNS, containment sump recirculation would be initiated within 72 hours following accident initiation.

The top five dominant cutsets, contributing approximately 60 percent of the AP1000 risk from internal event at shutdown, are described below. Each additional dominant cutset contributes less than three percent of the shutdown CDF from internal events. The applicant did not report the dominant shutdown accident sequences in the PRA. The staff requests the applicant to report the dominant shutdown accident sequences in the AP1000 shutdown PRA . This documentation issue is considered to be an Open Item 19.1.10.2-3 (see Section 19.1.10.2 of this report).

Cutset #1, with a CDF of 2.2E-08/yr and a 17 percent contribution, is initiated by a loss of CCS/SWS with the RCS drained. Common cause failure of all ADS stage 4 valves results in failure of gravity injection, leading to core damage.

Cutset #2, with a CDF of 1.9E-08/yr and a 15 percent contribution, is initiated by a loss of CCS/SWS with the RCS drained. Actuation of ADS stage 4 squib valves is successful. Common cause failure of six out of six high pressure squib valves fails gravity injection through the DVI lines, resulting in core damage. Manual IRWST injection via the RNS pump suction lines was not credited for this cutset.

Cutset #3, with a CDF of 1.9E-08/yr and a 15 percent contribution, is initiated by a loss of CCS/SWS with the RCS drained. Actuation of ADS stage 4 squib valves is successful. Postulated common cause failure of two-out-of-two low pressure squib valves was assumed to lead to core damage. Common cause failure of the low pressure squib valves (118A and 118B)

does not by itself prevent sump recirculation and cause core damage. However, as described in the AP1000 shutdown PRA, the applicant stated that retaining this cutset provides a conservatism in the AP1000 shutdown model.

Cutset #4, with a CDF of 8.6E-08/yr and a 7 percent contribution, is initiated by a loss of CCS/SWS with the RCS drained. Postulated common cause failure of the IRWST recirculation sump strainers due to plugging fails recirculation and results in core damage.

Cutset #5, with a CDF of 8.6E-08/yr and a 7 percent contribution, is initiated by a loss of CCS/SWS with the RCS drained. Postulated common cause failure of the IRWST strainers due to plugging fails gravity injection and results in core damage.

19.1.4.3 Risk-Important Design Features

Listed below are key AP1000 design features that significantly reduce the shutdown CDF compared to operating PWR designs. These design features are described below by initiating event category.

19.1.4.3.1 Loss of RNS or its support systems (CCW/SWS) during safe shutdown/cold shutdown with the RCS intact

Unlike current operating PWRs, the AP1000 PRHR system provides an additional path of core cooling which is diverse from the RNS, it does not depend on ac power for operation and is safety related (passive). The PRHR does not depend on traditional support systems, such as component cooling water, to operate. In addition, the PRHR is capable of functioning at low pressures and temperatures as long as the RCS is intact and pressurizer level is above twenty percent. However, manual actuation is required before reactor coolant system pressure increases to cause the normal residual heat removal valve to open.

In current PWRs, operator action is required to restore all interruptions of RHR. In the AP1000 design, should manual actuation of PRHR fail, an alternate core cooling path is automatically established using the CMTs for injection, ADS for depressurization, gravity injection from the IRWST, and long term cooling using containment recirculation.

19.1.4.3.2 LOCAs during safe shutdown/cold shutdown with the RCS intact

In current PWRs, operator action is required to mitigate all losses of RCS inventory (e.g., operator action is required to actuate injection). In the AP1000 design, should a RCS drain path occur that is un-isolable, RCS injection and core cooling are automatically provided using the CMTs, ADS, gravity injection from the IRWST, and containment recirculation (for long-term cooling).

19.1.4.3.3 LOOP/SBO during safe shutdown/cold shutdown with the RCS intact

The AP1000 design provides much better protection against LOOP/SBO events compared to current PWRs since the operator is not required to perform many recovery actions. Following a

LOOP event, the RNS pumps trip but an automatic restart of the RNS pumps is provided after the diesel generators start and the electrical buses are sequenced. Should the diesel generators fail to start resulting in a loss of ac power and instrument air, PRHR provides core cooling automatically, since the PRHR air-operated valves are expected to fail open. Should manual actuation of PRHR fail, an alternate core cooling path is automatically established using the CMTs, ADS, gravity injection and containment recirculation (this requires only dc power).

19.1.4.3.4 Loss of RNS due to inadvertent overdraining of the RCS to achieve mid-loop conditions

Previous PWR shutdown PRAs have reported that overdraining of the RCS during mid-loop conditions is a dominant contributor to shutdown risk. The AP1000 design has many design features, not present in current PWRs, to prevent loss of the RNS pumps due to air entrainment and cavitation. These features are discussed further below.

To prevent overdraining, the RCS hot and cold legs are vertically offset. This design permits draining of the steam generators for nozzle dam insertion with a hot leg level much higher than traditional designs. The RCS must be drained to a level which is sufficient to provide a vent path from the pressurizer to the steam generators (nominally 80 percent level).

To lower the level in the hot leg where vortexing can occur, the AP1000 design uses a step nozzle connection between the RCS hot leg and the RHR suction line. To prevent cavitation, the piping elevations and routing and the RNS net positive suction head (NPSH) requirements allow the RNS pumps to be started and operated with saturated conditions in the RCS. Also, there is no need to throttle RNS flow when the RCS is in mid-loop conditions.

If adequate NPSH is lost, recovery of RNS is expected to be quicker compared to operating PWR designs. The RNS pump suction line is sloped continuously upward from the pump to the reactor coolant system hot leg with no local high points. This design eliminates potential problems in refilling the pump suction line if a RNS pump is stopped when cavitating due to excessive air entrainment. This self-venting suction line allows the RNS pumps to restart immediately once an adequate level in the hot leg is re-established.

To assist the operator, the AP1000 design contains hot leg level instrumentation with indication in the main control room. Each hot leg contains one hot leg level channel, totally independent of each other. One level tap is at the bottom of the hot leg, and the other tap is on the top of the hot leg as close to the steam generator as possible. The AP1000 design also provides cold calibrated wide range pressurizer level that can measure RCS level down to the bottom of the hot legs. This pressurizer level indication can be used as an alternative way of monitoring level and can be used to identify inconsistencies in the hot leg level instrumentation.

Should overdraining of the RCS occur, the operator is not required to manually actuate RCS injection as in current PWRs. The safety related PMS provides: automatic isolation of normal CVS letdown on low hot leg level (one-out-of two basis). On low hot leg level, two safety related AOVs close automatically to isolate letdown. On low, low hot leg level, the PMS provides automatic actuation of IRWST injection (two-out-of-two basis), and automatic

actuation of fourth-stage ADS to prevent surge line flooding (two-out-of-two basis). Long-term cooling is provided by containment recirculation.

19.1.4.3.5 LOOP/SBO during RCS open conditions

The AP1000 design provides much better protection against LOOP/SBO events compared to current PWRs since the operator is not required to perform many recovery actions. Following a loss of offsite power, the RNS pumps trip, but an automatic restart of the RNS pumps is provided after the diesel generators start and the electrical buses are sequenced. Should the diesel generators fail to start, gravity injection from the IRWST and concurrent 4th stage ADS actuation (to prevent surge line flooding) is automatically provided on low hot leg level. Gravity Injection and 4th stage ADS require only 1E dc power train to operate. Long-term cooling is provided by containment sump recirculation.

19.1.4.3.6 Loss of RNS (due to LOCAs or loss of RNS or its support systems) during RCS open conditions

The AP1000 design provides better protection against losses of RNS compared to current plants since the operator is not required to mitigate the event. Following a loss of RNS, gravity injection from the IRWST and concurrent 4th stage ADS actuation (to prevent surge line flooding) is automatically provided on low hot leg level from the PMS system. On low IRWST level, automatic containment recirculation provides long term core cooling.

19.1.4.3.7 Boron dilution events

The RES Surry Shutdown PRA (NUREG-6144 Appendix I) evaluated a potential boron dilution event during reactor startup following a LOOP event, with subsequent startup of the reactor coolant pumps. This scenario was estimated in NUREG-6144 Appendix I as having a CDF of 9E-6 per year. The scenario assumes an occurrence of a LOOP event during RCS de-boration during startup. When the charging pumps are restarted by the emergency diesel generators, the pumps drain primary grade water from the volume control tank into the RCS through the cold leg. With none of the RCPs running and virtually no natural circulation present (due to very low decay heat), the boron dilution continues. The primary grade water gradually makes its way to the reactor vessel and settles at the bottom of the vessel. If offsite power is recovered and one of the RCPs is restarted a few moments later, this will send a slug of primary grade water into the core, causing a power excursion.

The boron dilution scenario described above is prevented by design from occurring in the AP1000 plant. Once the 1E dc and un-interruptible power supply system (UPS) battery chargers receive low input voltage, the PMS provides a boron dilution signal that automatically re-aligns CVS pump suction to the boric acid tank. This same signal also closes the two safety-related demineralized water supply valves.

Alternatively, should a boron dilution event occur during startup as a result of failure of the PLS system and failure of operator control of PLS, the safety related, boron dilution protection signal would be generated upon any reactor trip signal, source range flux multiplication signal, low

input voltage to the Class 1E dc power system battery chargers, or a safety injection signal. As described above, this signal automatically re-aligns CVS pump suction to the boric acid tank. This same signal also closes the two safety-related demineralized water supply valves. Boron dilution events during safe shutdown using the DILUTE mode of operation were quantified separately from the shutdown PRA. The applicant concludes that these events are a negligible contributor to the AP1000 shutdown CDF estimate.

19.1.4.4 Insights from the Risk Importance Studies

As discussed in section 19.1.3.1.4, the results of Westinghouses's AP1000 importance analyses are used to identify: (1) SSCs and/or human actions whose reported reliability contribute most to achieving the low assessed shutdown CDF (risk achievement worth) and (2) SSCs and/or human actions which would contribute most to a reduction in shutdown CDF if their reliability was improved (risk reduction worth). Since the reported AP1000 internal shutdown CDF is very low and clearly meets the Commission Safety goals and the EPRI ALWR CDF requirements (<10E-5 per year), the staff is focusing on the results of the applicant's risk achievement worth analyses. The staff is using these results to identify (1) the SSCs for which it is particularly important to maintain the reliability/availability levels assumed in the PRA (e.g.., by testing and maintenance) to avoid significant increases in CDF and (2) the human actions which if failed would have the largest impact on the shutdown CDF. However, in their response to RAI 720.038 dated 03/28/03 and 4/12/03, the applicant did not provide any importance analyses (e.g., risk achievement and risk reduction worth) even though the staff requested importance analyses in the follow up to RAI 720.038. This documentation issue is considered Open Item 19.1.10.2-3 (see Section 19.1.10.2 of this report).

The applicant, in performing the level 1 PRA for internal events at shutdown operation, identified the following risk-important tasks, using the risk importance analyses results and threshold values. Shutdown initiating events were also examined by the applicant to identify risk-important tasks where human error substantially contributes to the frequency of these events. These risk-important tasks should be taken into account in the human-system interface design, procedure development, and staffing requirements development. The process for inclusion of these tasks is addressed in DCD Tier 2 Section 18.5.

- Operator fails to recognize the need for RCS depressurization (LPM-MAN05).
- Operator fails to open the IRWST squib valves for gravity injection(IWN-MAN-00).
- Operator fails to recognize the need to open RNS V023 for gravity injection (RHN-MAN-05).

The following operator actions substantially contribute to the frequency of losing shutdown cooling via RNS. Therefore, the applicant considered the following to be risk important tasks.

- Operator inadvertently opens RNS V024 during safe/cold shutdown or during drained conditions in the RCS and fails to terminate the event by re-closing the valve,

- Operator fails to recognize hot-leg-level instrument failure and subsequently fails to close the safety related air-operated CVS letdown isolation valves (CVS-V045 and CVS-V047), and

- Operator fails to detect automatic failure of the CVS letdown isolation valves to close, and subsequently fails to manually close the valves, when low hot leg level is reached during draining of the RCS to reach mid-loop conditions.

19.1.4.5 Insights from the Sensitivity Studies

The applicant performed sensitivity studies to gain insights about the impact of uncertainties on the assessed shutdown CDF. Specifically, these studies show how sensitive the shutdown CDF is to potential biases in numerical estimates assigned to initiating event frequencies, equipment unavailabilities, and human error probabilities. The staff expects the applicant to document the results of the sensitivity studies (including cutsets) in the AP1000 Shutdown PRA. As discussed in Section 19.1.10.2 of this report, this documentation issue is considered Open Item 19.1.10.2-4.

Similar to full power, a separate sensitivity study was performed to investigate the impact of shutdown operation without credit for non-safety-related "defense in depth" systems. This study is called the "focused PRA". The results of the "focused PRA" and additional sensitivity studies are described below.

19.1.4.5.1 Shutdown CDF assuming minimal compliance with AP1000 TS

In both the baseline and the "focused" shutdown PRA models, the applicant credits two gravity injection paths to be available (including a small maintenance unavailability). However, the AP1000 TS allow one-out-of-two IRWST injection trains to be out of service during the entire cold shutdown period. (Reduced inventory operation and mid-loop operation are a subset of cold shutdown operation). The applicant also credits a third gravity injection path through the RNS pump suction lines. This third path requires RNS valve V-23 to open. RNS valve V-23 is a safety-related containment isolation valve and can be actuated using the PMS. However, the function of RNS V-23 is to open to provide gravity injection which is not a safety-related function. Therefore, the capability for RNS-V023 to open is not required by AP1000 TS during cold shutdown operation. With respect to RCS venting, Westinghouse credits all ADS stage 4 valves to be available in the PRA. However, AP1000 TS only require two ADS stage 4 valves to be operable. With respect to containment sump recirculation, the AP1000 TS only require one-out-of-two containment sump recirculation trains to be available.

In the bases of AP1000 TS, there is no discussion that planned maintenance of these three systems should be avoided during cold shutdown. The frequency and duration of IRWST, ADS, and RNS maintenance performed by a future COL holder has considerable uncertainty. Therefore, the staff asked the applicant to perform a sensitivity study assuming minimal compliance with AP1000 TS. This sensitivity study provides an upper bound of the shutdown CDF assuming the COL holder chooses to always perform planned maintenance on one IRWST injection path and recirculation path, two ADS stage 4 valves, and RNS valve V-23

during cold shutdown. The shutdown CDF for this sensitivity study increases to 2.2E-06 per year (a factor of ten higher than the full power CDF). Since no cutsets were submitted in the RAI response for this sensitivity study, this documentation issue is considered part of Open Item 19.1.10.2-4 (see Section 19.1.10.2 of this report).

19.1.4.5.2 Impact of operator error

Based on results of shutdown PRAs for operating PWRs, the staff recognizes the high risk significance of operator error during shutdown conditions. In current plants, loss of shutdown cooling is often caused by operator error, and all interruptions of shutdown cooling require an operator response to prevent core damage.

As explained in Section 19.1.4.3 of this report, the AP1000 design provides an automatic mitigation capability for all the initiators quantitatively analyzed in the AP1000 shutdown PRA. Therefore, the AP1000 dependency on operator action is significantly reduced compared to operating PWRs. The applicant performed a sensitivity study setting (1) all human error probabilities associated with event mitigation to 0.5 and (2) the human errors probabilities associated with preventing overdraining in attempt to reach mid-loop conditions to 0.5. In this sensitivity study, the CDF increases to at least 5.5E-05 per year. This CDF estimate includes setting the failure probability of the following two events to be 0.5. The first event is failure of the operator to diagnose hot leg instrument failure and stop reactor coolant draining. The second event is failure of the operator to respond to the low hot leg alarm and isolate the drain, given failure of the automatic actuation signal to close the CVS drain valves. These results indicate the need for the wide range pressurizer level indication which can be used to identify hot leg level indication problems. These results also point to the risk importance of the hot leg level alarms and the operator recovery actions associated with these alarms.

19.1.4.5.3 Risk impact of non-safety-related systems

The applicant performed a sensitivity study by assuming the AP1000 plant was operating at shutdown and all of the non-safety-related “defense-in-depth” systems were not available. This sensitivity study is referred to as the “focused” PRA. As described in Section 19.1.3.1.5 of this report, this study provides additional insights about the risk importance of the “defense-in-depth” systems. These insights were used to select non-safety-related systems that require "regulatory treatment" according to the RTNSS process.

Core cooling during modes 4, 5, and 6 is provided by the non-safety-related RNS system and its non-safety-related support systems. In the “focused” PRA model, the frequency of losing non-safety-related RNS and its support systems (CCW and SWS) remain the same as in the baseline PRA. However, in the “focused PRA”, all credit for the non-safety-related systems being able to mitigate a shutdown initiator was removed. These non-safety-related systems include RNS, DAS, and the diesel generators.

Except for LOOP accidents, no other changes to the event trees were required since all event mitigation functions are safety related. In the LOOP event tree, credit was removed for the

non-safety-related power supply. In the system fault trees, the station blackout fault trees were used for the Class 1E and the UPS systems so that only safety-related power supplies were credited.

The "focused" PRA shutdown CDF was estimated to be 1.23E-06. Over 85 percent of the risk results from LOOP initiated accidents during drained conditions and during non-drained conditions. Some of the dominant cutsets have the basic event IWX-MV-GO1. In the early versions of the AP600 PRA, the basic event, IWX-MV-GO1, was used to model common cause failure of the 4 out of 4 IRWST injection motor operated valves (MOVs) to open. The later versions of the AP600 design and the AP1000 design changed the 4 MOVs to squib valves. In the AP1000 design, the low pressure squib valves (120 A/B) in the recirculation lines were also changed to high pressure squib valves. In preparing the AP600 cutset file for use as the starting point in creating the AP1000 shutdown model, the basic event IWX-MV-GO1 was changed to, IWX-EV-SA, common cause failure of IRWST squib valves. This basic event has a failure probability of 2.6E-05. As a follow up to RAI 720.038, the staff needs to understand why basic event IWX-MV-GO1 appears in the "Focused PRA" cutsets for the AP 1000 design. The staff also needs a list of basic events and their description for the AP1000 shutdown model. This documentation issue is Open Item 19.1.10.2-5 (see Section 19.1.10.2 of this report).

In the "focused" PRA, the applicant did credit gravity injection through RNS valve V-023. This valve is a safety-related containment isolation valve and can be actuated using the PMS. However, the function of RNS V-023 is to open to provide gravity injection which is not a safety-related function. Therefore, the capability for RNS-V023 to open is not required by the AP1000 TS during cold shutdown operation.

Since the RNS and its support systems (CCW and SWS, and ac power) significantly contribute to the likelihood of having a shutdown initiator, these systems are subject to availability controls during Mode 5 and Mode 6 when the RCS is open. During Mode 5 and Mode 6 when the RCS is open, PRHR is not credited for core cooling. The availability controls are discussed in DCD Tier 2 Section 16.3.

19.1.5 Safety Insights from the External Events Risk Analysis

Three external events were analyzed in the AP1000 PRA. These are seismic, internal fires and internal floods. In many PRAs performed to date, these external events have had combined CDFs that are the same magnitude as for internal events. It is not unusual to see the combined CDFs for these events in the 1E-04 per year range. The methods used in the AP1000 PRA to evaluate external events are acceptable to the NRC because they provide the insights necessary to determine if any design or procedural vulnerabilities exist for these external events and because the methods provide insights needed for design certification requirements, such as ITAACs.

In SECY 93-087 the NRC identified the need for a site-specific probabilistic safety analysis and analysis of external events. The applicant did not perform an analysis (PRA or bounding) of the capability of the AP1000 design to withstand external flooding, tornadoes, hurricanes, and other site-specific external events. The applicant did submit evaluations of seismic, fires, and internal

flood events. The NRC requires, where applicable to the site, that the COL applicant perform a site-specific PRA-based analysis of external flooding, hurricanes, or other external events pertinent to the site to search for site-specific vulnerabilities. This is COL Action Item 19.1.5-1. In addition, the PRA used to support the AP1000 design certification will be updated, as necessary, when site-specific and plant-specific (as-built) information become available. Differences between the as-built plant and the design used as the basis for the AP1000 PRA will be reviewed to determine whether there is significant impact on PRA results. Special emphasis will be placed on areas of the design that either were not part of the certified design or were not detailed in the certification. As stated previously this is COL Action Item 19.1.1-1.

19.1.5.1 PRA-Based Seismic Margin Analysis (SMA)

The AP1000 is designed to withstand a 0.3g safe shutdown earthquake (SSE). Since the analyses used in designing the capability of structures, systems and components (SSCs) to withstand the SSE have significant margin in them, it is expected that a plant built to withstand the SSE actually will be able to withstand a much larger earthquake. A PRA-based margins analysis systematically evaluates the capability of the designed plant to withstand earthquakes without resulting in core damage, but does not estimate the CDF from seismic events. The margins analysis is a method for estimating the "margin" above the SSE, i.e., how much larger than the SSE an earthquake must be before it compromises the safety of the plant.

The capability of a particular SSC to withstand beyond design bases earthquakes is measured by the value of the peak ground acceleration (g-level) at which there is a high confidence that the particular SSC will have a low probability of failure (HCLPF). The HCLPF capacity of a certain SSC corresponds to the earthquake level at which, with high confidence (95 percent), it is unlikely (probability less than 5E-02) that failure of the SSC will occur. A HCLPF value for the entire plant is determined by finding the lowest sequence HCLPF that leads to core damage. It is a measure of the capability of the plant to withstand beyond design basis earthquakes without resulting in core damage. The plant HCLPF value, which is assessed from the SSC HCLPF values, has units of acceleration. The NRC has indicated (SECY-93-087) that a plant designed to withstand a 0.3g SSE should have a plant HCLPF value at least 1.67 times the SSE (i.e., 0.5g). The PRA-based seismic margins analysis shows that the AP1000 design meets (and likely exceeds) the 0.5g HCLPF value expectation, and is therefore, acceptable.

No credit is taken in the risk-based SMA for the non-safety-related "defense-in-depth" systems. Since such systems are not seismic Category I, it is conservatively assumed that they become unavailable as a consequence of the seismic initiating event. Since the non-safety-related diesel generators are assumed to be unavailable and the failure with the lowest HCLPF value which would initiate an accident is the loss of offsite power (HCLPF of ceramic insulators is 0.09g), all accident sequences are treated in the SMA as SBO sequences. The potential for adverse interactions between assumed seismically-damaged non-safety-related SSCs and safety-related systems was investigated and accounted for in the analysis. The event and fault trees developed for the internal events PRA were modified to accommodate seismic events. In this way the random failures and human errors modeled in the internal events portion of the PRA are captured in the seismic analysis. The modified event and fault trees were merged and cutsets for all sequences that lead to core damage were generated. These cutsets are of two

kinds. One kind contains only seismic failures (i.e., without any random failures or human errors). The other kind contains random failures and/or human errors in addition to seismic failures. In "quantifying" these cutsets, the HCLPF values of the seismic events (instead of mean values of failure probabilities) were used, while the probabilities of random failures and human errors are the same as for the internal events PRA. Most of the HCLPF values for components and structures were obtained using the conservative deterministic failure margin (CDFM) approach or the Probabilistic Fragility Analysis approach or the Deterministic approach (NUREG/CR-4482, 1986 and EPRI NP-6041, 1988). For electrical equipment, for which documented test results are available, the HCLPF values were obtained by comparing required response spectra to test response spectra for similar types of equipment. Generic fragility data was used when insufficient information was available to determine the HCLPF value by using one of the above mentioned approaches. The min/max approach[2] was used for the sequence and plant level HCLPF calculations. The review of these calculations by the staff indicated that they were performed in accordance with the rules of the min/max approach and were, therefore, found to be acceptable. Additional background information about the seismic margins methodology and its implementation to the AP1000 can be found in DCD Tier 2 Appendix 19A.

19.1.5.1.1 Dominant Accident Sequences for Seismic Events

The staff used the results of the risk-informed SMA provided by the applicant to identify "dominant" accident sequences for seismic events. The word dominant appears in quotes to emphasize that the terminology in the context of a seismic margins study is not the same as in a conventional PRA. While these sequences (and associated cutsets) dominate the HCLPF values for the plant, the margins approach does not permit a determination that these are the dominant contributors to seismic risk in a probabilistic sense. If random failures and human errors are ignored (i.e., when cutsets containing seismic failures only are considered), the plant HCLPF was estimated to be at least 0.5g. Since, in general, the plant HCLPF can be lower when certain random failures (or human errors) occur simultaneously with the seismic failure of certain SSCs, cutsets containing both seismic and non-seismic failures were examined to find out if there were any cutsets which would lower the plant HCLPF below 0.5g. This examination has shown that for AP1000 there are no such cutsets. For earthquakes that generate higher accelerations than the plant HCLPF value, there is no longer the same high degree of confidence that core damage will not occur. However, because a cliff-effect is not likely at or near the plant HCLPF value, the plant will most likely have some seismic margin above the plant HCLPF value (i.e., capability to withstand seismic events that generate higher accelerations than the plant HCLPF value).

The following four "dominant" seismic core damage sequences were identified by the risk-informed seismic margins analysis. They have the lowest HCLPFs (cutsets with seismic only

[2] In the min/max approach if there is an "ORed" sequence where the failure of any individual SSC would cause core damage, we take the lowest individual SSC HCLPF as the sequence HCLPF. If there is an "ANDed" sequence where the failure of all SSCs would cause core damage, we take the highest individual SSC HCLPF as the sequence HCLPF.

failures are considered) or the lowest combination of HCLPF with random failure/human error (when cutsets with both seismic and non-seismic failures are considered).

Seismic sequence #1, with HCLPF value 0.5g, is a seismically-induced break of the reactor coolant system pressure boundary which results in loss of coolant beyond the capacity of the emergency core cooling system (ECCS) to provide makeup. This leads directly to core damage. Major contributors are fuel failure (HCLPF value 0.5g), steam generator failure (HCLP value 0.54g) and pressurizer failure (HCLPF value 0.55g). This scenario, which is also assumed to lead to a large fission product release due to loss of containment integrity, determines the HCLPF value for the entire plant with respect to both CDF and LRF (i.e., 0.5g).

Seismic sequence #2 with HCLPF value 0.50g, is a seismically-induced structural collapse of parts of the Nuclear Island. Major contributors are collapse of (1) Shield Building wall or roof (0.51g), (2) passive containment cooling water tank (0.51g), (3) an interior (concrete) structure of containment (0.50g), and (4) IRWST structure (0.50g).

Seismic sequence #3, with HCLPF value 0.54g, is a seismically-induced ATWS event and failure of the automatic depressurization system (ADS). The most important cutsets, associated with this sequence, involve failure of reactor internals or core assembly which causes failure of the control rods to insert (HCLPF value of 0.50g) combined with failure of the Class 1E 120V ac control power (HCLPF value of 0.55g) which causes failure of ADS. The most important contributors to the seismically-induced failure of the Class 1E 125V ac power are (1) failure of the 125V dcC distribution panels (0.55g), (2) failure of the 120V ac distribution panels (0.55g), (3) failure of the 125V dc switchboard (0.55g), (4) failure of the transfer switch (0.55g) and (5) failure of the cable tray (0.54g).

Seismic sequence #4, with HCLPF value 0.54g, is a seismically-induced ATWS event with failure of the core makeup tanks (CMTs). The most important cutset, associated with this sequence, involves failure of reactor internals or core assembly which causes failure of the control rods to insert (0.50g) combined with failure of the CMTs (0.54g).

It should be noted that the analysis did not identify any important sequence containing mixed cutsets (i.e., cutsets made up of both seismic and non-seismic failures) where the HCLPF of the seismic portion is less than the plant HCLPF value (i.e., less than 0.5g). This means that there are no random failures or human errors likely to occur in a seismically-initiated accident sequence that would lower the plant HCLPF below 0.5g. Furthermore, the analysis has shown that even the most important mixed cutsets are not risk significant (they combine a seismically-induced failure which is equal to or higher than the plant HCLPF value and a random failure or human error probability which is less than 1E-02).

The applicant also performed a bounding analysis, using simplified conservative assumptions, to identify paths by which the containment could be bypassed, fail to isolate or fail. This analysis assumes that the containment fails when the reactor vessel fails due to failure of the fuel (HCLPF value 0.5g). Thus, the plant HCLPF for large release is assumed to be the same as for core damage. Since the plant HCLPF is at least 0.5g, the plant HCLPF is in accordance with SECY-93-087, and is therefore, acceptable. The applicant performed a SMA for plant

operation at power only. The staff examined the event tree models used in the internal events PRA for shutdown operation, using the SMA models and results performed for power operation, and concluded that the plant HCLPF value is at least 0.5g even during plant shutdown.

19.1.5.1.2 Risk Important Features and Operator Actions for Seismic Events

The margins approach does not allow a determination of which plant features are most important to risk using importance analyses. The margins approach does allow one to determine which plant features are important to the plant level HCLPF and the redundancy/diversity available in achieving that HCLPF. In order to make this determination, the staff examined each sequence that leads to core damage on the seismic event trees. None of the sequences has a seismic-only HCLPF less than 0.5g. The sequences were examined to determine whether the lowering of the HCLPF value of a single SSC or the increasing of the demand failure rate of a single system would result in a plant HCLPF less than 0.5g.

Important insights about the capability of the AP1000 design to withstand earthquakes that were drawn from the examination of the SMA results (accident sequences and associated cutsets) are summarized below.

- The majority of the seismic sequences require multiple failures of SSCs whose HCLPF is greater than 0.5g in order to drive the plant to core damage. A check of the capacity of as-built SSCs to meet the HCLPFs assumed in the AP1000 PRA will be provided by a seismic walkdown and whose details are to be developed by the COL applicant. This is COL Action Item 19A.2.5-1 (see Section 19A of this report).

- There is a number of important safety-related structures whose seismically-induced failure would lead directly to core damage. These include the fuel in the reactor vessel (0.50g), the shield building wall or roof (0.51g), the passive containment cooling water tank (0.51g), an interior (concrete) structure of containment (0.50g), the IRWST structure (0.50g), the SGs (0.54g), and the pressurizer (0.55g). The seismic margins analysis assumes that these structures will all have HCLPF values in excess of 0.5g. If any of these structures were built with a HCLPF lower than 0.5g, the plant HCLPF would also be lower than 0.5g.

- There is a number of accident sequences which include cutsets with multiple seismic failures (i.e., two or more seismic failures are required for core damage to occur) but only one of these events has a HCLPF value which is considerably higher than the plant HCLPF value (the other events in the cutset have HCLPF values equal to or just above the plant HCLPF value). If the value of this event is reduced to about 0.5g or below, the plant HCLPF will not change but there will be additional sequences with HCLPF value in the neighborhood of the plant HCLPF. Sequences containing this kind of cutsets are as follows:

  – ATWS sequences which involve failure of the reactor internals or core assembly which causes failure of the control rods to insert (HCLPF value 0.50g) in combination with one other failure whose HCLPF is considerably higher than the

plant HCLPF value of 0.5g, such as IRWST injection check valves (0.85g) and squib valves (0.85g)

– Large LOCA sequences which involve failure of Class 1E electrical components, such as the cable trays (0.54g) and the 125V dc distribution panels (0.55g), in addition to the large LOCA initiating failure (0.76g).

- The analysis did not identify any important sequence containing mixed cutsets (i.e., cutsets made up of both seismic and non-seismic failures) where the HCLPF of the seismic portion is less than the plant HCLPF value (i.e., less than 0.5g). The only sequences containing seismic/random combinations (mixed cutsets) which would lower the plant HCLPF below 0.5g, when certain non-seismic (random) failures occur, are loss of offsite power sequences which are initiated by failure of the ceramic insulators (HCLPF value 0.09g). However, the probability of such random failures occurring is extremely remote (in the range of 1E-07 or less). This means that it is highly unlikely that random failures or human errors would occur in a seismically-initiated accident sequence and would lower the plant HCLPF below 0.5g.

- The same human error rates and random failure rates that were used in the AP1000 internal events analysis were also used in the SMA. The PRA-based SMA did not identify any human reliability insights that were not already identified in the internal events analyses. An examination of the top mixed cutsets shows that human errors are not significant contributors to non-seismic failure probabilities.

The following is a list of important design features which contribute to the capability of AP1000 to withstand earthquakes.

- There are no safety-related SSCs with HCLPF values less than 0.50g.

- The reliance on passive safety-related systems and dc power for accident mitigation, minimizes the impact of non-seismic (random or human) failures on the plant HCLPF value.

- "Defense-in-depth" with respect to seismically induced failures. The only single seismically-induced failures that would lead directly to core damage involve gross collapse of structures in the nuclear island, such as failure of the fuel in the reactor vessel (0.50g) or collapse of the auxiliary building roof (0.51g). Such failures control the plant level HCLPF.

- No safety-related equipment is located outside the nuclear island.

- No interaction between the nuclear island and any other structures has a detrimental impact on Nuclear Island structures. A potential indirect seismic interaction is possible between the turbine building (designed to the Uniform Building Code requirements) and the auxiliary building (a Seismic Category I structure). An access bay protects important safety-related I&C equipment as well as the main control room and the remote

shutdown panel, located in the north end of the auxiliary building, from potential debris produced by a postulated seismically-induced collapse of the adjacent turbine building.

- The fragility of valve rooms labeled 11206/11207 where the passive core cooling system valves are concentrated is an important factor in the AP1000 capability to withstand earthquakes. A check of the capacity of as-built SSCs to meet the HCLPFs assumed in the AP1000 PRA will be provided by a seismic walkdown and whose details are to be developed by the COL applicant. This is COL Action Item 19A.2-1 (see Section 19A of this report).

19.1.5.1.3 Insights from Uncertainty, Importance, and Sensitivity Analyses for Seismic Events

One of the reasons for performing an uncertainty analysis is to display the range of values within which the results of an analysis could reasonably be expected to fall. The use of a PRA-based seismic margins analysis inherently makes use of the breadth of information being considered. This is because HCLPF values can be thought of as the g-level at which one has 95 percent confidence that less than 5 percent of the time the equipment will fail (i.e., involve the tails of the curves). It was not found necessary to combine (use convolution) a seismic hazards analysis with equipment fragilities, since hazard curves have a large uncertainty which reduces their value in helping to make judgements about the seismic risk. From seismic PRA analyses, it is clear that uncertainties in the hazard curves would dominate the uncertainties in equipment and structure fragilities. For the AP1000 PRA-based SMA, no uncertainty analysis was performed because uncertainty is directly reflected in the margins method. Also, since the margins method does not quantify risk (e.g., in terms of core damage frequency), importance analyses were not performed. Westinghouse did, however, perform sensitivity analyses to evaluate the effects of changes in certain assumptions used in the SMA. The most important insights from the sensitivity studies are listed below.

- A decrease in the "generic" HCLPF values assumed in the SMA for several SSCs, such as ADS MOVs (0.81g) and pipe supports (0.81g), will not impact the plant HCLPF as assessed in the SMA. However, decreasing such "generic" HCLPF values will impact the results. This is not surprising since they affect a large numbers of components. There are always one or more sequences whose HCLPF is controlled by one or more of the components with "generic" HCLPFs, so it is necessary to assure that these HCLPFs are not inappropriately low in the as-built plant (this will be confirmed by the COL applicant during a seismic walkdown of the as-built plant). This process is part of COL Action Item 19.1.5-2.

- Increasing the fuel HCLPF value to any value above 0.5g, the plant HCLPF will still be 0.5g but will be dominated by gross structural collapse of interior containment (0.5g) and the IRWST (0.5g).

- Increasing the HCLPF values of fuel, interior containment and the IRWST from 0.5g to any value above 0.51g, the plant HCLPF will increase to 0.51g and will be dominated by the gross structural collapse of containment cooling tank (0.51g), auxiliary building (0.51g) and shield building roof (0.51g).

- Increasing the HCLPF values of fuel, interior containment, IRWST, containment cooling tank, auxiliary building, and shield building roof to values above 0.54g, the plant HCLPF would increase to 0.54g and will be dominated by cable tray failure (0.54g) and failure of CMT tanks (0.54g).

- The plant HCLPF or the SMA insights about the AP1000 design are not impacted by potential, but unlikely, seismic interactions between the turbine building and the auxiliary building.

- Since no credit is taken in the SMA for the non-safety-related "defense-in-depth" systems to mitigate seismic events and the SMA has shown that the plant HCLPF is at least two-thirds the ground motion acceleration of the design-basis SSE (SECY-93-087), the results of the SMA do not impact the probabilistic criteria (see Section 19.1.7 of this report) used to select non-safety-related systems for "regulatory treatment" according to the RTNSS process.

19.1.5.2 Internal Fires Risk Analysis

The applicant performed a fire risk analysis, for both at-power and shutdown conditions, to search for potential design vulnerabilities and identify important safety insights about the AP1000 design needed to support certification requirements, such as ITAACs. The analysis uses: 1) available plant-specific design information, including the locations of major equipment and cables, of rated fire barriers, and automatic detection and suppression equipment, 2) industry fire safety data, including the frequency of fires in different compartments, the reliability of automatic and manual suppression, the reliability of fire barriers, and 3) the plant internal events PRA model (without credit for the "defense-in-depth" non-safety-related systems) to assess the CDF associated with internal fire. The approach used is a modified Fire Induced Vulnerability Evaluation (FIVE) methodology (EPRI TR-100370, 1992) and is generally consistent with fire risk assessment methods used to evaluate conventional plants (e.g., NUREG/CR-2300, 1983 and NUREG/CR-4840, 1989).

In general, the fire PRA is performed largely as a screening level analysis and employs a number of conservative assumptions. Somewhat less conservative assumptions are employed for two fire areas[3]: the containment and the main control room (MCR). Key features of the fire PRA are as follows.

- For most fire areas, the analysis assumes that, given a fire in the area, all of the equipment in the area is lost. Thus, the analysis does not take credit for the possibility of fire self-extinguishment or suppression before the loss of equipment within the affected area. This treatment is likely to be quite conservative for most plant areas. However, it may only be slightly conservative for plant areas housing sensitive electronic

[3]The AP1000 fire areas are defined in the DCD. They are separated from each other by fire barriers with ratings of 2 hours or more. A fire area can be separated into “fire zones” which are defined for analytical convenience and need not be separated by barriers.

components, since these are more susceptible to the effects of heat, humidity, and smoke.

- For the containment and the MCR, the analysis is more detailed. Based on the separation of equipment within each area, fire scenarios involving subsets of equipment are identified and analyzed. In the case of the MCR, the analysis accounts for the possibility that MCR fires are extinguished before they cause equipment damage or MCR evacuation.

- The analysis allows for the possibility of fire growth into a second fire area when the barrier between two areas contains any type of penetration. The likelihood of automatic suppression system failure (if such a system is installed) and the likelihood of barrier failure are used in determining the likelihood of fire growth. If growth occurs, it is assumed that all equipment in both areas is lost. The analysis considers only the possibility of fire growth to one adjacent fire area (i.e., it is assumed that the likelihood of growth to multiple areas is negligible).

- The analysis explicitly treats the possibility of fire-induced spurious actuations of ADS valves. Fire-induced hot shorts in relevant safety- and DAS-related cables and cabinets are treated as leading to medium LOCA (MLOCA) or large LOCA (LLOCA) scenarios when the reactor is at power. Fire-induced MLOCA scenarios are also treated when the reactor is shutdown (but not in mid-loop). Credit is not taken for the potential use of fiber optics cabling and digitally encoded signals in portions of the control system.

- The analysis employs the "focused" PRA model to determine the conditional core damage probability, given the loss of a set of equipment due to fire. Such model does not take credit for the performance of the non-safety-related "defense-in-depth" systems.

- The analysis treats the possibility of operator recovery actions. These actions involve the manual actuation of equipment from the MCR or the remote shutdown workstation (RSW) as backup to automatic actuation (actions by local equipment operators are not credited). Consequently, the human error probabilities used in the recovery analysis are not modified to reflect fire-specific impacts on operator performance. The analysis relies on two important assumptions. First, a large fire in the MCR or RSW will not affect the automatic actuation of equipment. Second, ex-MCR or RSW activities, e.g., coordination of fire-fighting activities and plant response, will not place any significant additional burden on the MCR operators.

- The hot/cold shutdown (HCSD) and mid-loop (ML) analyses are performed in a manner very similar to that used for the at-power analysis. The primary difference is in the containment fire frequencies (transient fires not considered in the at-power analysis are included in the HCSD and ML analyses).

The AP1000 fire PRA reflects the generally strong separation between the four safety-related power and control divisions. The only plant fire areas containing all four divisions are the MCR,

the RSW area, and the containment. The MCR is continuously manned and the RSW area is not normally enabled. Additionally, because of the AP1000's digital I&C design, fires within these areas are not expected to inhibit the automatic actuation of safe shutdown equipment. Within the containment, redundant divisions are generally separated by continuous structural or fire barriers without penetrations and by labyrinth passageways (in a few cases, the divisions are separated by large open spaces without intervening combustibles). Because of the general divisional separation and the I&C design, a single fire in the plant is not expected to damage enough equipment to cause core damage; additional (non-fire caused) failures are required for this to occur.

19.1.5.2.1 Dominant Accident Sequences Leading to Core Damage for Internal Fires

The applicant quantified the CDF associated with internal fires, for both at power operation and during shutdown, by using applicable event and fault tree models from the internal events PRA. The fire-induced CDF was assessed to be about 5.6E-08 per year for fires occurring during power operation and about 8.5E-08 per year for fires occurring during shutdown. The applicant considers the above mentioned CDF estimates to be conservative (based on several, previously mentioned, conservative assumptions made in the analysis). The staff believes that such a conclusion is not possible without a detailed PRA. The staff's review did not concentrate on bottom-line numbers but rather on important modeling assumptions and the relative insights that the internal fires analysis provides about the design. Based on this information, the staff was able to conclude that the AP1000 design is capable of withstanding severe accident challenges from internal fires in a manner superior to most, if not all, operating plant designs. The internal fires PRA has provided useful safety insights for inclusion in ITAAC, COL Action Items, and RAP. Since detailed PRA-based internal fires analyses at some operating plants have shown that fire-induced sequences can be leading contributors to CDF, the COL applicant should provide an updated internal fires PRA that takes into account design details (e.g., cable routing, door and equipment locations and fire detection and suppression system locations) to search for internal fire vulnerabilities in the detailed design. This is COL Action Item 19.1.5-3.

19.1.5.2.1.1 Operation at power

The top ten fire areas, contributing over 90 percent of the total CDF from internal fires at power operation, and their dominant fire scenarios are listed below.

Fire area #1, with a CDF of about 1.3E-08/yr and about 23.5 percent contribution to the total CDF from internal fires at power operation, is the north-northeast (NNE) quadrant of the maintenance floor inside the containment (fire area 1100 AF 11300B). A fire in this area is assumed to fail or degrade the actuation of in-containment safety-related equipment supported by cabling passing through the area (fire zone). Important equipment assumed failed are the Class 1E power and control divisions A and C, one CMT, one PRHR isolation valve and one CCS flow path to the containment. The dominant fire scenarios associated with a fire in fire area 1100 AF 11300B are:

- Fire suppression is successful and the fire does not propagate. However, "hot shorts" occur that cause the spurious opening of a stage 1, 2 and 3 line leading to a medium

LOCA. The fire induced medium LOCA is not mitigated by the remaining safety systems, leading to core damage. This scenario contributes about 8.5E-09/yr to the fire CDF.

- Fire suppression fails and the fire propagates causing the failure of DAS. In addition, "hot shorts" occur that cause the spurious opening of a stage 1, 2 and 3 line leading to a medium LOCA. The fire induced medium LOCA is not mitigated by the remaining safety systems, leading to core damage. This scenario contributes about 3.1E-09/yr to the fire CDF.

- Fire suppression is successful, the fire does not propagate and there are no "hot shorts" that could cause the spurious opening of ADS valves. However, the fire induced transient is not mitigated by the remaining safety systems, leading to core damage. This scenario contributes about 8.3E-10/yr to the fire CDF.

- Fire suppression fails but fire does not propagate. However, "hot shorts" occur that cause the spurious opening of a stage 1, 2 and 3 line leading to a medium LOCA. The fire induced medium LOCA is not mitigated by the remaining safety systems, leading to core damage. This scenario contributes about 7.2E-10/yr to the fire CDF.

Fire area #2, with a CDF of about 9.2E-09/yr and about 16.5 percent contribution, is the operating deck inside the containment (fire area 1100 AF 11500). A fire in this area is assumed to fail or degrade the actuation of in-containment safety-related equipment supported by cabling passing through the area (fire zone). Important equipment assumed failed are the Class 1E power and control divisions B and D, the main feedwater and the startup feedwater. The dominant fire scenario associated with a fire in this area is due to "hot shorts" that cause the spurious opening of a stage 1, 2 and 3 line leading to a medium LOCA. The fire induced medium LOCA is not mitigated by the remaining safety systems, leading to core damage. This scenario contributes about 9.0E-09/yr to the fire CDF.

Fire area #3, with a CDF of about 6.7E-09/yr and about 12 percent contribution, includes the auxiliary building corridors at Elevation 100 feet and 117 feet 6 inches (fire area 1200 AF 03). A fire in this area is assumed to fail equipment located in the area and cause the failure or degradation of equipment located elsewhere which receive power or actuation signals through cables passing through the area. Important equipment assumed failed are I&C cables for divisions B and D (since no cables dedicated to any ADS valves pass through this area, the operation of the ADS valves is not impacted), DAS cables for manual actuation of ADS stage 4 valves and division B and D cables to the reactor trip switchgear. The dominant fire scenarios associated with a fire in fire area 1200 AF 03 are:

- a fire-induced transient not mitigated by the remaining safety systems, leading to core damage (contributes about 4.4E-09/yr to the fire CDF), and

- a fire-induced spurious actuation of one ADS stage 4 valve (due to damage in a DAS cable) which is not mitigated by the remaining safety systems, leading to core damage (contributes about 2.2E-09/yr to the fire CDF).

Fire area #4, with a CDF of about 5.1E-09/yr and about 9 percent contribution, is the turbine building floor (fire area 2000 AF 01). A fire in this area is assumed to fail one or both trains of MFW, SFW CCW and CAS (depending on whether fire suppression is available and successful in the zones, within the fire area, where such equipment is located). The dominant fire scenario associated with a fire in this area is a loss of MFW transient with SFW CCW and CAS unavailable. The fire-induced loss of MFW transient is not mitigated by the remaining safety systems, leading to core damage. This scenario contributes about 5.1E-09/yr to the fire CDF.

Fire area #5, with a CDF of about 4.3E-09/yr and about 8 percent contribution, is the battery and battery charger room 2 inside the annex building (fire area 4031 AF 02). A fire in this area is assumed to fail the non-Class 1E ac and dc power and DAS. The dominant fire scenario associated with a fire in this area is fire-induced transient which is not mitigated by the remaining safety systems, leading to core damage. This scenario contributes about 4.3E-09/yr to the fire CDF.

Fire area #6, with a CDF of about 4.0E-09/yr and about 7 percent contribution, is the battery and battery charger room 1 inside the annex building (fire area 4031 AF 01). A fire in this area is assumed to fail the non-Class 1E ac and dc power and DAS. The dominant fire scenario associated with a fire in this area is fire-induced transient which is not mitigated by the remaining safety systems, leading to core damage. This scenario contributes about 3.9E-09/yr to the fire CDF.

Fire area #7, with a CDF of about 2.3E-09/yr and about 4 percent contribution, is the auxiliary building non-Class 1E electrical compartment at Elevation 100 feet (fire area 1230 AF 02). A fire in this area is assumed to fail the non-Class 1E ac and dc power, DAS and division B and D cables to the reactor trip switchgear. The dominant fire scenario associated with a fire in this area is fire-induced transient which is not mitigated by the remaining safety systems, leading to core damage. This scenario contributes about 2.1E-09/yr to the fire CDF.

Fire area #8, with a CDF of about 2.1E-09/yr and about 3.7 percent contribution, is the auxiliary building division B battery, dc equipment, and I&C room (fire area 1201 AF 02). A fire in this area is assumed to fail division B power and control. The dominant fire scenarios associated with a fire in fire area 1200 AF 03 are:

- a fire-induced spurious actuation of one ADS stage 4 valve (a large LOCA) which is not mitigated, leading to core damage (contributes about 1.0E-09/yr to the fire CDF), and

- a fire-induced spurious opening of a stage 1, 2 and 3 line leading to medium LOCA which is not mitigated, leading to core damage (contributes about 6.5E-10/yr to the fire CDF).

Fire area #9, with a CDF of about 2.0E-09/yr and about 3.6 percent contribution, is the yard building (fire area 0000 AF 00). A fire in this area is assumed to cause a LOOP without recovery event which is not mitigated by the remaining safety systems, leading to core damage.

Fire area #10, with a CDF of about 1.8E-09/yr and about 3.2 percent contribution, is the auxiliary building division C battery, dc equipment, and I&C, and I&C penetration room (fire area 1202 AF 03). A fire in this area is assumed to fail division C power and control. The dominant fire scenarios associated with a fire in fire area 1200 AF 03 are:

- a fire-induced spurious actuation of one ADS stage 4 valve (a large LOCA) which is not mitigated, leading to core damage (contributes about 1.2E-09/yr to the fire CDF), and

- a fire-induced spurious opening of a stage 1, 2 and 3 line leading to medium LOCA which is not mitigated, leading to core damage (contributes about 3.8E-10/yr to the fire CDF).

The AP1000 PRA predicts the at-power fire risk to be dominated by fire-induced spurious actuation of ADS valves leading to a LOCA event (about 54 percent contribution). Spurious opening of one ADS stage 1, 2 and 3 line (a medium LOCA) contributes about 44 percent while spurious opening of a stage 4 squib valve (a large LOCA) contributes about 10 percent. Most of the remaining CDF (46 percent) is attributed two transients (about 30 percent), loss of main feedwater (about 12 percent) and LOOP (about 4 percent). With respect to fire areas, the AP1000 PRA predicts that about 41 percent of the fire-induced CDF during power operation is associated with fires inside the containment, about 29 percent with fires in the electrical areas of the auxiliary building, about 15 percent with fires in the annex building (mostly the battery rooms), about 11 percent with fires in the turbine building, and the remaining 4 percent with yard fires. The PRA predicts an almost insignificant contribution to CDF from fires in the MCR. Due to differences in the level of conservatism employed in the analysis for the various areas of the plant (e.g., the analysis for postulated fires in the MCR is more detailed and less conservative than the analysis for the auxiliary building), a comparison of contributions to risk from the various plant areas will not yield useful results. The staff, however, finds that this analysis is adequate for the purpose of identifying potential vulnerabilities and for gaining insights about the design which can be used to support design certification requirements, such as ITAACs.

An examination of the dominant cutsets shows that none of the identified internal fire events leads to core damage unless additional random (i.e., non-fire related) failures occur. However, some dominant cutsets involve a single non-fire basic event. Although most of the random failures involve CCF of electrical, mechanical, or I&C equipment and software, a number of these failures involve single component failures. Thus, the AP1000 fire PRA predicts that there may be scenarios (although of low probability) where a single fire has the capability of bringing the plant within one failure of core damage. This conclusion, however, may be biased because of the conservatism used in the analysis. For example, a further examination of cutsets involving a single random CCF which is a single component failure, shows that they would not lead to core damage (i.e., they would not be cutsets) had non-safety-related "defense-in-depth" systems, such as DAS and RNS, been credited in the fire risk analysis. Availability control of such "defense-in-depth" systems, according to the RTNSS process, averts potential situations where a single fire has the capability of bringing the plant within one failure of core damage.

19.1.5.2.1.2 Low Power and Shutdown Operation

The applicant's fire analysis for shutdown operation was submitted on March 28, 2003. A high level staff review has shown that the AP1000 fire risk analysis is significantly different than the AP600 analysis (e.g., differences in the grouping of fire areas, combustible loadings and fire propagation). For this reason there was not adequate time for the staff to evaluate the fire analysis for shutdown operation and draw conclusions to be included in this report. The adequacy of the AP1000 shutdown fire risk analysis is still being reviewed by the staff and is considered an open item in the AP1000 DSER (see Section 19.1.10.2 of this report).

19.1.5.2.2 Risk Important Design Features and Operator Actions for Internal Fires

The following is a list of important design features which contribute to the reduced fire risk associated with the AP1000 design as compared to operating reactors.

- Separation of divisions. In most areas of the plant, the 4 safety-related electrical divisions (Divisions A through D) are in separate fire areas, i.e., they are separated barriers of at least 2-hour fire rating or equivalent. In particular, the major rooms housing divisional cabling and equipment (the battery rooms, dc equipment rooms, I&C rooms, and penetration rooms) are separated by 3-hour rated fire walls without openings. There are no doors, dampers, or seals in these walls. The rooms are served by separate ventilation subsystems. In order for a fire to propagate from one divisional room to another, it must move past a 3-hour barrier (e.g., a door) into a common corridor and enter the other room through another 3-hour barrier (e.g., another door).

- Separation of automatic actuation systems from MCR and RSW. The MCR and the RSW are the only two plant areas where all 4 divisions can be affected by a single fire with significant likelihood. For fires in these areas, the plant is designed to have an independent, automatic means to reach safe shutdown. (In fact, operator actions from the MCR and RSW are not required according to the design; these actions are treated as backups to the automatic response.)

- Separation of safety divisions within containment. The containment is the third fire area containing all 4 divisions. Redundant divisions are generally separated by "continuous structural or fire barriers without penetrations and by labyrinth passageways." In a few situations, the divisions are separated by large open spaces without intervening combustibles.

- There is no cable spreading room in the AP1000 design.

- No safety-related equipment is located in the turbine building. There is a 3-hour fire barrier wall between the turbine building and the safety-related areas of the nuclear island.

- The vast majority of cables in the MCR are low voltage; this is expected to reduce the likelihood of self-ignited fires.

- If control room evacuation is necessary, the RSW provides complete redundancy in terms of control for all safe shutdown functions.

- Passive safety-related systems do not require cooling water or ac power. Therefore, the passive safety-related systems of the AP1000 are less susceptible to fire-induced failures than the currently operating plants' active safe shutdown equipment.

- The fire PRA identified only two fire-specific operator actions: (1) operator action to switch off the electrical power for each division in case of fire to avoid spurious actuation of valves, and (2) operator action to manually actuate a valve to allow fire water to reach the automatic fire suppression system in containment maintenance floor (fire area 1100 AF 11300B). The AP1000 design is significantly less dependent on human actions to mitigate internal fires than operating reactors. The COL applicant will develop procedures for implementing these fire-specific operator actions. This is a COL Action Item in the DSER (see Section 19.1.10.1 of this report).

It should be noted that the use of digital I&C is expected to increase the likelihood of fire-induced loss of function in the I&C equipment (cabinet) rooms, due to the sensitivity of the I&C electronic components to heat, smoke, and humidity (from suppression activities). The AP1000 fire PRA accounts for this sensitivity by conservatively assuming the loss of all equipment in a fire area if a fire occurs. However, the degree of conservatism of this assumption is believed to be relatively small for the I&C rooms (as compared to other areas of the plant which contain more rugged components).

19.1.5.2.3 Insights from Uncertainty, Importance, and Sensitivity Analyses for Internal Fires

No uncertainty and importance analyses were performed by the applicant for internal fires. Due to the conservatism in the approach taken in performing the AP1000 internal fire PRA, The applicant judged that uncertainty and importance analyses would result in biased insights. Since no credit was taken for the non-safety-related "defense-in-depth" systems, the results and insights of the fire risk analysis can be used directly in the criteria for selecting non-safety-related systems for "regulatory treatment" according to the RTNSS process. The fire-induced CDF estimate (for both at power and during shutdown operation) is based on conservative assumptions and still is about an order of magnitude smaller than the CDF estimate for internal events obtained with the "focused" PRA model (i.e., when no credit is taken for the non-safety-related "defense-in-depth" systems). This means that the fire PRA results do not have a significant impact on the probabilistic criteria (reported in Section 19.1.7 of this report) used to select non-safety-related systems for "regulatory treatment" according to the RTNSS process. The only exception is the manual ESF actuation by DAS which was credited in the fire PRA (ADS stage 4 line opening by DAS) to meet the success criteria for depressurization during spurious opening of ADS paths leading to a LOCA event. TSs will be in place to ensure the availability of manual ESF actuation by DAS.

The applicant performed a series of sensitivity studies to gain insights about the impact of uncertainties on fire risk. Important insights from these studies are summarized below:

- Increasing the "hot short probability" assumed in the fire risk analysis by a factor of two, would increase the plant fire CDF for power operation about 3 times (from 5.6E-08/yr to about 1.6E-07/yr). This result shows that the fire risk is sensitive to "hot short" failure assumptions. The AP1000 design recognizes this sensitivity and has incorporated features to minimize the consequences of hot shorts. Spurious actuation of ADS valves is prevented by the use of a valve controller circuit which requires multiple hot shorts for actuation, physical separation of potential hot short locations (e.g., routing of ADS cables in low voltage cable trays and the use of arm and fire signals from separate PMS cabinets), and provisions for operator action to remove power from the fire zone.

- Increasing the failure probability of the two fire-specific human actions (discussed in Section 19.1.5.2.2 above) to 1 (i.e., no credit for such operator actions is taken), would increase the plant fire CDF for power operation almost 5 times (from 5.6E-08/yr to about 2.6E-07/yr). This bounding analysis result shows some sensitivity of the fire CDF to reasonable increases of the fire-specific operator action failure probabilities but not large enough, by itself, to impact PRA conclusions about the design.

- Increasing the failure probability of manual ADS actuation by DAS by an order of magnitude, would increase the plant fire CDF for power operation about 4 times (from 5.6E-08/yr to about 2.2E-07/yr). This result indicates some sensitivity of the fire CDF to reasonable increases of manual DAS actuation failure probability. However, this sensitivity is not large enough, by itself, to impact PRA conclusions about the design.

19.1.5.3 Internal Flooding Risk Analysis

Due to the lack of detailed design information needed to identify exactly the potential flood sources and flood levels, such as pipe routing, drain capacities and locations, and other flood mitigating devices like sloped floors or curbs, the applicant chose not to perform a detailed PRA to assess the risk from internal flooding associated with the AP1000 design. Instead, the applicant performed an internal flooding PRA which is commensurate with the level of detail available and making conservative assumptions, where detailed information was not available, to bound the flooding analysis. The staff finds that this analysis is adequate for the purpose of identifying potential vulnerabilities and for gaining insights about the design which can be used to support design certification requirements, such as ITAACs.

The performance of the internal flooding PRA included four stages. During the first stage, information required to perform the flooding analysis was collected, such as identifying areas that contain potential flooding sources and/or equipment required for plant operation and safe shutdown of the plant. During the second stage, an initial screening of the areas identified during the first stage was accomplished, using conservative assumptions (e.g., total immersion and failure of equipment in affected areas) and taking into account the potential for propagation to other areas, to identify areas where flooding could cause a reactor trip or affect safe shutdown. During the third phase, a detailed screening of the areas identified in the second stage was accomplished (e.g., by determining maximum expected flood height, evaluating the potential for spray of safe-shutdown equipment and the potential for propagation into other areas), to identify plant areas where flooding could have an impact on safe-shutdown

equipment modeled in the internal events PRA. During the fourth stage, the risk from flooding in the areas which were not screened out during the second and third stages was quantified using models, with appropriate assumptions, from the internal events analysis.

In performing the AP1000 internal flooding PRA, the applicant considered all buildings and locations in the screening phase of the study. Buildings in which an internal flood could result in a reactor trip or affect safe shutdown are the nuclear island (containment building and auxiliary building), the annex building, the turbine building, the diesel generator building, and the circulating water pumphouse. The second (initial screening) and third (detailed screening) stages of the study resulted in nine potential internal flooding locations for quantification. Quantification of potential scenarios for these locations resulted in a total CDF, from internal floods that occur when the plant is operating at power, of about 1E-09 per year.

The risk analysis for internal flooding during shutdown operation was performed in a manner similar to the analysis for power operation. The screening of areas performed as part of the at-power analysis was reviewed for applicability to shutdown operation based only on safe shutdown equipment required during shutdown operation. This screening resulted in eight flooding scenarios. Quantification of these eight scenarios resulted in a total CDF, from internal floods that occur during shutdown operation, of about 3E-09 per year. However, during staff review of RAI response 720.38 (dated 3/28/03 and 4/12/2003), the staff noted some math errors that increase the shutdown CDF from internal floods to 4E-9 per year. Flooding scenario number 6, a rupture of the 20.3 cm (8 in.) fire main extension that fails RNS during drained conditions, appears to have been mis-calculated. This is identified as a Confirmatory Item 19.1.10.2-1 (see Section 19.1.10.2 of this report).

The applicant considers the above mentioned CDF estimates to be conservative upper bounds (based on conservative bounding assumptions made in the analysis). Although such a conclusion is not possible without a detailed PRA, the staff finds that the applicant's analysis provides adequate information to draw conclusions about the capability of the design to prevent and mitigate challenges from internal floods. The staff's review did not concentrate on bottom-line numbers but rather on the relative insights that the internal flood analysis provides. The staff believes that the AP1000 design is capable of withstanding severe accident challenges from internal floods in a manner superior to operating plants and that the conclusions from the internal flood risk analysis performed by the applicant complement this belief. The internal flood risk analysis has provided useful safety insights for inclusion in ITAAC, COL Action Items, and RAP. Since detailed PRA-based internal flood analyses at some operating plants have shown that flood-induced sequences can be leading contributors to CDF, the COL applicant should provide an updated internal flood PRA that takes into account design details (e.g., pipe routing, door locations, and flood barriers) to search for internal flooding vulnerabilities in the detailed design. This is COL Action Item 19.1.5-4.

19.1.5.3.1 Dominant Accident Sequences for Internal Floods

The applicant quantified the CDF associated with internal floods, for both at power operation and during shutdown, by using applicable event and fault tree models from the internal events PRA.

19.1.5.3.1.1 Operation at Power

The top five flooding scenarios, contributing over 90 percent of the total CDF from internal flooding at power operation, are summarized below.

Flooding scenario #1, contributing about 20 percent, is initiated by flow from a rupture of an expansion joint in the circulating water system (CWS) located in the turbine building Elevation 100'-0" general area. It is assumed that the flooding and spraying damages all equipment contained in this area, such as main and startup feedwater, condensate, component cooling water, service water and a portion of the non-Class 1E ac power system. This leads to a “loss of main feedwater to both steam generators” or “loss of CCW/SSW” accident initiating event with several non-safety-related support and balance of plant equipment unavailable. There are several combinations of random failures leading to core damage in this flooding scenario. The two dominant ones are as follows:

- stuck-open main steamline safety valve or PORV and consequential SGTR followed by failure of either the IRWST gravity injection or the recirculation from the containment sump, and

- failure of PRHR followed by failure of either the IRWST gravity injection or the recirculation from the containment sump.

Flooding scenarios #2 and #3, each contributing about 20 percent, are similar to scenario #1. They are both initiated by ruptures in the turbine building Elevation 100'-0" general area, as is the case for scenario #1, with same consequences in terms of both equipment failures and propagation to other areas. Scenario #2 is initiated by flow from a rupture in the turbine cooling water system (TCS) while scenario #3 is initiated by flow from a rupture in the heater drain system.

Flooding scenario #4, contributing about 16 percent, is initiated by flow from a rupture of condensate, main or startup feedwater, or fire protection piping located in a room of the turbine building Elevation 135'-3" general area. From there it propagates under the doors to other rooms at the same level as well as to lower level areas (turbine building Elevation 117'-6" and 100'-0" general areas) via floor grating. It is assumed that the flooding and spraying damages all equipment contained in these areas, such as main and startup feedwater, condensate, component cooling and service water, a portion of the non-Class 1E ac power system and compressed air. This leads to a “loss of main feedwater to both steam generators” accident initiating event with several non-safety-related and balance of plant equipment unavailable. There are several combinations of random failures leading to core damage in this flooding scenario. The dominant ones are the same as for scenarios #1, #2 and #3.

Flooding scenario #5, contributing about 14 percent, is initiated by flow from a rupture of the condensate, main or startup feedwater, or fire protection piping located in the turbine building Elevation 117'-6" general area. From there it propagates via floor grating to the Elevation 100'-0" areas. It is assumed that the flooding and spraying damages all equipment contained in these areas, such as main and startup feedwater, condensate, component cooling

water, service water and a portion of the non-Class 1E ac power system. This leads to a “loss of CCW/SSW” or a “loss of main feedwater to both steam generators” accident initiating event with several non-safety-related and balance of plant equipment unavailable. There are several combinations of random failures leading to core damage in this flooding scenario. The dominant ones are the same as for the other top contributing scenarios.

None of the identified internal flooding events during operation at power leads to core damage unless additional random failures occur.

19.1.5.3.1.2 Low Power and Shutdown Operation

The top two flooding scenarios, contributing about 90 percent of the total CDF from internal flooding during shutdown operation, are summarized below.

Shutdown flooding scenario #1, contributing about 45 percent, is initiated by flow from a rupture of the component cooling water, service water or fire protection system piping in the turbine building during mid-loop operation (RCS drained condition). It is assumed that this break, and the subsequent flooding and spraying, damages all equipment contained in the turbine building. This causes a loss of decay heat removal accident initiating event due to the loss of component cooling/service water. Subsequent random failure to inject by either one of the two IRWST gravity injection lines leads to core damage.

Shutdown flooding scenario #2, contributing about 45 percent, is initiated by flow from a rupture of the chemical and volume control or fire protection system piping in the auxiliary building radiologically controlled area (RCA) during mid-loop operation (RCS drained condition). It is assumed that the flooding and spraying damages the normal residual heat removal system (RNS) contained in the auxiliary building RCA area and causes a loss of decay heat removal accident initiating event. Subsequent random failure to inject by either one of the two IRWST gravity injection lines leads to core damage.

None of the identified internal flooding events during shutdown operation leads to core damage unless additional random failures occur.

19.1.5.3.2 Risk-Important Design Features and Operator Actions for Internal Floods

The following is a list of important design features which contribute to the small impact of internal floods in the AP1000:

- Connections to sources of large quantity of water are outside the nuclear island (Containment and auxiliary building) and the annex building.
- There is no safety-related equipment located in the turbine and annex buildings.
- Flow from any postulated ruptures above grade level (Elevation 100'-0") in the turbine building flows down to grade level via floor grating and stairwells. This grating in the

floors also prevents any significant propagation of water to the auxiliary building via flow under the doors.

- The bounding flooding source for the turbine building is a break in the circulating water piping at grade level. Flow from this break runs out from the building to the yard through a relief panel in the turbine building west wall and limits the maximum flood level to less than 6 inches. Flooding propagation to areas of the adjacent auxiliary and annex buildings, via flow under doors or backflow through the drains, is possible but is bounded by a postulated break in those areas.

  - Propagation to the auxiliary building valve/piping penetration room at grade level (the only auxiliary building area that interfaces with the turbine building) – because of the presence of water tight walls and floor combined with drains and access doors to outside, the maximum flood height in the valve/piping penetration room is 36 inches and the flooding does not propagate beyond this area.

  - Propagation to the annex building – flow is directed by the sloped floor to drains and to the yard area through the door of the annex building.

- Flow from any postulated ruptures above grade level (Elevation 100'-0") in the annex building is directed by floor drains to the annex building sump which discharges to the turbine building drain tank. Alternate paths include flows to the turbine building via flow under access doors and down to grade level via stairwells and elevator shaft.

- The floors of the annex building are sloped away from the access doors to the auxiliary building in the vicinity of the access doors to prevent migration of flood water to the non-radiologically controlled areas of the nuclear island where all safety-related equipment, except for some containment isolation valves, is located.

- To prevent flooding in a RCA in the auxiliary building from propagating to non-RCAs (where all safety-related equipment except for some containment isolation valves is located), the non-RCAs are separated from the RCAs by 2 and 3-foot walls and floor slabs. In addition, electrical penetrations between RCAs and non-RCAs in the auxiliary building are located above the maximum flood level.

- Physical separation of safety-related equipment and systems performing redundant functions provides defense-in-depth against internal floods.

- The few penetrations through flood protection walls in the nuclear island that are below the maximum flood level are watertight.

- There are no watertight doors used for flood protection.

- The two 72-hour Class 1E division B and C batteries are located above the maximum flood height in the auxiliary building considering all possible flooding sources (including propagation from sources located outside the auxiliary building).

- The mechanical and electrical equipment in the auxiliary building are separated to prevent propagation of leaks from the piping and mechanical equipment areas to the Class 1E electrical and Class 1E I&C equipment rooms.

- There are two compartments inside containment (PXS-A and PXS-B) containing safe-shutdown equipment other than containment isolation valves that are floodable (i.e., below the maximum flood height of Elevation 108'-2"). Each of these two compartments contains redundant and essentially identical equipment (one accumulator with associated isolation valves as well as isolation valves for one CMT, one IRWST injection line and one containment recirculation line). These two compartments are physically separated so that a flood in one compartment cannot propagate to the other. Drain lines from the PXS-A and PXS-B compartments to the reactor vessel cavity and steam generator compartment are protected from backflow by redundant backflow preventers.

- Containment isolation valves located below the maximum flood height inside containment or in the auxiliary building are normally closed and would not fail open when submerged. Also, there is a redundant, normally closed, containment isolation valve located outside containment in series with each of these valves.

- Plugging of the drain headers is prevented by designing them large enough to accommodate more than the design flow and by making the flow path as straight as possible. Drain headers are at least 10.2 cm (4 in.) in diameter and include features, such as check valves and siphon breaks, that prevent backflow.

- The walls, floors and penetrations are designed to withstand the maximum anticipated hydrodynamic loads.

- The two diesel generators are housed in separate compartments in the Diesel Generator Building with no water propagation paths between the compartments.

- Doors in the Circulating Water Pumphouse prevent flooding the circulating water pumps.

- The main feature of the AP1000 design that contributes to the low CDF associated with internal flooding during shutdown operation is the IRWST. It provides a reliable means of removing decay heat which is not affected by the internal flooding scenarios.

The operator actions modeled in the internal flooding PRA are those used in the internal events PRA plus four additional operator actions to diagnose and isolate a flooding in the north air handling equipment area (Elevation 135'-3") of the annex building (due to the postulated rupture of the 20.3 cm (8 in.) main fire extension) from propagating to the Elevation 66'-6" area of the auxiliary building where the 24-hour Class 1E batteries are located. This scenario would become a dominant internal flooding scenario if all of the human actions were assumed to fail. However, the CDF of this scenario would still be several orders of magnitude lower than the

CDF from internal events. Therefore, no additional significant insights are gained from the internal flooding PRA regarding human errors.

19.1.5.3.3 Insights from the Uncertainty, Sensitivity and Importance Analyses (Internal Flooding)

No uncertainty, importance or sensitivity analyses were performed for internal floods. Because of the conservatism in the approach taken in performing the AP1000 internal flood analysis, in conjunction with the very small assessed CDF from internal floods, such analyses would not provide any useful insights. Important insights from the staff's review of the flood risk analysis performed by the applicant are summarized below.

- The AP1000 design is significantly less dependent on human actions to mitigate internal floods than operating reactors.

- If no credit is taken for the non-safety-related "defense-in-depth" systems to mitigate the flooding events occurring during power operation of the plant, the CDF due to internal flooding would increase by less than one order of magnitude (to less than 1E-08/yr). This result does not change significantly when the uncertainties associated with failure probabilities, reported in Section 19.1.3.1.5 of this report for internal events, are taken into account. This increase in CDF is very small and does not impact the criteria (reported in Section 19.1.7) used to select non-safety-related systems for "regulatory treatment" according to the RTNSS process.

- If no credit is taken by the non-safety-related "defense-in-depth" systems to mitigate floods occurring during shutdown operation, the CDF due to internal flooding would not increase significantly. Such small increase would not impact the probabilistic criteria (reported in Section 19.1.7 of this report) used to select non-safety-related systems for "regulatory treatment" according to the RTNSS process.

19.1.6 Use of PRA in the Design Process

The applicant used PRA in the design process to achieve the following objectives:

- identify vulnerabilities in operating reactor designs and introduce features and requirements that reduce or eliminate these vulnerabilities

- quantify the effect of new design features and operational strategies on plant risk to confirm the risk reduction credit for such improvements

- select among alternative features, operational strategies or design options

Westinghouse used PRA results and insights from operating reactor experience, as well as from the advanced pressurized water reactor (APWR) SP-90 and Sizewell designs, to identify and evaluate potential vulnerabilities in operating reactor designs. This information was first used to introduce special "advanced" design features, such as those described in

Section 19.1.2 of this report, and make the transition from the operating PWR and APWR designs to the AP600 and AP1000 designs. Once these features were introduced, PRA was used to quantify its effect on risk and confirm acceptable reduction or elimination of vulnerabilities, including compliance with the Commission's safety goals. Examples are the CDF reduction estimates (by accident-initiating event category) and associated AP1000 features which contribute to such reduction, reported in Section 19.1.3.1.2 of this report. Since the AP1000 design is based on the AP600 design, the AP600 PRA insights have been used as the starting point.

The following are examples of ways in which the applicant enhanced the AP1000 design by adding or modifying design features or operational requirements based on the AP1000 PRA:

- Changed the normal position of the two MOVs in the sump recirculation lines (which are in series with squib valves) from closed to open to improve the reliability of these paths. This change eliminated the contribution to risk from the failure mode to open the MOVs.

- A low boron core was incorporated into the AP1000 design to reduce the potential contribution of ATWS to plant risk. This change resulted from the observation that for AP600 the ATWS contribution to large release frequency (LRF) was high in relation to other initiating events.

- A third line was added to the passive containment cooling drain lines to increase the water drain reliability of the system. The isolation valve used in the third path is an MOV, which is diverse from the AOVs used in the other two lines. This change resulted from the determination that there is uncertainty regarding long-term containment cooling capability by natural air circulation alone (for AP600 natural air circulation cooling was sufficient for an indefinite time).

- The design of the squib valves in the sump recirculation lines was changed to include two low pressure (LP) and two high pressure (HP) squib valves. This diversification reduces the common cause failure probability of the recirculation lines which is a dominant contributor to risk.

The PRA has been used to select among alternative designs. An example is the design of the accumulators. As a result of the increase in core power with respect to AP600, the AP1000 design requires injection of a larger quantity of borated water by the accumulators during a large LOCA to mitigate the accident. PRA was used to select between a design with increased accumulator capacity with respect to AP600 (which would allow using only one accumulator in the success criteria for large LOCA accidents) and the design with same accumulator capacity used in AP600 (which would require injection by both accumulators to mitigate a large LOCA). It was determined that increasing the accumulator capacity would not reduce significantly the plant risk. Therefore, it was decided to provide the same accumulator capacity in the AP1000 design as in the AP600 design.

Operational changes were also made based on the PRA. Such an example is the change of the procedure for draining the IRWST into the sump to preserve reactor vessel integrity

following core melt. The procedure for this severe accident response has been modified so that the operator action associated with IRWST draining is performed earlier to allow more time for operator success and also fill the cavity as soon as possible.

Finally, PRA was used to identify non-safety-related "defense-in-depth" SSCs that require regulatory oversight (according to the RTNSS process) and to evaluate several severe accident mitigation design alternatives (SAMDAs) by examining the benefits associated with each of these design alternatives.

19.1.7 PRA Input to the "Regulatory Treatment of Non-Safety-Related Systems" (RTNSS) Process

The NRC and the ALWR Steering Committee reached consensus on a process for resolving the RTNSS issue (SECY-94-084). This process included the use of both probabilistic and deterministic criteria to achieve the following objectives: (1) determine whether regulatory oversight for certain non-safety-related systems was needed, (2) identify risk important SSCs for regulatory oversight (if it were determined that regulatory oversight was needed), and (3) decide on an appropriate level of regulatory oversight for the various identified SSCs commensurate with their risk importance. The following two probabilistic criteria are used to achieve such objectives:

- The AP1000 design should meet the Commission's safety goal guideline for CDF of less than 1E-04/yr with no credit for the performance of any non-safety-related "defense-in-depth" systems for which there will be no regulatory oversight according to the RTNSS process.

- The AP1000 design should meet the Commission's safety goal guideline for LRF of less than 1E-06/yr with no credit for the performance of the non-safety-related "defense-in-depth" systems for which there will be no regulatory oversight according to the RTNSS process.

In applying these criteria, the RTNSS process stresses the importance of accounting for uncertainties and also taking into consideration the risk importance of SSCs contributing to initiating event frequencies. Specifically, the RTNSS process provides that the following two items must be addressed:

- Uncertainties, such as in the assumed reliability values for passive system components.

- Non-Safety-related SSCs contributing to initiating event frequencies could be subject to regulatory oversight which is commensurate with their reliability/availability missions.

The applicant used its AP1000 "focused" PRA model, which does not credit non-safety-related systems for accident mitigation (except for the RPV thermal insulation system), and assessed CDF and LRF values which meet both probabilistic criteria. In addition, the applicant provided probabilistic arguments showing that no additional regulatory oversight is needed for SSCs contributing to initiating event frequencies, except for the RNS during cold shutdown and

refueling. The applicant placed availability controls on RNS and its support systems (SWS, CCS, and ac power) when RCS level is not visible in the pressurizer until the refueling cavity is half full and the upper internals are removed. The staff's review found that this additional regulatory oversight for RNS and its support systems (CCW, SSW and ac power) must be extended to Mode 5 operation when the RCS is open (see Section 19.1.4.5 of this report). The applicant agreed to require additional regulatory oversight for RNS and its support systems (CCW, SSW and onsite ac power) for the whole period of Mode 5 when the RCS is open, as discussed in DCD Tier 2 Section 16.3.

Furthermore, the staff review found that the issue of uncertainties (e.g., those associated with the assumed reliability values for passive system components) had not been addressed. Staff sensitivity studies have shown that the "focused" PRA results (e.g., CDF and LRF) are sensitive to the reliability values used in the PRA for certain passive system components which have significant uncertainties associated with them. The results of such sensitivity studies have shown that when more bounding data are used in the PRA in order to address uncertainties, both probabilistic criteria are met only when credit is taken for some additional non-safety-related "defense-in-depth" systems. Therefore, the need for regulatory oversight of certain SSCs has been determined and is discussed below and in Chapter 22 of this report.

The results of the uncertainty and importance analyses were used to select SSCs for sensitivity studies. These analyses indicated that the following SSCs have the largest impact on PRA results, such as CDF and LRF, used in the criteria for selecting non-safety-related SSCs for regulatory oversight according to the RTNSS process:

- reactor trip components, such as circuit breakers
- ESF actuation components, such as software
- passive system check valves and explosive (squib) valves

A series of sensitivity studies were performed by the staff to investigate the impact of uncertainties in the performance of these SSCs on PRA results, under the assumption of plant operation without credit for one or more non-safety-related "defense-in-depth" systems. These studies provided additional insights about the risk importance of the various "defense-in-depth" systems which were taken into account in selecting non-safety-related systems for "regulatory treatment" according to the RTNSS process (detailed results and insights related to CDF are reported in Section 19.1.3.1.5 of this report while insights related to LRF and CCFP are reported in Section 19.1.3.2 of this report). The most important insights from such sensitivity studies, as they relate to the RTNSS process, are summarized below.

- Availability control of the RT function of DAS provides an efficient means for minimizing the impact of uncertainties in reactor trip components, such as circuit breakers, on PRA results used in the criteria for selecting non-safety-related SSCs for regulatory oversight according to the RTNSS process. Such availability control should include the two M-G set CBs because the RT function of DAS requires the availability (to open) of both these CBs.

- Availability control of the ESF actuation function of DAS provides an efficient means for minimizing the impact of uncertainties associated with ESF actuation components, such as digital I&C system software, on PRA results used in the criteria for selecting non-safety-related SSCs for regulatory oversight according to the RTNSS process.

- Availability control of the RNS (including its support systems) provides an efficient means for minimizing the impact of uncertainties associated with passive system check valves and explosive (squib) valves on PRA results used in the criteria for selecting non-safety-related SSCs for regulatory oversight according to the RTNSS process.

For AP600, the staff also have determined the following:

- Criterion #1 (i.e., CDF less than 1E-04/y) is fully satisfied when an unavailability of 0.25 or less is assumed in the PRA for DAS (for both the reactor trip and ESF actuation functions) and for RNS. This requires an "average" yearly availability of at least 75 percent for such systems.

- Criterion #2 (i.e., LRF less than 1E-06/y) is fully satisfied when an unavailability of 0.1 or less is assumed in the PRA for each of the automatic and manual portions of DAS (for both the reactor trip and ESF actuation functions) and for RNS. This requires an "average" yearly availability of at least 90 percent for such systems or subsystems.

The staff cannot reach similar conclusions for AP1000 at this time. As explained in Section 19.1.10 of this report, additional information is needed which will provide the link between the PRA results and the level of regulatory oversight needed to meet the above mentioned criteria. This is Open Item 19.1.10.1-3.

19.1.8 PRA Input to the Design Certification Process

PRA has been used in the design certification process to achieve the following objectives: (1) develop an in-depth understanding of design robustness and tolerance of severe accidents initiated by either internal or external events, (2) develop a good appreciation of the risk significance of human errors associated with the design, and characterize the key errors in preparation for better training and refined procedures, and (3) identify important safety insights related to design features and assumptions made in the PRA to support certification requirements, such as ITAACs, design RAP (D-RAP) requirements, TSs, as well as COL and interface requirements.

The first two objectives are achieved by identifying the dominant accident sequences as well as the risk-important design features and human actions (see Sections 19.1.3 to 19.1.5). The third objective is achieved by using PRA insights and assumptions to develop design certification requirements. In its response to RAI 720.038, the applicant provided a preliminary and, recently, a revised list of “design certification requirements.” The staff is still reviewing the list of “design certification requirements” proposed by the applicant, especially in light of assumptions and insights related to differences in PRA models between the AP600 and AP1000 designs. The staff expects the final list of “design certification requirements” to be in agreement with the

resolution of all open items identified in the AP1000 DSER. This is an open item in the AP1000 DSER (see Section 19.1.10.1 of this report). The currently available preliminary list of design certification "requirements" is reported below.

19.1.8.1 General and plant-wide requirements

- Risk important SSCs have been identified and included in the D-RAP (DCD Tier 2 Section 17.4).

- The COL applicant referencing the AP1000 design will perform a seismic walkdown to ensure that the as-built plant conforms to the design used as the basis for the seismic margins evaluation and that seismic spatial systems interactions do not exist. Details of the process will be developed by the COL applicant.

- The COL applicant referencing the AP1000 certified design will review differences between the as-built SSC HCLPFs to those assumed in the AP1000 seismic margin evaluation. Deviations from the HCLPF values or assumptions in the seismic margins evaluation should be evaluated to determine if vulnerabilities have been introduced.

- The COL Applicant will maintain an operation reliability assurance process based on the system reliability information derived from the PRA and other sources. The COL applicant will incorporate the list of risk-important SSCs, as presented in the DCD section on D-RAP, in its D-RAP and operation reliability assurance process.

- The COL applicant will use information regarding risk-important operator actions from the PRA, as presented in DCD Tier 2 Chapter 18 on human factors engineering, in developing and implementing procedures, training and other human reliability related programs.

- As deemed necessary, during the detailed design phase, the COL applicant will update the PRA, including the fire and flood analyses for both at-power and shutdown operation. Using the final design information and site-specific information, the COL applicant will re-evaluate the qualitative screening of external events. The updated PRA will include any site-specific susceptibilities found, and the applicable external events.

- There is no safety-related equipment located outside the nuclear island.

- A combination of multiple isolation valves, valve interlocking, increase in the piping pressure limits and pressure relief capability protects the AP1000 against interfacing systems LOCA (ISLOCA).

- The AP1000 safety-related I&C system will use solid state switching devices and electro-mechanical relays resistant to relay chatter. Use of these devices and relays minimizes the mechanical discontinuities associated with similar devices at operating reactors.

- The AP1000 design does not use watertight doors for flood protection.

- The AP1000 design minimizes potential flooding sources in safety-related equipment areas, to the extent possible. The design also minimizes the number of penetrations through enclosure or barrier walls below the probable maximum flood level. The design enables all flood barriers (e.g., walls, floors and penetrations) to withstand the maximum anticipated hydrodynamic loads.

- Plugging of the drain headers is minimized by designing them large enough to accommodate more than the design flow and by making the flow path as straight as possible.

- There is no cable spreading room in the AP1000 design.

- Separation or protection of equipment and cabling among the divisions of safety-related equipment and separation of safety-related from nonsafety-related equipment, minimizes the probability that a fire or flood would affect more than one safety-related system or train except in some areas inside containment where equipment will be capable of achieving safe shutdown before damage.

- The following minimize the probability for fire or flood propagation from one area to another and help limit risk from internal fires and floods:

  - Fire barriers are sealed, to the extent possible (i.e., doors).

  - Structural barriers that function as flood barriers are watertight below the maximum flood level.

  - The COL applicant will establish administrative controls to maintain the performance of the fire protection system.

  - Requirements for fire and flood barrier and maintenance will be implemented in COL applicant programs. The purpose of these requirements is to ensure the reliable performance of fire barriers (e.g., through appropriate inspection and maintenance of doors, dampers, and penetration seals) and of flood barriers (e.g., through appropriate maintenance of all water tight penetrations during power operation to prevent the propagation of water from one area to the next).

  - When a fire door, fire barrier penetration, or flood barrier penetration must be open to allow specific maintenance (e.g., during plant shutdown), appropriate compensatory measures will be taken to minimize risk. Risk during shutdown is minimized by appropriate outage management, administrative controls, procedures, and operator knowledge of plant configuration. In particular, this will require configuration control of fire/flood barriers to ensure the integrity of fire and flood barriers between areas containing equipment performing redundant safe shutdown functions.

- The design provides fire detection and suppression capability. The design also provides flooding control features and sump level indication. Compensatory measures are expected to be taken by the COL applicant to maintain adequate detection and suppression capability during maintenance activities.

- In addition to the MCR that has its own dedicated ventilation system, there are separate ventilation systems for each of the two pairs of safety-related equipment divisions supporting redundant functions (i.e., divisions A&C and B&D). Furthermore, the plant ventilation systems include features to prevent propagation of smoke from a non-safety-related area to a safety-related area or between safety-related areas supported by two different divisions. The COL applicant will ensure the reliable performance of such smoke propagation prevention features.

- The COL applicant will implement the maintenance guidelines as described in the Shutdown Evaluation Report (WCAP-14837).

- The COL applicant will control transient combustibles. This is particularly important during shutdown operation with ongoing maintenance activities.

19.1.8.2 Main Control Room and Remote Shutdown Workstation

- Redundancy in MCR operations is provided within the MCR itself for fires in which control room evacuation is not required.

- Although a MCR fire may defeat manual actuation of equipment from the MCR, it will not affect the automatic functioning of safe shutdown equipment via PMS or manual operation from the RSW. This is because of the location of the PMS cabinets, in which the automatic functions are housed, in fire areas separate from the MCR.

- The RSW provides sufficient instrumentation and control to bring the plant to safe shutdown conditions in case the control room must be evacuated. There are no differences between the MCR and the RSW controls and monitoring that would be expected to affect safety system redundancy and reliability.

- The RSW provides redundancy of control and monitoring for safe shutdown functions in the event that the evacuation of the main control room is required.

- The MCR has its own dedicated ventilation system and is pressurized. This eliminates the possibility of smoke, hot gases, and fire suppressants, originated in areas outside the control room from entering the control room via the ventilation system.

- The MCR and the RSW are in separate fire and flood areas. They have separate and independent ventilation systems.

- AP1000 MCR fire ignition frequency is limited as a result of the use of low-voltage, low-current equipment and fiber optic cables.

19.1.8.3 Containment/Shield Building

- Redundant containment isolation valves in each line protect containment isolation functions from the impact of internal fires and floods. The location of these valves is in separate fire and flood areas. Different power and control divisions serve these valves, if powered. The location of one isolation component in a given line is always inside containment, while the location of the other is outside containment, and the containment wall is a fire/flood barrier.

- Although the containment is a single fire area, adequate design features exist to ensure the plant can achieve safe-shutdown conditions. Such features include separation (structural or space), suppression, lack of combustibles and operator actions.

- There are two compartments inside containment (PXS-A and PXS-B) containing safe-shutdown equipment that are below the maximum flood height. Each of these two compartments contains redundant and essentially identical equipment (one accumulator with associated isolation valves as well as isolation valves for one CMT, one IRWST injection line and one containment recirculation line). A pipe break in one of these compartments can cause that room to flood. A structural wall physically separates these two compartments to ensure that a flood in one compartment does not propagate to the other. Drain lines from the PXS-A and PXS-B compartments to the reactor vessel cavity and steam generator compartment are protected from backflow by redundant backflow preventers.

- Containment isolation valves located below the maximum flood height inside containment or in the auxiliary building are normally closed and are designed to fail closed.

- The passive containment cooling system (PCS) cooling water not evaporated from the vessel wall flows down to the bottom of the inner containment annulus. Screens prevent clogging (e.g., by the entry of small animals into the drains) of two 100 percent drain openings, located in the side wall of the shield building. These drains are always open. The annulus drains will have the same (or higher) HCLPF value as the shield building so that the drain system will not fail at lower acceleration levels causing water blocking of the PCS air baffle.

- The ability to close containment hatches and penetrations following an accident during Modes 5 and 6, before steam is released into the containment, is important. The COL applicant is responsible for developing procedures and training to address this issue. This is COL Action Item 19.1.8-5.

- The COL applicant should provide administrative controls to control foreign debris from being introduced into the containment during maintenance and inspection operations, to prevent plugging of the containment sump screens. This is COL Action Item 19.1.8-6.

19.1.8.4 Auxiliary Building

- The design provides separate ventilation systems for each of the two pairs of safety-related equipment divisions supporting redundant functions (i.e., divisions A&C and B&D). This prevents smoke, hot gases, and fire suppressants originating in divisions A or C from propagating to divisions B and D.

- 3-hour rated fire walls without openings separate the major rooms housing divisional cabling and equipment (the battery rooms, dc equipment rooms, I&C rooms, and penetration rooms). There are no doors, dampers, or seals in these walls. Separate ventilation subsystems serve the rooms. In order for a fire to propagate from one divisional room to another, it must move past a 3-hour barrier (e.g., a door) into a common corridor and enter the other room through another 3-hour barrier (e.g., another door).

- An access bay protects important safety-related I&C equipment as well as the main control room and the remote shutdown panel, located in the north end of the auxiliary building, from potential debris produced by a postulated seismically-induced structural collapse of the adjacent turbine building.

- There are no normally open connections to sources of "unlimited" quantity of water in the auxiliary building.

- Separation of the non-RCAs from the RCAs by 2 and 3-foot walls and floor slabs prevent flooding in a RCA in the auxiliary building from propagating to non-RCAs. In addition, the location of electrical penetrations between RCAs and non-RCAs in the auxiliary building are above the maximum flood level.

- The location of the two 72-hour rated Class 1E division B and C batteries are above the maximum flood height in the auxiliary building considering all possible flooding sources (including propagation from sources located outside the auxiliary building).

- Flood water propagated from the turbine building to the auxiliary building valve/piping penetration room at grade level (the only auxiliary building area that interfaces with the turbine building) is directed to drains and to the outside through access doors. This, combined with the presence of water tight walls and floor of the valve/penetration room, limits the maximum flood height in the valve/piping penetration room (to about 91 cm (36 in.)) and prevents flooding from propagating beyond this area.

- The mechanical and electrical equipment in the auxiliary building are separated to prevent propagation of leaks from the piping and mechanical equipment areas to the Class 1E electrical and Class 1E I&C equipment rooms.

19.1.8.5 Turbine Building

- The turbine building contains no safety-related equipment. There is a 3-hour fire barrier wall between the turbine building and the safety-related areas of the nuclear island.

- The location of the connections to sources of a "large" quantity of water are in the turbine building. They are the service water system (SWS) which interfaces with the component cooling water system (CCS) and the circulating water system (CWS) which interfaces with the turbine building closed cooling system (TCS) and the condenser. Features that minimize flood propagation to other buildings are:

  - Flow from any postulated ruptures above grade level (Elevation 100'-0") in the turbine building flows down to grade level via floor grating and stairwells. This grating in the floors also prevents any significant propagation of water to the auxiliary building via flow under the doors.

  - A relief panel in the turbine building west wall at grade level directs the water outside the building to the yard and limits the maximum flood level in the turbine building to less than 15.2 cm (6 in.). Flooding propagation to areas of the adjacent auxiliary building, via flow under doors or backflow through the drains, is possible but is bounded by a postulated break in those areas.

19.1.8.6 Annex Building

- There is no safety-related equipment located in the annex building.

- The sloped floor directs flood water in the annex building grade level to drains and to the yard area through the door of the annex building.

- Floor drains to the annex building sump that discharges to the turbine building drain tank directs flow from postulated ruptures above grade level in the annex building. Alternate paths include flows to the turbine building via flow under access doors and down to grade level via stairwells and elevator shaft.

- The floors of the annex building slope away from the access doors to the auxiliary building in the vicinity of the access doors to prevent migration of flood water to the non-radiologically controlled areas of the nuclear island, the location of all safety-related equipment except for some containment isolation valves.

- There are no connections to sources of "unlimited" quantity of water (i.e., open connections) in the annex building.

19.1.8.7 Reactor Coolant System

- To prevent overdraining, the RCS hot and cold legs are vertically offset which permits draining of the steam generators for nozzle dam insertion with a hot-leg level much higher than traditional designs. This level is nominally 80 percent level in the hot leg.

- Use of a step nozzle connection between the RCS hot leg and the RNS suction line lowers the level in the hot leg at which vortexing can occur. The step nozzle is a 50.8 cm (20 in.) schedule 140 pipe, approximately 0.61 m (2 ft) long.

- Should vortexing occur, the maximum air entrainment into the pump suction was shown experimentally to be no greater than 5 percent.

- There are two safety-related RCS hot-leg level channels, one located in each hot leg. These level instruments are independent and do not share instrument lines. These level indicators are in place primarily to monitor RCS level during mid-loop operations. One level tap is at the bottom of the hot leg, and the other tap is on the top of the hot leg as close to the steam generator as possible.

- Wide range pressurizer level indication (cold calibrated) provides measurement of RCS level to the bottom of the hot legs. The upper level tap connects to an ADS valve inlet header above the top of the pressurizer. The lower level tap connects to the bottom of the hot leg. This non-safety-related pressurizer level indication can serve as an alternative way of monitoring level and as a means to identify inconsistencies in the safety-related hot-leg level instrumentation.

- The RNS pump suction line slopes continuously upward from the pump to the reactor coolant system hot leg with no local high points. This design eliminates potential problems in refilling the pump suction line if an RNS pump is stopped when cavitating as a result of excessive air entrainment. This self-venting suction line allows the RNS pumps to immediately restart once re-establishment of an adequate level in the hot leg occurs.

- The COL applicant should have procedures and policies to maximize the availability of the non-safety-related wide range pressurizer level indication (cold calibrated) during RCS draining operations during cold shutdown. Training should be given to the operators on how to use this indication to identify inconsistencies in the safety-related hot-leg level instrumentation to prevent RCS overdraining. This is COL Action Item 19.1.8-7.

19.1.8.8 Passive Core Cooling Systems

The passive core cooling system (PXS) is composed of the (1) the accumulator subsystem, (2) the CMT subsystem, (3) the IRWST subsystem, and (4) the PRHR subsystem. In addition, the ADS, which is part of the RCS, also supports passive core cooling functions.

19.1.8.9 Accumulators

The accumulators provide a safety-related means of safety injection of borated water to the RCS. The following are some important aspects of the accumulator subsystem as represented in the PRA:

- There are two accumulators, each with an injection line to the reactor vessel/DVI nozzle. Each injection line has two check valves in series.

- The reliability of the accumulator subsystem is important. The accumulator subsystem is included in the D-RAP.

- Diversity between the accumulator check valves and the CMT check valves minimizes the potential for common cause failures.

19.1.8.10 Core Makeup Tanks

The CMTs provide safety-related means of high-pressure safety injection of borated water to the RCS.

The following are some important aspects of the CMT subsystem as represented in the PRA:

- There are two CMTs, each with an injection line to the reactor vessel/DVI nozzle. Each CMT has a normally open pressure balance line from an RCS cold leg. Each injection line is isolated with a parallel set of air-operated valves (AOVs). These AOVs open on loss of Class 1E dc power, loss of air, or loss of the signal from the PMS. The injection line for each CMT also has two normally open check valves in series.

- Actuation of the CMT AOVs from PMS and DAS is automatic and manual. Indication of their positions and alarms are in the control room.

- CMT level instrumentation provides an actuation signal to initiate automatic ADS and provides the actuation signal for the IRWST squib valves to open.

- The CMTs are risk-important for power conditions because the level indicators in the CMTs provide an open signal to ADS and to the IRWST squib valves as the CMTs empty. The CMT subsystem is included in the D-RAP. The CMT AOVs are stroke-tested quarterly.

- The TSs require the CMTs to be available from power conditions down through cold shutdown (Mode 1 through Mode 5) with RCS pressure boundary intact.

19.1.8.11 In-Containment Refueling Water Storage Tank

The IRWST subsystem provides a safety-related means of performing (1) LPSI following ADS actuation, (2) long-term core cooling via containment recirculation, and (3) reactor vessel cooling through the flooding of the reactor cavity by draining the IRWST into the containment. Some important aspects of the IRWST subsystem as represented in the PRA are listed below.

- The IRWST subsystem has the following flowpaths:

  - Two (redundant) injection lines from IRWST to reactor vessel DVI nozzle. A parallel set of valves isolates each line; each set with a check valve in series with a squib valve.

  - Two (redundant) recirculation lines from the containment to the reactor vessel DVI injection line. Each recirculation line has two paths: one path contains a squib valve and a MOV, the other path contains a squib valve and a check valve.

  - The two MOV/squib valve lines also provide the capability to flood the reactor cavity.

- There are screens for each IRWST injection line and recirculation line which prevents clogging by debris or other materials generated in the IRWST or containment sump. The COL Applicant will maintain the reliability of the IRWST subsystem, including the IRWST and containment recirculation screens.

- Explosive (squib) valves provide the pressure boundary and protect the check valves from any potential adverse impact of high differential pressures.

- The explosive (squib) valves and MOVs are powered by Class 1E power. Indication of their positions and alarms are in the control room.

- Actuation of the squib valves and MOVs for injection and recirculation via PMS is automatic and manual. Actuation via DAS is manual.

- Actuation of the squib valves and MOVs for reactor cavity flooding is manual via PMS and DAS from the control room.

- The injection squib valves and the recirculation squib valves in series with check valves are diverse from the other recirculation squib valves in order to minimize the potential for common cause failure between injection and recirculation/reactor cavity flooding.

- Automatic IRWST injection at shutdown conditions is provided using PMS low hot leg level logic.

- Exercising of the IRWST injection and recirculation check valves occurs at each refueling. Testing of the IRWST injection and recirculation squib valve actuators occurs every 2 years for 20 percent of the valves (this does not require valve actuation). Stroke testing of IRWST recirculation MOVs occurs quarterly.

- The reliability of the IRWST subsystem is important. The IRWST subsystem is included in the D-RAP.

- Technical Specifications require IRWST injection and recirculation to be available from power conditions to refueling without the cavity flooded (from Mode 1 though Mode 6).

- The operator action to flood the reactor cavity is determined in Emergency Response Guideline AFR-C.1, which instructs the operator to flood the reactor cavity when the core-exit thermocouples reach 648.9°C (1200°F).

- The PXS recirculation valves are automatically actuated by a low IRWST level signal or manually from the control room, if automatic actuation fails.

19.1.8.12 Passive Residual Heat Removal System

The PRHR provides a safety-related means of performing the following functions: (1) removes core decay heat during accidents, (2) allows adequate plant performance during transient (non-LOCA and non-ATWS) accidents without ADS, (3) allows automatic termination of RCS leak during a SGTR accident without ADS, and (4) allows the plant to ride out an ATWS event without rod insertion.

The PRA models incorporate the following important aspects of the PRHR design and operation features:

- Opening the redundant parallel AOVs actuates the PRHR. These AOVs are designed to fail open on loss of Class 1E power, loss of air, or loss of the signal from the PMS.

- Two redundant and diverse I&C systems automatically actuate the PRHR AOVs: (1) the safety-related PMS and (2) the non-safety-related DAS. Manual actuation of the PRHR can also be achieved from the control room using either PMS or DAS.

- Diversity of the PRHR AOVs from the AOVs in the CMTs minimizes the probability for common cause failure of both PRHR and CMT AOVs.

- Indications of the positions of the inlet and outlet PRHR valves, including alarms, are in the control room.

- The PRHR AOVs are stroke-tested quarterly. The PRHR HX is tested to detect system performance degradation every 10 years.

- Use of the PRHR HX for long-term cooling will result in steaming to the containment. The steam will normally condense on the containment shell and return to the IRWST by safety-related features (gutter system). Connections to the IRWST are provided from the spent fuel system (SFS) and chemical and volume control system (CVS) to extend PRHR operation. A safety-related makeup connection is also provided from outside the containment through the normal RNS to the IRWST.

- Capability exists and guidance is provided for the control room operator to identify a leak in the PRHR HX of 1,892 lpd (500 gpd) or higher. This limit is based on the assumption that a single crack leaking this amount would not lead to a PRHR HX tube rupture under the stress conditions involving pressure and temperature gradients expected during design basis accidents, which the PRHR HX is designed to mitigate.

- The PRHR HX, in conjunction with the PCS, can provide core cooling for an indefinite period of time. After the IRWST water reaches its saturation temperature, the process of steaming to the containment initiates. Condensation occurs on the steel containment vessel, and the condensate is collected in a safety-related gutter arrangement, which returns the condensate to the IRWST. The gutter normally drains to the containment sump, but when the PRHR HX actuates, safety-related actuation valves in the gutter drain line shut and the gutter overflow returns directly to the IRWST. The following design features provide proper re-alignment of the gutter system valves to direct water to the IRWST:

  - the IRWST gutter and its drain isolation valves are safety-related

  – on loss of compressed air, loss of Class 1E dc power, or loss of the PMS signal the valves that re-direct the flow will, by design, fail closed

  – the drain isolation are actuated automatically by PMS and DAS.

- Technical Specifications require the PRHR to be available, with RCS boundary intact, from power conditions down through cold shutdown (from Modes 1 through 5).

- The PRHR provides a safety-related means of removing decay heat following loss of RNS cooling during shutdown conditions with the RCS intact.

19.1.8.13 Automatic Depressurization System

ADS provides a safety-related means of depressurizing the RCS. The following are some important aspects of ADS as represented in the PRA:

- ADS has four stages. Two separate groups of valves and lines comprise each stage. Stages 1,2, and 3 discharge from the top of the pressurizer to the IRWST. Stage 4 discharges from the hot leg to the RCS loop compartment.

- Each stage 1, 2, and 3 line contains two MOVs in series. Each stage 4 line contains an MOV valve and a squib valve in series.

- The valve arrangement and positioning for each stage, by design, reduces spurious actuation of ADS.

  - Stage 1, 2, and 3 MOVs are normally closed and have separate controls
  - A stage 4 squib valve actuation requires signals from two separate PMS cabinets
  - Stage 4 is blocked from opening at high RCS pressures.

- Actuation of the ADS valves via the PMS is automatic and manual. Via the DAS, actuation is manual.

- The ADS valves are powered from Class 1E power. The control room contains their positions indications as well as alarms.

- Stroke-testing of stage 1, 2, and 3 valves occurs during every cold shutdown. Testing of the stage 4 squib valve actuators occurs every 2 years for 20 percent of the valves.

- Because of the potential for counter-current flow limitation in the surgeline, it is essential to establish and maintain venting capability with ADS Stage 4 for gravity injection and containment recirculation following an extended loss of RNS when the RCS is open during shutdown operations.

- The Stage 4 ADS squib valves receive a signal to open during shutdown conditions using PMS low hot leg level logic.

- The ADS Stages 1,2, and 3, connected to the top of the pressurizer, provide a vent path to preclude pressurization of the RCS during shutdown conditions if decay heat removal is lost.

- The reliability of the ADS is important. The ADS is included in the D-RAP.

- Technical Specifications require ADS to be available during power operation and shutdown conditions until the cavity is flooded (i.e., from Mode 1 through Mode 6).

- Depressurization of the RCS through ADS minimizes the potential for high-pressure melt ejection events. Procedures will be provided for use of the ADS for depressurization of the RCS after core uncovery.

- The ADS mitigates high pressure core damage events which can produce challenges to containment integrity due to the following severe accident phenomena:

    - High pressure melt ejection
    - Direct containment heating
    - Induced steam generator tube rupture
    - Induced RCS piping rupture and rapid hydrogen release to containment.

19.1.8.14 Instrumentation and Control Systems

The following three I&C systems are credited in the PRA for providing monitoring and control functions during accidents: (1) the safety-related PMS, (2) the non-safety-related DAS, and (3) the non-safety-related PLS.

The PMS provides a safety-related means of performing the following functions:

- automatic and manual reactor trip,

- automatic and manual actuation of engineered safety features (ESF), and

- monitor the safety-related functions during and following an accident as required by Regulatory Guide 1.97.

The DAS provides a non-safety-related means of performing the following functions:

- automatic and manual reactor trip,
- automatic and manual actuation of selected ESF, and
- provides control room indication for monitoring of selected safety-related functions.

The PLS provides a non-safety-related means of performing the following functions:

- automatic and manual control of non-safety-related systems, including "defense-in-depth" systems (e.g., RNS), and
- provides control room indication for monitoring overall plant and non-safety-related system performance.

The following are some important aspects of PMS as represented in the PRA:

- The PMS initiates an automatic reactor trip and an automatic actuation of ESF. The PMS also provides manual initiation of reactor trip. The PMS uses a 2-out-of-4 initiation logic which reverts to 2-out-of-3 coincidence logic if one of the four channels is bypassed. The PMS does not allow simultaneous bypass of 2 redundant channels.
- The PMS has redundant divisions of safety-related post-accident parameter display.
- Each of the four PMS redundant divisions receives power from its respective Class 1E dc and UPS division.
- The PMS provides fixed position controls in the control room.
- The reliability of the PMS is provided by the following:
  - The reactor trip functions are divided into two subsystems.
  - The ESF functions are processed by two microprocessor-based subsystems that are functionally identical in both hardware and software.
- Four sensors normally monitor variables used for an ESF actuation. These sensors may monitor the same variable for a reactor trip function.
- Provisions are in place for continuous automatic PMS system monitoring and failure detection/alarm.

- PMS equipment accommodates, by design, a loss of the normal heating, ventilation, and air conditioning (HVAC). The passive heat sinks protect PMS equipment on failure or degradation of the active HVAC.

- The reliability of the PMS is important. The PMS is included in the D-RAP.

- The PMS software is designed, tested, and maintained to be reliable under a controlled verification and validation program written in accordance with Institute of Electrical and Electronics Engineers (IEEE) 7-4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power generating Stations,” (1993), that has been endorsed by Regulatory Guide 1.152. Elements that contribute to a reliable software design include:

    - A formalized development, modification, and acceptance process in accordance with an approved software QA plan (paraphrased from IEEE standard, Section 5.3, "Quality")

    - A verification and validation program prepared to confirm the design implemented will function as required (IEEE standard, Section 5.3.4, "Verification and Validation")

    - Equipment qualification testing performed to demonstrate that the system will function as required in the environment it is intended to be installed in (IEEE standard, Section 5.4, "Equipment Qualification")

    - Design for system integrity (performing its intended safety function) when subjected to all conditions, external or internal, that have significant potential for defeating the safety function (abnormal conditions and events) (IEEE standard, Section 5.5, "System Integrity")

    - Software configuration management process (IEEE standard, section 5.3.5, "Software Configuration Management").

The following are some important aspects of DAS as represented in the PRA:

- The PRA assumes diversity that eliminates the potential for common cause failures between PMS and DAS. The DAS automatic actuation signals are generated in a diverse manner from the PMS signals. Diversity between the DAS and PMS is achieved by the use of different architecture, different hardware implementations, and different software.

- DAS provides control room displays and fixed position controls to allow the operators to take manual actions.

- DAS actuates using 2-out-of-2 logic. Actuation signals are output to the loads in the form of normally de-energized, energize-to-actuate signals. The normally de-energized

output state, along with the dual 2-out-of-2 redundancy, reduces the probability of inadvertent actuation.

- The actuation devices of DAS and PMS are capable of independent operation that is not affected by the operation of the other. The DAS is designed to actuate components only in a manner that initiates the safety function.

- Implementation of the DAS manual initiation functions bypasses the signal processing equipment of the DAS automatic logic. This is assumed in the PRA to eliminate the potential for common cause failures between automatic and manual DAS functions.

- Implementation of the DAS reactor trip function is through a trip of the control rods via the motor-generator (M-G) set field breakers which are separate and diverse from the reactor trip breakers.

- The DAS is an important "defense-in-depth" system. The availability of DAS, with respect to both its reactor trip and ESF actuation functions, will be controlled. In addition, the DAS (including the M-G set field breakers) is included in the D-RAP.

The following are some important aspects of PLS as represented in the PRA:

- PLS has redundancy to minimize plant transients.

- PLS provides capability for both automatic control and manual control.

- Signal selector algorithms provide the PLS with the ability to obtain inputs from the PMS. The signal selector algorithms select those protection system signals that represent the actual status of the plant and reject erroneous signals.

- Distribution of PLS control functions are across multiple distributed controllers so that single failures within a controller do not degrade the performance of control functions performed by other controllers.

19.1.8.15 Onsite Power

The onsite power system consists of the main ac power system and the dc power system. The main ac power system is a non-Class 1E system. The dc power system consists of two independent systems: the Class 1E dc system and the non-Class 1E dc system.

The main onsite ac power system is a non-Class 1E system comprised of a normal, preferred, and standby power supplies. It distributes power to the reactor, turbine, and balance of plant auxiliary electrical loads for startup, normal operation, and normal/emergency shutdown.

The Class 1E dc and UPS system (IDS) provides reliable power for the safety-related equipment required for the plant instrumentation, control, monitoring, and other vital functions needed for shutdown of the plant.

The non-Class 1E dc and UPS system (EDS) consists of the electric power supply and distribution equipment that provide dc and uninterruptible ac power to non-safety-related loads.

The following are some important aspects of the main ac power system as represented in the PRA:

- The arrangement of the buses permits feeding functionally redundant pumps or groups of loads from separate buses and enhances the plant operational reliability.

- During power generation mode, the turbine generator normally supplies electric power to the plant auxiliary loads through the unit auxiliary transformers. During plant startup, shutdown, and maintenance, the main ac power is provided by the preferred power supply from the high-voltage switchyard. The onsite standby power system powered by the two onsite standby diesel generators supplies power to selected loads in the event of loss of normal and preferred ac power supplies.

- Two onsite standby diesel generator units, each furnished with its own support subsystems, provide power to the selected plant nonsafety-related ac loads.

- On loss of power to a 6900 V diesel-backed bus, the associated diesel generator automatically starts and produces ac power. The normal source circuit breaker and bus load circuit breakers are opened, and the generator is connected to the bus. Each generator has an automatic load sequencer to enable controlled loading on the associated buses.

The following are some important aspects of the Class 1E dc and UPS system (IDS) as represented in the PRA:

- There are four independent, Class 1E 125 V dc divisions. Divisions A and D each consists of one battery bank, one switchboard, and one battery charger. Divisions B and C are each composed of two battery banks, two switchboards, and two battery chargers. The first battery bank in the four divisions is designated as the 24-hour battery bank. The second battery bank in Divisions B and C is designated as the 72-hour battery bank.

- The 24-hour battery banks provide power to the loads required for the first 24 hours following an event of loss of all ac power sources concurrent with a design basis accident. The 72-hour battery banks provide power to those loads requiring power for 72 hours following the same event.

- Battery chargers are connected to dc switchboard buses. The input ac power for the Class 1E dc battery chargers is supplied from non-Class 1E 480 V ac diesel-generator-backed motor control centers.

- The 24-hour and 72-hour battery banks are housed in ventilated rooms apart from chargers and distribution equipment.

- Each of the four divisions of dc systems are electrically isolated and physically separated to prevent an event from causing the loss of more than one division.

- The Class 1E batteries are included in the D-RAP.

The following are some important aspects of the non-Class 1E dc and UPS system as represented in the PRA:

- The non-Class 1E dc and UPS system consists of two subsystems representing two separate power supply trains.

- EDS load groups 1, 2, and 3 provide 125 V dc power to the associated inverter units that supply the ac power to the non-Class 1E uninterruptible power supply ac system.

- The onsite standby diesel-generator-backed 480 V ac distribution system provides the normal ac power to the battery chargers.

- The batteries are sized to supply the system loads for a period of at least two hours after loss of all ac power sources.

19.1.8.16 Normal Residual Heat Removal System

The RNS provides a non-safety-related means of core cooling during accidents through: (1) RCS recirculation cooling during shutdown conditions, (2) low pressure pumped makeup flow from the SFS cask loading pit and long-term recirculation from the containment sump, and (3) heat removal from the IRWST during PRHR operation. Such RNS functions provide defense-in-depth in mitigating accidents, in addition to that provided by the passive safety-related systems.

The RNS also provides a safety-related means of performing the following functions: (1) Containment isolation for the RNS lines that penetrate the containment, (2) isolation of the reactor coolant system at the RNS suction and discharge lines, and (3) pathway for long-term, post-accident makeup of containment inventory.

The following are some important aspects of RNS as represented in the PRA:

- The RNS has redundant pumps (separate non-Class 1E buses with backup connections from the diesel generators power these pumps) and redundant heat exchangers.

- The RNS is manually aligned from the control room to perform its core cooling functions. The performance of the RNS is indicated in the control room.

- The RNS containment isolation and pressure boundary valves are safety-related. The MOVs are powered by Class 1E dc power.

- For long-term recirculation operation, the RNS pumps take suction from only one of the two sump recirculation lines. Unrestricted flow through both parallel paths (one containing an MOV and a squib valve in series, the other containing a check valve and a squib valve in series) is required for success of the sump recirculation function when both RNS pumps are running. If one of the two parallel paths fails to open, operator action (in the control room through PMS) is required to manually throttle the RNS discharge MOV (V011) to prevent pump cavitation. Emergency response guidelines provide guidance for aligning the RNS pumps for long-term recirculation.

- With the RNS pumps aligned either to the IRWST or the containment sump, the pumps' NPSH is adequate to prevent pump cavitation and failure even when saturation of the IRWST or sump inventory occurs.

- The following AP1000 design features contribute to the low likelihood of interfacing system LOCAs through the NRHR system:

  - The portion of the RNS outside containment is capable of withstanding the operating pressure of the RCS.

  - Each RNS line is isolated by at least three valves.

  - Interlocking of the pump suction isolation valves, connecting the RNS pumps to the RCS hot leg, with RCS pressure prevents opening of the valves until the RCS pressure is less than 3.10 MPa (450 psig). This prevents overpressurization of the RCS when the RNS is aligned for shutdown cooling.

  - A relief valve located in the common RNS discharge line outside containment provides protection against excess pressure.

  - The two remotely operated MOVs connecting the suction and discharge headers, respectively, to the IRWST are interlocked with the isolation valves connecting the RNS pumps to the hot leg. This prevents inadvertent opening of any of these two MOVs when the RNS is aligned for shutdown cooling and potential diversion and draining of reactor coolant system.

  - The operability of the RNS is tested, via connections to the IRWST, immediately before its alignment to the RCS hot leg, for shutdown cooling, to ensure that there are not any open manual valves in the drain lines.

- The reliability of the IRWST suction isolation valve (V023) to open on demand (for RNS injection during power operation and for IRWST gravity injection via the RNS hot leg connection during shutdown operation) is important. The IRWST suction isolation valve (V023) is included in the D-RAP.

- During cold shutdown and refueling conditions with the RCS open, RNS V-023 provides an alternative gravity injection path. The COL applicant will have policies that maximize

the availability of this valve and procedures to open this valve during cold shutdown and refueling operations when the RCS is open and the PRHR cannot be used for core cooling. This is COL Action Item 19.1.8.9.

- Performance of planned maintenance affecting the RNS cooling function and its support systems will occur in Modes 1, 2 and 3 when the RNS is not normally operating.

- Since inadvertent opening of RNS valve V024 results in a draindown of RCS inventory to the IRWST and requires gravity injection from the IRWST, the COL applicant will have administrative controls to ensure that inadvertent opening of this valve is unlikely. This is COL Action Item 19.1.8-10. This error will be taken into account in the control room design. This is COL Action Item 19.1.8-11.

- The RNS is an important "defense-in-depth" system for accidents initiated while the plant is at power or at mid-loop during shutdown. The RNS and its support systems (CCW, SWS and diesel generators) are RTNSS-important and their availability will be controlled.

19.1.8.17 Component Cooling Water System

The CCS is a non-safety-related system that removes heat from various components and transfers the heat to the service water system. The following are some important aspects of the CCS as represented in the PRA:

- The CCS is arranged into two trains. Each train includes one pump and one heat exchanger.

- During normal operation, one CCS pump is operating. The standby pump alignment will create an automatic start in case of a failure of the operating CCS pump.

- Loading of the CCS pumps on the standby diesel generator is automatic in the event of a loss of normal ac power. The CCS, therefore, continues to provide cooling of required components if normal ac power is lost.

19.1.8.18 Service Water System

The SWS is a non-safety-related system that transfers heat from the component cooling water heat exchangers to the atmosphere. The following are some important aspects of the SWS as represented in the PRA:

- The SWS is arranged into two trains. Each train includes one pump, one strainer, and one cooling tower cell.

- During normal operation, one SWS train of equipment is operating. The alignment of the standby pump ensures an automatic start in case of a failure of the operating SWS pump.

- Loading of the SWS pumps and cooling tower fans onto their associated standby diesel bus is automatic in the event of a loss of normal ac power. Both pumps and cooling tower fans automatically start after power from the diesel generator is available.

19.1.8.19 Chemical and Volume Control System

The chemical and volume control system (CVS) provides a safety-related means to accomplish the following tasks: (1) terminate inadvertent RCS boron dilution and (2) preserve containment integrity by isolation of the CVS lines penetrating the containment. In addition, the CVS provides a non-safety-related means to perform the following functions: (1) provide makeup water to the RCS during normal plant operation, (2) provide boration following a failure of reactor trip, and (3) provide coolant to the pressurizer auxiliary spray line.

The following are some important aspects of CVS as represented in the PRA:

- The CVS has two makeup pumps and each pump is capable of providing normal makeup.

- The configuration is such that one CVS pump operates on demand while the other CVS pump is in standby. The operation of these pumps will alternate periodically.

- The two safety-related air-operated valves provide isolation of normal CVS letdown during shutdown operation on low hot leg level.

- The safety-related PMS boron dilution signal automatically re-aligns CVS pump suction to the boric acid tank. This signal also closes the two safety-related CVS demineralized water supply valves. This signal actuates on reactor trip signal (interlock P-4), source range flux doubling signal, or low input voltage to the Class 1E dc power battery chargers.

- The COL applicant will maintain procedures to respond to low hot leg level alarms. This is COL Action Item 19.1.8-12.

19.1.8.20 Startup Feedwater System

SFW pumps provide a non-safety-related means of delivering feedwater to the SGs when the main feedwater pumps are unavailable during a transient. This capability provides an alternate core cooling mechanism to the PRHR heat exchanger for non-LOCA or SGTR accidents which minimizes the PRHR challenge rate. The SFW pumps are included in the D-RAP.

19.1.8.21 Passive Containment Cooling System

Flooding of the PCS annulus because of plugging of the upper annulus drains is a potential mechanism for the failure of PCS cooling. The probability of plugging is minimized in the design by including the following: (1) two 100 percent drains in the side wall of the shield building, with protective screens to prevent entry of small animals into the drains, and (2) a

technical specification requirement to perform surveillance of the annulus floor and drains every two years to identify and to eliminate debris that can potentially plug the drains.

19.1.8.22 Containment Isolation System

DAS, in addition to PMS, controls containment isolation valves in lines that represent risk-significant release paths to further limit offsite releases following core melt accidents. These lines are: containment purge supply and exhaust, and normal containment sump. D-RAP includes the containment isolation valves controlled by DAS as risk-significant SSCs. Short term availability controls for DAS address the operability of DAS actuation of these isolation valves.

19.1.8.23 Reactor Cavity Flooding System

The AP1000 design includes a safety-related reactor cavity flooding system to prevent reactor vessel breach and ex-vessel phenomena in the event of a severe accident. The following design features comprise the system:

- two 20.3 cm (8 in.) diameter recirculation lines that provide a path for gravity draining the IRWST to the reactor cavity,

- a squib valve and a motor operated valve in each recirculation line, each powered from the Class 1E dc power supply, and actuated from the control room, and

- a reactor vessel thermal insulation system designed specifically to enhance RPV cooling, as described in Section 19.2.3.3.1 of this report.

Included as risk-significant SSCs within D-RAP are the containment recirculation squib valves and isolation MOVs, and containment recirculation screens.

In-Service Inspection and Testing Programs provide surveillance and maintenance requirements on the related piping and valves.

Specific guidelines are given for the operator action to flood the reactor cavity. Emergency Response Guideline AFR.C-1 instructs the operator to flood the reactor cavity if injection to the RCS cannot be recovered or containment radiation reaches levels that indicate fission product releases as determined by a core damage assessment guideline.

Key aspects of the reactor cavity flooding system will be confirmed by ITAAC.

19.1.8.24 RPV Thermal Insulation System

The AP1000 design includes a reflective reactor vessel insulation system that provides an engineered flow path to allow the ingression of water and venting of steam for externally cooling the vessel in the event of a severe accident involving core relocation to the lower plenum. Key attributes of the insulation system are:

- RPV/insulation panel clearances, water entrance and steam exit flow areas, and loss coefficients derived from the ULPU Configuration V tests with proto-typical RPV insulation,

- the entrance and exit of the insulation boundary incorporate water inlets and steam vents that open because of buoyant forces during cavity flood-up, and

- insulation panels and support members designed to withstand the pressure differential loading associated with the ERVC boiling phenomena, as determined from the UPLU Configuration V tests.

There are no applications of coatings to the outside surface of the reactor vessel that will inhibit the wettability of the surface.

A metal grating covers the opening between the vertical access tunnel and the RCDT room that will prevent any large pieces of debris from entering the reactor cavity.

The doorway between the reactor cavity compartment and the RCDT room includes a normally-closed damper. The design of this damper enables it to open passively during containment flood-up to permit flooding of the reactor cavity from the RCDT room, and continued water flow through the opening.

The COL applicant will complete the design of the reactor vessel insulation system. This will include the final design and sizing of the water inlets and outlets, RPV/insulation clearances and water/steam flow areas using ULPU Configuration V test data, and structural analysis of the reactor vessel insulation panels and support members using hydrostatic and dynamic load information derived from ULPU Configuration V test data.

The reactor vessel insulation system and the damper between the reactor cavity and the RCDT room are included as risk-significant SSCs in the reliability assurance program, and key aspects of the as-built system will be confirmed by ITAAC.

19.1.8.25 Reactor Cavity Design for Direct Containment Heating

The reactor cavity and RPV arrangement provide no direct flow path for the transport of particulated molten debris from the reactor cavity to the upper containment regions.

19.1.8.26 Reactor Cavity Design for Ex-Vessel Fuel-Coolant Interactions

The design can withstand a best-estimate ex-vessel steam explosion without loss of containment integrity.

19.1.8.27 Reactor Cavity Design for Core Concrete Interactions

The AP1000 is designed for in-vessel retention of molten core debris, however, the reactor cavity design incorporates features that extend the time to basemat melt-through in the event of RPV failure. The cavity design includes:

- a minimum floor area of 48 m^2 for spreading of the molten core debris
- a minimum thickness of concrete above the embedded containment liner of 2.8 ft (0.85 m)
- there is no buried piping in the concrete beneath the reactor cavity, and no enclosed sump drain lines in either the reactor cavity floor or reactor cavity sump concrete. Thus, there is no direct pathway from the reactor cavity to outside the containment in the event of core concrete interactions.
- a 24-inch high curb encompassing the cavity sump, with a number of sleeved, small diameter openings through the curb at floor level that will permit water to drain into the sump, but will solidify molten core debris before it enters the sump. Thus, there is no direct pathway for core debris to enter the sump.

The specifications do not include a specific type of concrete for use in the basemat.

19.1.8.28 Hydrogen Igniter System

The AP1000 design includes a hydrogen igniter system to limit the concentration of hydrogen in the containment during severe accidents. The features of the system are:

- 64 glow plug igniters distributed throughout the containment
- powered from the non-safety-related onsite ac power system, but also capable of being powered by offsite ac power, onsite non-essential diesel generators, or non Class 1E batteries via dc-to-ac inverters.
- manually actuated from the control room when core exit temperature exceeds 1200F, as an initial step in ERG AFR.C-1 to ensure that the igniter activation occurs before rapid cladding oxidation.

The igniter system is non-safety-related but is subject to investment protection short-term availability controls.

The AP1000 design also includes two non-safety-related PARs located within the containment. The PARs are provided for defense-in-depth protection against the buildup of hydrogen following a design basis loss of coolant accident. Although the PARs are expected to function to reduce combustible gas concentrations during severe accidents as well, they are not credited in the PRA.

19.1.8.29 Protection of Containment from Diffusion Flames

The containment layout prevents the formation of diffusion flames that can challenge the integrity of the containment shell. Specifically:

- the openings from the passive injection system (PXS) and CVS compartments that can vent hydrogen to the CMT room are either away from the containment wall and electrical penetration junction boxes, or covered by a secure hatch,
- IRWST vents near the containment wall are oriented to direct releases away from the containment shell, and
- IRWST vents near the containment wall are equipped with louvers that are normally closed, and designed to open at higher differential pressures than the IRWST pipe vents, and then reclose under their own weight when the differential pressure is reduced.

The above provisions will be confirmed by ITAAC. The IRWST vents will also be included within the scope of D-RAP.

Operation of ADS stage 4 or operation of the IRWST louvered vents will preferentially direct the hydrogen releases to a more central location within containment, where diffusion flames would not adversely impact the containment.

19.1.8.30 Non-safety Containment Spray

The AP1000 design includes a non-safety grade containment spray system with the capability to supply water to the containment spray header from an external source in the event of a severe accident. Loss of ac power does not contribute significantly to the core damage frequency, therefore, non-safety-related containment spray does not need to be ac independent. The COL applicant will develop and implement severe accident management guidance for use of the non-safety containment spray system as part of COL Action Item 19.2.5-1 regarding the severe accident management program.

19.1.8.31 Containment Vent

In the event of a severe accident that results in gradual containment pressurization, it is possible to vent the AP1000 containment. The COL applicant, as part of COL Action Item 19.2.5-1 regarding the severe accident management program, will identify the specific penetration(s) to be used for containment venting and develop and implement severe accident management guidance for venting containment using the framework provided in WCAP-13914, Revision 3.

19.1.8.32 Accident Management

The COL applicant will develop and implement severe accident management guidance and procedures using the framework provided in WCAP-13914, Revision 3 (see COL Action Item 19.2.5-1).

19.1.9 Conclusions and Findings

The NRC has evaluated the AP1000 design PRA quality (considering information received as of March 2003) and its use in the design and certification processes. The NRC expects to continue its interaction with the applicant in order to resolve the remaining open items listed in Section 19.1.10 of this report before making a final determination regarding the adequacy of the quality and completeness of the AP1000 PRA for its intended purposes, such as supporting the design and certification processes. However, based on current PRA information the NRC can tentatively conclude that the approaches used by the applicant for both the core damage and containment analyses are logical and sufficient to achieve the desired goals of describing and quantifying potential core damage scenarios and containment performance during severe accidents. The NRC also concludes that the use of PRA in the AP1000 design process helped improve the unique passive features of the design by better understanding plant response, including potential system interactions, during postulated beyond-design-basis accidents. Such features contributed to the reduced CDF and CCFP estimates of the AP1000 design when compared with operating PWRs. PRA results and insights were used to identify areas where it is particularly important to implement the certification and operational requirements assumed during the design and certification processes (e.g., ITAACs, RTNSS requirements, D-RAP, COL Action Items and Technical Specifications). The NRC expects that, following satisfactory resolution of open items listed in Section 19.1.10 of this report, it will be shown that the AP1000 design meets NRC's safety goals and represents an improvement in safety over operating PWRs in the United States.

19.1.10 Resolution of DSER Open Items

In reviewing the AP1000 PRA, the NRC staff has relied significantly on the similarity between the AP1000 and the AP600 designs (e.g., with respect to system design and functions, spatial arrangements and system capabilities) to reduce the review effort. This similarity allowed using the AP600 PRA as the starting point for the AP1000 PRA. The staff reviewed the quality of the PRA submittal by evaluating the models, techniques, methodologies, assumptions, data, and calculational tools that were utilized by the applicant. In addition, the staff reviewed the AP1000 PRA for completeness by comparing it with PRAs performed for current generation and advanced pressurized water reactor (PWR) designs to ensure that known safety significant PWR issues either do not apply to AP1000 design or they are appropriately modeled in the PRA. The staff has placed a special emphasis on PRA modeling of novel and passive features in the design as well as addressing issues related to these features, such as the issue of thermal-hydraulic (T-H) uncertainties and the reliability of digital I&C software.

Open, confirmatory and COL action items related to level 1 PRA for power operation (both internal and external events) are discussed in Section 19.1.10.1. Open, confirmatory and COL

action items related to shutdown operation (both internal and external events) are discussed in Section 19.1.10.2. Finally, open, confirmatory and COL action items related to levels 2 and 3 of the PRA for power operation are discussed in Section 19.1.10.3.

19.1.10.1 Level 1 PRA for Power Operation (Internal and External Events)

The staff's review of the quality of the level 1 PRA for operation at power relied, to the extent possible, on the similarity of the AP1000 design to the AP600 design previously certified by the staff. The first step has been to understand important differences between the two designs having the potential to impact the PRA models. The large power uprate resulted in a series of design and operational differences between the two designs (e.g., differences in sizes and capabilities of systems, differences in spatial arrangements of systems and design modifications to improve reliability). Once such differences were identified, the next step of the review was to examine what PRA models of the AP600 design were impacted and expected to be revised in the AP1000 design. The following step was to focus the review on those portions of the PRA models which were not previously reviewed by the staff. The final step was to ensure that the revised portions of the PRA did not impact other PRA areas and to look for any changes made in the AP600 PRA models and data beyond those needed to address issues related to the power uprate. The staff's review verified that the major impact of the design differences, between the AP600 and AP1000 designs, on the level 1 PRA models for power operation were related to (1) success criteria for safety systems and operator actions used in the PRA event trees and (2) spatial arrangements and size changes which impacted the external event analyses.

Based on the review of the various elements of the AP1000 level 1 PRA at power operation (e.g., accident sequence and system failure models, success criteria and failure data) and the review of the applicant's use of PRA results and insights to identify design certification requirements, the following issues were identified which the staff believes need additional attention by the applicant. Following the issuance of this draft report, the staff expects to interact with the applicant on the resolution of these issues.

19.1.10.1.1 Digital Instrumentation and Control

In Chapter 26 of the AP1000 PRA, a design option for the PMS in addition to the one modeled in the PRA is proposed. The option to use the Common Qualified Platform (Common Q) is proposed because of the rapid changes that are taking place in the digital computer and graphic display technologies employed in the modern human systems interface. The applicant assumes that the use of the Common Q option, in the place of the PRA PMS model, does not have any impact on the design certification process because such a process focuses upon the process used to design and implement instrumentation and control systems for the AP1000 rather than on the specific implementation. The staff requested the applicant (see RAI 720.035) to explain the process that will be used to verify that a PMS designed with the "Common Q" option will have equivalent or better reliability than the system modeled in the PRA and how the introduction of the "Common Q" option will affect important PRA-based insights about the PMS.

In its response to RAI 720.035, the applicant asserted that the PRA results are not sensitive to small changes in PMS failure probabilities and that the general architecture of the Common Q PMS is similar to that modeled in the AP1000 PRA. In addition, the applicant stated that the AP600 I&C functional requirements, which have received design certification, will be retained to the maximum extent compatible with the Common Q hardware and software. Also, it is stated that although the details of the AP1000 PRA model follow the AP600 design, the Common Q hardware and software provide a degree of redundancy that is equivalent to the redundancy modeled in the AP1000 PRA. However, the staff believes that further clarification of this issue is needed to ensure that the "Common Q" option will have the same or better reliability than the PMS design modeled in the PRA. A comparison of important features between the "Common Q" option and the PMS modeled in the PRA could help clarify this issue. This comparison should include features found by the PRA to be important contributors to the assumed high reliability of the PMS. Such a comparison, may identify the need for additional or different "design certification requirements" for the "Common Q" option" of PMS. This is Open Item 19.1.10.1-1.

19.1.10.1.2 PRA Input to Design Certification Process

An important objective of the AP1000 design certification PRA is to identify important PRA insights and assumptions and make sure that they are addressed in the design certification through "design certification requirements," such as requirements for ITAAC, the requirement for a D-RAP and COL action items. These requirements will be incorporated in the DCD to ensure that any future plant which references the design will be built and operated in a manner that is consistent with important assumptions made in the design certification PRA.

In its response to RAI 720.038, the applicant provided a preliminary and, recently, a revised list of "design certification requirements." The staff expects the final list of "design certification requirements" to be in agreement with the resolution of all open items identified in the AP1000 DSER. The staff is still reviewing the list of "design certification requirements" proposed by the applicant, especially in light of assumptions and insights related to differences in PRA models between the AP600 and AP1000 designs (e.g., differences in assumptions made in the fire risk analysis). The staff expects the applicant to continue providing requested information to ensure that all important assumptions made in the design certification PRA are appropriately included in the final list of design certification requirements. This is Open Item 19.1.10.1-2

19.1.10.1.3 PRA Input to RTNSS Process

An important objective of the AP1000 PRA is to provide risk-informed input to design certification regarding the need for regulatory oversight of certain non-safety-related systems (RTNSS). The same process used in the AP600 design certification is also used in the AP1000 design certification. The staff asked the applicant (see RAI 720.039) to use the results of the AP1000 PRA to provide input to the RTNSS process. Although the applicant has identified RTNSS systems (documented in WCAP-15985, "AP1000 Implementation of the Regulatory Treatment of Nonsafety-Related Systems Process," Revision 1, April 2003), the NRC staff does not have enough information to make a determination regarding the proper use of PRA results and insights in the RTNSS process.

The staff requested the applicant provide all steps in the process of using PRA results to identify non-safety-related systems for regulatory oversight as well as the type and level of such oversight. These steps are needed for the following reasons:

- show the link between the plant risk when only safety-related systems are credited in the PRA and the plant risk when the selected systems for regulatory oversight (including the type and level of such oversight) are credited in the PRA

- compare to the probabilistic criteria (safety goals, including the containment performance goal) documented in Section 19.1.7 of this report and SECY-94-084

- account for important uncertainties in the AP1000 PRA models (as stated in SECY-94-084). Examples of such uncertainties are discussed in the sensitivity studies documented in Section 19.1.3.1.5 of this report. In addition, the uncertainty in the large LOCA initiating event frequency assumed in the PRA (see RAI 720.027) and the uncertainty in the success criteria used for passive containment cooling by air flow (see RAI 720.030) should be addressed.

This information has not been provided by the applicant. This is Open Item 19.1.10.1-3

19.1.10.1.4 Impact of Uncertainties on PRA Results and Conclusions

The staff review has identified two AP1000-specific areas of uncertainty which individually, or collectively with other areas of uncertainty (e.g., uncertainty associated with failure probabilities of squib valves), have the potential to affect the PRA results and conclusions regarding the need for "certification requirements," such as ITAACs, RTNSS and COL action items. These uncertainties have also the potential to increase the number of "low margin risk significant" sequences which should be analyzed conservatively to bound thermal-hydraulic (T-H) uncertainty and determine success criteria for systems and operator actions. These two areas of uncertainty are discussed below.

One area of uncertainty is related to initiating event frequencies assumed in the PRA. The staff requested additional information (see RAI 720.027) about differences in initiating event category frequencies used in the AP600 and the AP1000 PRAs for large LOCAs and SGTR accidents. The applicant's response to RAI 720.027 did not address adequately the basis for the decrease of such initiating event frequencies which have a significant impact on the PRA results. For the large LOCA category, the applicant states that in the AP1000 PRA "operating experience" data reported in NUREG/CR-5750 for pipe breaks were used. However, the NUREG/CR-5750 data rely on expert opinion and include significant uncertainty. In addition, since NUREG/CR-5750 was published additional information (e.g., Davis Besse finding) is available. For SGTR events, the frequency used in the AP1000 PRA is based on a more recent calculation that was performed in conjunction with a replacement steam generator project which is proprietary to the applicant. The staff believes that the impact of uncertainties on PRA results and insights, associated with the frequencies of large LOCAs and SGTR accidents assumed in the AP1000 PRA, needs to be investigated and addressed appropriately by the design certification process.

A second area of uncertainty is related to the success criteria assumed in the AP1000 PRA for passive containment cooling by air flow. The AP1000 PRA event trees include a top event for containment cooling (event CHR). It is stated that *"For success paths that result in steam release to the containment, the success of containment cooling (PCS or RNS) is modeled. If containment cooling is successful, then the path ends in an OK state. If PCS water cooling is not successful, then the path goes to a special OK end state to allow containment integrity sensitivity studies to be made."* This "special OK" end state is labeled "late containment failure (LCF)" end state and defined as an end state *"...where the containment heat removal by either passive containment cooling system (PCS) or component cooling water (CCS) heat exchangers via normal residual heat removal (RHR) fails."* The staff requested clarification (see RAI 720.030) about the meaning of the "special Ok" status. The applicant responded that a sensitivity study shows that even if the LCF state is considered to be a core damage, the plant CDF would increase by only 29 percent. The staff needs further information regarding the impact of this assumption on the focused PRA, where no credit is taken for the non-safety-related systems, and on the RTNSS process.

The impact of these two areas of uncertainty on the results of the PRA, including the PRA results used in the RTNSS process, should be addressed in the design certification process. This is Open Item 19.1.10.1-4.

19.1.10.1.5 Success Criteria and Thermal-Hydraulic Uncertainty

Event tree paths that do not result in core damage are identified. These success paths, utilize the minimum sets of equipment necessary to meet the success criteria for systems and operator actions needed to mitigate accidents and prevent core damage. The success criteria are described in Section 6.2 of the PRA to be those conditions necessary to ensure that the critical safety functions are maintained. These critical safety functions are:

- Decay heat removal (core cooling)
- RCS inventory control
- RCS pressure control
- Reactivity control
- Containment heat removal and containment isolation

The discussions in this section describe the thermal-hydraulic basis for success paths to ensure that the first 4 critical safety functions are maintained. The basis for ensuring that success paths for maintaining the containment heat removal and containment isolation function is discussed in Section 19.2.4 of this report.

For AP1000 the applicant lists the minimum sets of equipment necessary to mitigate various plant failure events at power in Table 6-1 of the PRA. These are the minimum sets of equipment that ensure that the critical safety functions will be met. Justifications for success are referenced for each case. Many of the justifications are based on analyses using the computer codes that are used to verify the design basis in the DCD. These design basis codes have been reviewed by the NRC staff as discussed in Chapter 21.6 of this report. These codes include LOFTRAN for transients and ATWS analysis, WCOBRA/TRAC for LBLOCA and long-

term cooling analysis and NOTRUMP for SBLOCA analysis. Other justifications are based on AP600 analyses and analyses for AP1000 using the MAAP4 computer code which the staff has not reviewed but which has been benchmarked against NOTRUMP results for AP600 as discussed in WCAP-14869 "MAAP4/NOTRUMP Benchmarking to Support the Use of MAAP4 for AP600 PRA Success Criteria Analysis" dated April 1997. The staff's evaluation of MAAP4 analyses for the AP1000 PRA is described in the following paragraphs.

The occurrence of an ATWS event will be unlikely at AP1000 reactors since the plants will be equipped with a diverse actuation system (DAS) in addition to the reactor protection system. For the PRA the applicant performed thermal-hydraulic analyses of ATWS events assuming both reactor trip actuation systems failed. Analyses were performed for a loss of feedwater event which was determined to be the limiting ATWS precursor for AP600. The applicant utilized the LOFTRAN computer code which has been approved by the NRC staff for analysis of loss of feedwater events (see Section 21.6 of this report). These analyses demonstrated that the ASME emergency stress limits will not be exceeded once the core fuel burnup reaches an equilibrium so that the core moderator reactivity coefficient will always be less than -12.5 pcm/^{O}F. For the first cycle the core moderator coefficient was determined to be in excess of -10.0 pcm/^{O}F for 40 percent of the cycle time. Under these conditions the ASME emergency stress limits might be exceeded. The NRC staff has determined that the consequences of ATWS have been adequately calculated for AP1000 using LOFTRAN and the results are acceptable to use in the PRA since Westinghouse has used approved methodology.

Large break LOCA thermal-hydraulic analyses are described in Chapter 15 of the DCD as part of the design basis for AP-1000. These analyses are performed using the WCOBRA/TRAC computer code. For the PRA the applicant performed additional large break LOCA analysis of a double-ended cold leg break and inadvertent ADS stage 4 valve actuation. Unlike the DCD analyses, containment isolation was assumed to have failed. All four ADS stage 4 valves were assumed to operate whereas only three ADS stage 4 valves were assumed to operate for the Chapter 15 design basis. These analyses are acceptable for use to determine success criteria for systems and operator actions used in the PRA.

Long-term cooling following a LOCA is analyzed by the applicant as discussed in DCD Tier 2 Chapter 15. These analyses are also performed using the WCOBRA/TRAC computer code. For the PRA, the applicant performed additional long-term cooling analyses of double-ended DVI line breaks with and without containment isolation. DVI line breaks represent a limiting condition for long-term cooling since one train of injection water would be spilled on the floor. The applicant assumed all four ADS stage 4 valves to be operable for the case when containment isolation was assumed to have failed. A single failure of one ADS stage 4 valve is assumed with containment isolation successful. Use of WCOBRA/TRAC for long-term cooling analysis requires that the initial conditions, passive safety systems performance and, containment conditions be input from other calculations. For the DCD analyses these inputs are generated by the NOTRUMP and the WGOTHIC computer codes. The NRC staff review of these computer codes is described in Section 21.6 of this report. For the two additional long-term cooling analyses that the applicant performed for the PRA, the initial conditions and other inputs to WCOBRA/TRAC were obtained from analyses using MAAP4. This input includes the reactor system water mass and distribution at the beginning of IRWST injection, the

containment pressure during the analysis, and the injection from the passive systems. The NRC staff has not reviewed MAAP4 for long-term cooling analysis. The NRC staff requires that computer codes which it has reviewed be utilized to provide inputs to WCOBRA/TRAC as is done in the design basis analyses or that the applicant submit the appropriate MAAP4 models for staff review. This concern has been transmitted to the applicant for resolution.

In addition to the issue involving use of MAAP4 input with WCOBRA/TRAC, the NRC staff has requested other justification for the minimum equipment sets listed by Westinghouse in Table 6-1 of the PRA. The applicant has agreed to supply the additional requested information. This additional information is to include the following:

- Justification that a large break LOCA can be mitigated if one of the two CMTs fail.

- Justification that adequate water can be maintained within the containment to provide for long term core cooling if containment isolation fails.

- Justification that one of the two startup feedwater pumps can deliver adequate water to the two SGs following an ATWS event.

- There are 12 references to AP600 PRA sections as the basis for determining success. The applicant needs to justify in each case that the evaluations performed for AP600 are applicable to AP1000.

- As discussed in the response to RAI 720.025, the applicant assumes that 30 minutes of core cooling is available following a small break LOCA, steam generator tube rupture or transient with no CMT or accumulator injection. The 30 minutes is based on MAAP4 calculations for AP600 and MAAP4 calculations for AP1000 but with fewer failures. The NRC staff has requested that appropriate calculations be performed for AP1000 using a computer code which the NRC staff has reviewed.

The issue of T-H uncertainties rises from the “passive” nature of the safety-related systems used for accident mitigation. Passive safety systems rely on natural forces, such as gravity, to perform their functions. Such driving forces are small compared to those of pumped systems and the uncertainty in their values, as predicted by a "best-estimate" T-H analysis, can be of comparable magnitude to the predicted values themselves. Therefore, some accident sequences with frequency high enough to impact results, which are not predicted to lead to core damage by a "best-estimate" T-H analysis, may actually lead to core damage when T-H uncertainties are considered in the PRA models. T-H uncertainties and their impact on PRA models are being considered in the certification of the AP1000 design using the same approach that was used in the AP600 design certification.

The applicant utilized the MAAP4 code for many of the analyses of small and medium LOCA events sequences to address the issue of T-H uncertainties. The applicant has been using MAAP4 for PRA analyses rather than NOTRUMP, which is the design basis analysis code, since many computer runs are required and MAAP4 runs much faster than NOTRUMP.

The applicant has not submitted the MAAP4 code for NRC staff review therefore, the staff can not directly accept the results of analyses using MAAP4. During the AP-600 review the applicant submitted WCAP-14869 which provides benchmark studies with the NOTRUMP code for a series of small and medium LOCA event sequences. As discussed in NUREG-1512, the staff found that, in most cases MAAP4 and NOTRUMP predicted similar trends for system behavior in the base cases and sensitivity analyses. On the basis of the benchmark study comparisons, the staff determined MAAP4 to be an adequate screening tool for addressing T-H uncertainties and determining PRA success criteria for the AP600, subject to certain limitations as discussed in WCAP14869. The applicant evaluated the limitations discussed in the topical report and concluded that MAAP4 could be used as a screening tool for evaluating PRA success criteria for AP1000. The staff agrees with this conclusion with the limitation that those success paths that give marginal results with MAAP4 or utilize minimum sets of equipment should be verified using a computer code which the NRC staff has reviewed. The MAAP4 code uses a number of nonphysical models for the thermal/hydraulic conditions within the reactor system. These models are controlled by input provided by the code analyst to obtain the desired result. MAAP4 therefore does not provide a rigorous solution of reactor system conditions during transient and accidents. Thus, the results need to be confirmed using more rigorous methods as discussed in Open Item 19.1.10.1-5 below.

During the AP600 PRA evaluation, the NRC staff requested the applicant to evaluate the thermal/hydraulic uncertainty in the calculational results used in the PRA including those from MAAP4 code. Rather than performing detailed uncertainty evaluations, the applicant chose to perform a set of bounding calculations using NOTRUMP and WCOBRA/TRAC. The bounding calculations were made conservative by use of an elevated core decay heat equivalent to 1.2 times the 1971 ANS standard. These bounding analyses for AP600 are described in WCAP-14800 “AP600 PRA Thermal/Hydraulic Uncertainty Evaluation for Passive System Reliability,” dated June 1997. The applicant took this same approach for AP1000. Bounding calculations for AP1000 are described in Appendix A to the AP1000 PRA.

As described in Appendix A to the PRA, the applicant performed detailed event tree analyses to determine those event sequences which could not be judged to have either assured success (OK end states) or probable failure, success being defined as not producing extensive core damage or large offsite radiation release. The assured success paths consist of those sets of equipment assumed available for the design basis and failures determined to be less severe for the reactor system than those of the design basis. Some of the event sequences which were given an OK end state by the applicant have not yet been properly justified using a computer code which the staff has reviewed. Those include the following sequences:

- Sequences that assume failure of one of the four ADS stage #4 valves and also assume failure of containment isolation.

- Large break LOCA sequences that assume failure of one of two CMTs.

In addition to the OK sequences, other events were judged to have an uncertain outcome (UC end states) because the failures which were assumed were beyond design basis or MAAP4 analyses indicated an extended time of core uncovery. The UC end states were judged to be

candidates for further verification by performing bounding analyses using NOTRUMP and WCOBRA/TRAC. A listing of the UC end states and reference to the bounding analyses demonstrating success was provided by Westinghouse in Table A.5.1.2 of Appendix A to the PRA. Not all of the sequences producing UC end states are shown to be bounded. Those sequences which have not been bounded involve extensive equipment failures so that the contribution to the overall risk from these sequences is very low. The unbounded sequences therefore have no effect on the conclusions of the PRA.

As part of the AP1000 PRA review the NRC staff performed audit calculations for the applicant's NOTRUMP and MAAP4 analyses. The staff utilized the RELAP5 computer code. RELAP5 is an advanced thermal/hydraulic simulation tool developed by the staff. The RELAP5 core model is somewhat more detailed than in NOTRUMP or MAAP4 in that a hot rod was modeled having a higher heat flux than the average core. The same set of failures was assumed by the staff as by the applicant. The following three cases were run. The first two cases compare NOTRUMP with RELAP5 predictions while the third case compares MAAP4 with RELAP5 predictions.

Case #1 (The applicant identifies this sequence as Case A in Appendix A to the PRA) involves the following: 3.0 inch hot leg break; both CMT fail to inject; one of two accumulators inject; complete failure of ADS-1,2,3; manual actuation of ADS-4; containment isolation fails; decay heat at 1.2 times the 1971 ANS standard.

Case #2 (The applicant identifies this sequence as Case C in Appendix A to the PRA) involves the following: double ended DVI line break; one CMT fails to inject; both accumulators fail to inject; complete failure of ADS-1,2,3; one of 4 ADS-4 valves fails closed; the PRHR heat exchanger is blocked; containment isolation fails; decay heat at 1.2 times the 1971 ANS standard.

Case #3 involves the following: 3.5 inch hot leg break; one accumulator fails to inject; one of 4 ADS-4 valves fails closed; containment isolation fails.

The RELAP5 results resembled those from NOTRUMP both in the timing of events and in consequences. Both NOTRUMP and RELAP5 predicted a limited amount of core uncovery for the two cases analyzed. The amount of core uncovery was insufficient however, to cause core heating beyond accepted limits. The staff agrees with the applicant that the event sequences analyzed by NOTRUMP and RELAP5 are success for the PRA. Furthermore, the results demonstrate the robust design of the AP1000 for small break LOCA mitigation since even with many multiple failures excessive core heating does not occur.

For the MAAP4 - RELAP5 comparison, both codes predicted that the core remained covered for the case analyzed. The timing of events was different in the two analyses. RELAP5 predicted a faster rate of reactor depressurization than did MAAP4 however, MAAP4 predicted earlier ADS stage #4 valve actuation. MAAP4 predicted sudden changes in break flow compared to RELAP5. The sudden changes in break flow are likely the result of simplifying assumptions in MAAP4 which permit the code to run rapidly. The differences in code results

demonstrate the need to benchmark MAAP4 results against those from a more sophisticated analytical method such as NOTRUMP.

In conclusion, the applicant has utilized a systematic approach in categorizing success paths for the PRA for the purpose of minimizing the number of analyses needed to justify success. In many cases the MAAP4 code was used to identify the limiting sequences. To justify that the limiting sequences provide for adequate core cooling, the applicant has performed bounding analyses using conservative computer codes that the NRC staff has reviewed for design basis accidents. In some instances the NRC staff has identified limiting sequences that have not been bounded. Other sequences have not been analyzed for AP1000 but success has been inferred by the applicant from analyses performed for AP600. These deficiencies are an open item in the AP1000 DSER.

The deficiencies are listed below with reference to the NRC staff RAI where the issue was first raised:

(a) Additional justification in needed for long-term cooling analyses for which the initial and boundary conditions were obtained from analyses using MAAP4 for input into WCOBRA/TRAC (RAI 720.013)

(b) Additional justification should be provided that a large break LOCA can be mitigated if one of the two CMTs fail (RAI 720.012-2)

(c) Additional justification should be provided that adequate water can be maintained within the containment to provide for long term core cooling if containment isolation fails (RAIs 720.021 and 720.024)

(d) Additional justification should be provided that one of the two startup feedwater pumps can deliver adequate water to the two steam generators following an ATWS event (RAI 720.024)

(e) Additional justification should be provided that evaluations made for AP600 are appropriate to be used in the AP1000 PRA Table 6-1 and in the response to RAI 720.025 where the applicant assumes that 30 minutes of core cooling is available following a small break LOCA, steam generator tube rupture or transient with no accumulator injection (RAIs 720.024 and 720.025)

(f) Additional justification should be provided that sequences which assume failure of one of the four ADS stage 4 valves and also assume failure of containment isolation, will end in successful core cooling (RAIs 720.012-1,4, 720.009 and 720.017).

This is Open Item 19.1.10.1-5.

19.1.10.1.6 Fire-Specific Operator Actions

The fire PRA identified the following two fire-specific operator actions:

(1) Operator action to switch off the electrical power for each division in case of fire to avoid spurious action of valves

(2) Operator action to manually actuate a valve to allow fire water to reach the automatic fire suppression system in containment maintenance floor (fire area 1100 AF 11300B)

The COL applicant will develop procedures for implementing these fire-specific operator actions. This is a COL action item in the AP1000 DSER and Open Item 19.1.10.1-6.

19.1.10.2 Level 1 PRA for Shutdown Operation (Internal and External Events)

The staff's review of the quality of the AP1000 Shutdown PRA relied on the staff's familiarity and review of the AP600 shutdown PRA. The AP600 shutdown PRA was used as the starting point to develop the AP1000 PRA due to similarity between the two designs. (No fault trees were developed specifically for the AP1000 shutdown model.) The staff's review focused on how the PRA covered the risk impact of AP1000 design changes and the risk impact of shorter response times for operator actions given higher decay heat loads at shutdown.

Based on the review of the various elements of the AP1000 shutdown PRA (e.g., initiating event frequencies, event trees, success criteria and human error probabilities) and the review of the applicant's use of PRA results and insights to identify design certification requirements, the staff identified the following issues which need additional attention by the applicant. Following the issuance of this draft report, the staff expects to interact with the applicant on resolving these issues.

19.1.10.2.1 Shutdown Risk due to Vacuum Refill Operations

The applicant stated that the shutdown risk due to vacuum refill operations are included in the calculation of shutdown risk during vented drained conditions. The staff is reviewing the applicant's response to RAI 720.99 (dated 3/28/03 and 4/12/03) to determine if the shutdown risk due to vacuum refill operations is included in the calculation of shutdown risk during vented drained conditions. The staff noted during their review of the applicant's response to RAI 720.99 that investment protection short term availability controls do not include RNS and its support systems such as component cooling water system, service water system, and ac power supplies during vacuum refill operations. Assuming an extended loss of RNS during vacuum refill operations, the staff questions using the RNS suction relief valve to relieve RCS pressure should the operators not open the ADS valves. The operators may instead isolate the RNS suction relief valve to isolate RCS leakage. This is Open Item 19.1.10.2-1.

19.1.10.2.2 Dominant Shutdown Accident Sequences

The applicant did not report the dominant shutdown accident sequences in the AP1000 shutdown PRA. The staff requests Westinghouse to report the dominant shutdown accident sequences in the AP1000 shutdown PRA. This is Open Item 19.1.10.2-2.

19.1.10.2.3 Shutdown Risk Importance Analysis

As requested by the staff in the follow up to RAI 720.38, Westinghouse did not provide any importance analyses (such as risk achievement and risk worth) in their response to RAI 720.38 (dated 03/28/03 and 4/12/03). This is Open Item 19.1.10.2-3.

19.1.10.2.4 Shutdown PRA Sensitivity Studies

The staff will confirm that the results of the sensitivity studies (including cutsets) are documented into the AP1000 Shutdown PRA . This is Open Item 19.1.10.2-4.

In the bases of AP1000 TS, there is no discussion that planned maintenance of these three systems should be avoided during cold shutdown. The frequency and duration of IRWST, ADS, and RNS maintenance performed by a future COL holder has considerable uncertainty. Therefore, the staff asked the applicant to perform a sensitivity study assuming minimal compliance with AP1000 TS. This sensitivity study provides an upper bound of the shutdown CDF assuming the COL holder chooses to always perform planned maintenance on one IRWST injection path and recirculation path, two ADS stage 4 valves, and RNS valve V-23 during cold shutdown. The shutdown CDF for this sensitivity study increases to 2.2E-06 per year (a factor of ten higher than the full power CDF). Since no cutsets were submitted in the RAI response for this sensitivity study, this documentation issue is considered part of Open Item 19.1.10.2-4

19.1.10.2.5 Documentation of Shutdown Focused PRA Results

The “focused” PRA shutdown CDF was estimated to be 1.23E-6. Over eighty five percent of the risk resulted from a loss of offsite power during drained conditions and during non-drained conditions. Some of the dominant cutsets have the basic event IWX-MV-GO1. In the early versions of the AP600 PRA, the basic event, IWX-MV-GO1, was used to model common cause failure of the 4 out of 4 IRWST injection motor operated valves (MOVs) to open. The later versions of the AP600 design and the AP1000 design changed the 4 MOVs to squib valves. In the AP 1000 design, the low pressure squib valves (120 A/B) in the recirculation lines were changed to high pressure squib valves. In preparing the AP600 cutset file for use as the starting point in creating the AP1000 shutdown mode, the basic event IWX-MV-GO1 was changed to, IWX-EV-SA, common cause failure of IRWST squib valves. This basic event has a failure probability of 2.6E-5. As a follow-up to RAI 720.38, the staff needs to understand why basic event IWX-MV-GO1 appears in the “Focused PRA” cutsets for the AP1000 design. The staff also needs a list of basic events and their description for the AP1000 shutdown model. This is Open Item 19.1.10.2-5.

19.1.10.2.6 Shutdown Fire Risk Evaluation

The applicant submitted the AP1000 shutdown fire risk evaluation on 3/28/03. The AP1000 fire risk analysis has a different grouping of fire areas and different combustible loadings than the AP600 shutdown fire risk evaluation. Therefore, the adequacy of the AP1000 shutdown fire risk evaluation is still being reviewed by the staff. This is Open Item 19.1.10.2-6.

19.1.10.2.7 Shutdown Flooding Risk Evaluation

During staff review of RAI response 720.38, the staff noted some math errors that increase the shutdown CDF from internal floods to 4E-9 per year. Flooding scenario number 6, a rupture of the 20.3 cm (8 in.) fire main extension that fails RNS during drained conditions, appears to have been mis-calculated. This is Confirmatory Item 19.1.10.2-1.

19.1.10.3 Levels 2 and 3 PRA

The staff's review of the quality of the AP1000 Level 2 and 3 PRA relied on the similarity of the AP1000 design and PRA to that for the previously certified AP600, and on the staff's familiarity with the AP600 design and PRA. The review considered the impact of design and operational differences between the two designs on the PRA models and risk insights, as well as how the important containment challenges for AP600 are addressed in the AP1000 design.

The review verified that: (1) the impact of these differences on factors such as decay heat level, accident progression, containment and RPV loads, containment pressure capacity, system success criteria (e.g., for external reactor vessel cooling), and accident source terms are appropriately addressed in the AP1000 PRA, and (2) the risk levels and risk insights for the two designs are substantially the same. The latter conclusion is due in part to a number of design enhancements in AP1000 that address features or challenges important to risk, most notably, refinements in the reactor vessel insulation system to promote external reactor vessel cooling at the higher decay heat levels for AP1000, the addition of louvers to the IRWST vents along the containment wall to reduce the potential for diffusion flames, and the addition of a third, diverse PCS injection line to improve the reliability of PCS.

Based on the review of the various elements of the AP1000 Level 2 and 3 PRA, the following issues were identified that the staff believes need additional attention by the applicant. Following the issuance of this draft report, the staff expects to interact with the applicant on resolving these issues.

19.1.10.3.1 Representative Sequences for Assigning Source Terms

The accident sequences used to represent the various release categories are identified and briefly described in PRA Chapter 45. Additional sequence information is provided in PRA Chapter 34. The basis for selecting the representative sequence for each release category is not provided. Such information is necessary in order to confirm that the sequence selected to represent each release category is reasonably representative of the collection of sequences assigned that category, in terms of the magnitude, timing, energy, and elevation of release. Based on the limited information that was provided, the staff noted a number of inconsistencies. Specifically, for release category CFE releases from the ADS Stage 4 valves enter directly into containment rather than into the IRWST, and given the location of the valves relative to the containment shell, would not result in containment failure from diffusion flames as assumed in the PRA. For release category CFL containment failure is assumed at 3 hours, which is inconsistent with the time frame for late containment failure. Also, important details impacting the release characteristics need to be documented, such as whether an additional

decontamination factor is credited in determining the source term for SGTR events (as it was in AP600), and the containment isolation failure location and size assumed for containment isolation sequences. This is Open Item 19.1.10.3-1.

19.1.10.3.2 Major Contributors to System Failures

The major causes of reactor cavity flooding failure and hydrogen igniter failure in AP1000 have not been provided. Such information is useful for identifying major contributors to system failure and confirming that reasonable measures have been taken to reduce risk. The staff will request that the applicant provide this information for AP1000. This is Open Item 19.1.10.3-2.

19.2 Severe Accident Performance

19.2.1 Introduction

The purpose of Section 19.2 is to evaluate the approach proposed by the applicant for resolving severe accident issues for the AP1000 design and determine whether the criteria in SECY-93-087, SECY-96-128, SECY-97-044 and the corresponding SRMs dated July 21, 1993, January 15 and June 30, 1997, respectively, have been met.

To provide adequate protection of the public health and safety, current NRC regulations require conservatism in design, construction, testing, operation, and maintenance of nuclear power plants. A defense-in-depth approach has been mandated in order to prevent accidents from happening and, if accidents should occur, to mitigate their consequences. Siting in less populated areas is emphasized. Furthermore, the NRC, State, and local governments mandate emergency response capabilities to provide additional defense-in-depth protection to the surrounding population.

The reactor and containment systems design are a vital link in the defense-in-depth philosophy. Current reactors and containments are designed to withstand a LOCA and to comply with the siting criteria of 10 CFR Part 100 and general design criteria of Appendix A to 10 CFR Part 50. The large-break LOCA and other accidents analyzed in accordance with the NRC's SRP are documented in Chapters 6 and 15 of the AP1000 DCD Tier 2.

The high-level of confidence in the defense-in-depth approach results, in part, from stringent requirements for meeting the single failure criterion, redundancy, diversity, quality assurance, and utilization of conservative models. The staff concludes that existing requirements ensure a safe containment design.

The NRC also has requirements to address conditions beyond the traditional design-basis spectrum, such as anticipated transients without scram (10 CFR 50.62), SBO (10 CFR 50.63), and combustible gas control (10 CFR 50.44); however, a definitive set of regulatory requirements for addressing specific severe accident phenomena does not exist. However, an assessment of the severe accident response of a proposed design provides useful insights regarding its response to accidents of extremely low likelihood that are beyond the plant design basis. Existing regulations that require conservative analyses and inclusion of features for

design-basis events provide margin for severe accident challenges. This design-basis margin coupled with regulatory guidance to address severe accidents in the form of policy positions ensures a robust design that satisfies the Commission's policy statement on severe accidents.

19.2.2 Deterministic Assessment of Severe Accident Prevention

19.2.2.1 Severe Accident Preventive Features

The design of the AP1000 copes with plant transients and LOCAs without any adverse impact on the environment. However, the potential does exist, albeit remote, for a LOCA or seemingly ordinary plant transient coupled with numerous plant failures to progress to a severe accident with the potential for substantial offsite releases. Such potential is seen through the use of PRA methods.

Accident initiators are separated into two general groups: transients and LOCAs. Transients include planned reactor shutdowns and transients that result in reactor scrams. Examples of transients are manual shutdown, steamline or feedline break, LOOP, and loss of feedwater. In addition to these transients, there is an entire spectrum of LOCAs that are accident initiators. LOCAs fall into three categories: small, medium, and large, dependent on the size of the line break.

Following the accident initiator, normal and emergency plant systems respond to control reactivity, reactor pressure, reactor water level, steam generator water level, and containment parameters within the design-bases spectrum. Of most importance is to ensure inventory control and sufficient heat removal from the core to prevent overheating and subsequent fuel damage. Failure to provide heat removal or inventory control results in core uncovery, fuel overheating, and the potential for oxidation and melting of the reactor core.

In response to accident initiators identified through operating reactor experience and performance of probabilistic risk assessments, the NRC developed criteria for ALWRs to prevent the occurrence of such initiators from leading to a severe accident. In SECY-93-087 the staff specifies these criteria and includes design provisions for the following: anticipated transients without scram, mid-loop operation, SBO, fires, and ISLOCA.

19.2.2.1.1 Anticipated Transients Without Scram

An ATWS is an anticipated operational occurrence followed by the failure of the trip portion of the RPS. Anticipated operational occurrences are those conditions of normal operation that are expected to occur one or more times during the life of the nuclear power plant and include, but are not limited to, loss of power to reactor coolant pumps, tripping of the turbine generator set, isolation of the main condenser, and loss of all offsite power. Depending on the transient and its severity, the plant may recover and continue normal operation, or the plant may require an automatic shutdown (scram) via the RPS. The RPS is designed to safely shut down the reactor to prevent core damage.

These transients, when coupled with a failure of the RPS, may lead to conditions beyond what some plants were originally designed to meet. In these cases, the reactor must be manually scrammed in order to avoid reactor fuel damage or coolant system damage. Subsequent failure of the manual scram system and inadequate core cooling would lead to core damage.

Transients with the greatest potential for significant damage to the reactor core and containment are those that lead to an increase in reactor pressure and temperature, a loss of feedwater, or a failure of the RPS to scram the reactor. During an ATWS event, reactor power, pressure, and temperature must be controlled or the potential exists for a severe accident.

In SECY-93-087, the staff indicated that it was evaluating the passive designs to ensure compliance with Commission regulations and guidance regarding ATWS. Regulations to address ATWS were promulgated in 10 CFR 50.62. The Commission issued further guidance in its SRM of June 26, 1990, which stated that diverse scram systems should be provided. However, the Commission also directed that the staff should accept an applicant's alternative to the diverse scram system, if the applicant can demonstrate that the consequences of an ATWS are acceptable.

As described in Section 7.7.1.11 of the AP1000 DCD Tier 2, the AP1000 has a DAS. The staff's evaluation of the DAS to meet the requirements of 10 CFR 50.62 is contained in Sections 7.7.2 and 15.2.9 of this report. On the basis of the staff's evaluation of the DAS to meet the requirements 10 CFR 50.62, the staff concludes that the AP1000 design conforms to the ATWS criteria specified in SECY-93-087.

19.2.2.1.2 Mid-Loop Operation

During refueling or maintenance activities, the reactor coolant system is sometimes reduced to a "mid-loop" level. During this period, the potential exists for loss of decay heat removal capability as a result of air entrainment of the RHR pumps. In SECY-93-087, the staff indicates that all passive plants must have a reliable means of maintaining decay heat removal capability during all phases of shutdown activities, including refueling and maintenance. Westinghouse summarizes the specific AP1000 design features that address mid-loop operations in DCD Tier 2 Section 5.4.7.2.1. Availability controls for the normal heat removal system (RNS) during mid-loop operations have been provided in Table 16.3-2, "Investment Protection Short-Term Availability Controls," of the DCD Tier 2. On the basis of the staff's evaluation in Section 19.3, "Shutdown Evaluation," and Chapter 22, "Regulatory Treatment of Non-safety Systems," of this report and the additional availability controls provided for the RNS during normal and reduced inventory in Table 16.3-2 of the DCD Tier 2, the staff concludes that the AP1000 design conforms to the mid-loop operation criteria specified in SECY-93-087. Short term availability controls are evaluated in Chapter 22 of this report.

19.2.2.1.3 Station Blackout

An SBO involves the complete loss of ac electric power to the essential and nonessential switchgear buses in a nuclear power plant (i.e., a LOOP concurrent with turbine trip and unavailability of the onsite emergency ac power system).

In accordance with SECY-90-016, the evolutionary designs provided a large-capacity, alternate ac power source with the capability to power one complete set of normal safe-shutdown loads. However, the AP1000 does not rely on active systems for safe shutdown following an event. The AP1000 design has redundant non-safety-related onsite ac power sources (diesel generators) to provide electrical power for the non-safety-related active systems that provide defense-in-depth. In SECY-93-087, which expanded on the guidance given in SECY-90-016, the staff indicated that it believed that the diesel generators might require some regulatory treatment.

The staff outlined the process for resolving the RTNSS in Commission Policy paper SECY-94-084, dated March 28, 1994. This process includes a combination of probabilistic and deterministic criteria to identify risk-significant, non-safety-related systems. The staff evaluated non-safety-related ac power sources relative to these criteria in Section 8.5.2.3 of this report. Additional availability controls have been provided for the electrical power systems in Table 16.3-2, "Investment Protection Short-Term Availability Controls," of the DCD Tier 2. On the basis of the staff's evaluation in Section 8.5.2.1, "Station Blackout," of this report and the additional availability controls provided in Table 16.3-2 of the DCD Tier 2, the staff concludes that the AP1000 design conforms to the SBO criteria specified in SECY-93-087, and is therefore, acceptable. Short term availability controls are evaluated in Chapter 22 of this report.

19.2.2.1.4 Fire Protection

The Commission concluded that fire protection issues that have been raised through operating experience and the External Events Program must be resolved for passive LWRs. In SECY-93-087, the staff recommended that the Commission approve the position that the passive plants be reviewed against the enhanced fire protection criteria specified for evolutionary designs in SECY-90-016. The Commission, in an SRM dated June 26, 1990, subsequently approved this position. In an SRM dated July 21, 1993, the Commission approved the staff's position for passive plants and asked to be kept informed of the staff's resolution of the issue related to common-mode failures through common ventilation systems. A description of the AP1000's fire protection system is in DCD Tier 2 Section 9.5.1 and the fire protection analysis is contained in DCD Tier 2 Appendix 9A. The staff's acceptance of the AP1000 fire protection systems relative to the criteria in SECY-93-087 is discussed in Section 9.5.1 of this report.

19.2.2.1.5 Intersystem Loss-of-Coolant Accident

ISLOCAs are defined as a class of LOCAs in which a breach occurs in the interface of the RCS pressure boundary with a system of lower design pressure. The breach may occur in portions of piping located outside of the primary containment, causing a direct and potentially unisolable discharge from the RCS to the environment. An ISLOCA is of concern because of potential direct releases to the environment, loss of core cooling, and loss of core makeup. An ISLOCA occurs when high pressure is introduced to a low-pressure system as the result of valve(s) failure or an inadvertent valve actuation. In either case, the overpressurization can cause the low-pressure system or components to fail.

In SECY-93-087, the staff recommended that the Commission approve the position that the passive plants be reviewed for compliance with the ISLOCA criteria approved in the Commission's SRM of June 26, 1990, relating to SECY-90-016. In an SRM dated July 21, 1993, the Commission approved the staff's position for passive plants.

In SECY-90-016, the staff recommended that designs reduce the possibility of a LOCA outside containment by designing (to the extent practicable) all systems and subsystems connected to the RCS to an ultimate rupture strength (URS) at least equal to the full RCS pressure. The "extent practicable" phrase is a realization that all systems must eventually interface with atmospheric pressure and that for certain large tanks and heat exchangers, it would be difficult or prohibitively expensive to design such systems to a URS equal to full RCS pressure. The staff further recommended that systems that have not been designed to withstand full RCS pressure should include the following attributes: (a) the capability for leak testing of the pressure isolation valves, (b) valve position indication that is available in the control room when isolation valve operators are de-energized, and (c) high-pressure alarms to warn control room operators when rising reactor coolant pressure approaches the design pressure of attached low-pressure systems and both isolation valves are not closed.

The staff evaluated the issue of ISLOCA for AP1000, relative to the criteria of SECY-90-016, as part of its resolution of Generic Safety Issue 105 in Section 20.3 of this report. The staff concludes that the AP1000 design conforms to the ISLOCA criteria specified in SECY-90-016.

19.2.3 Deterministic Assessment of Severe Accident Mitigation

19.2.3.1 Overview of the AP1000 Containment Design

The AP1000 primary containment design is a freestanding cylindrical steel vessel with ellipsoidal upper and lower heads. The steel vessel is 4.76 cm (1.875 in.) thick and has a design pressure of 508 kPa (59 psig). The vessel has an inner diameter of 39.62 m (130 ft) and net free volume of 58,333 m^3 (2,060,000 ft^3). The design basis leak rate is 0.10 weight percent per day of the containment air mass at the DBA peak pressure. A seismic Category 1 reinforced concrete shield building surrounds the containment.

The design provides passive containment cooling in case the normal containment fan coolers are not available or an accident has occurred that requires containment heat removal at elevated pressures and temperatures. The PCS is a safety-related system that removes heat directly from the containment vessel and transmits it to the environment. The PCS uses the steel containment vessel as a heat transfer surface. The surrounding concrete shield building is used, along with a baffle, to direct air from the top-located air inlets down to a lower elevation of the containment and back up along the containment vessel. A 2,858 m^3 (755,000 gallon) water storage tank is supported by the shield building to allow gravity drain of the water exterior to, and on the top of the steel containment vessel. Indications of inadequate containment cooling, such as high containment pressure or temperature, automatically initiate the PCS water flow. These signals open valves to initiate the flow of water onto the top of the containment vessel. The air and the evaporated water exhaust through an opening in the roof of the shield building.

19.2.3.2 Severe Accident Progression

A description of the processes, both physical and chemical, that may occur during the progression of a severe accident, and how these phenomena affect containment performance, follows in this section. Due to the complex processes involved there will be potential variability in the postulated core melt progression scenarios. Assessments reported previously in NUREG/CR-5132, NUREG/CR-5597, and NUREG/CR-5564 provide generic insights that are also applicable to the AP1000 design. The following is a summary of the accident progression information applicable to the AP1000 response to postulated severe accident scenarios.

Severe accident progression can be divided into in-vessel and ex-vessel phases. The in-vessel phase generally begins with insufficient decay heat removal and can lead to melt-through of the reactor vessel. The ex-vessel phase involves the release of the core debris from the reactor vessel into the containment, which results in phenomena such as core-concrete interaction, fuel-coolant interaction, and direct containment heating.

19.2.3.2.1 In-Vessel Melt Progression

In severe accidents that proceed to vessel failure and release of molten core material into the containment, the 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 encompasses the phenomena and processes involved in a severe core damage accident starting with core uncovery and initial heatup, and continuing until either of the following occurs: (a) stabilization and cooling of the degraded core within the reactor vessel, or (b) breach of the reactor vessel occurs and molten core material is released into the containment. The phenomena and processes in the AP1000 that can occur during in-vessel melt progression include:

- core heatup resulting from loss of adequate cooling,
- metal-water reaction and cladding oxidation,
- eutectic interactions between core materials,
- melting and relocating cladding, structural materials, and fuel,
- formation of blockages near the bottom of the core as a result of the solidification of relocating molten materials (wet core scenario),
- drainage of molten materials to the vessel lower head region (dry core scenario),
- formation of melt pool, natural circulation heat transfer, crust formation, and crust failure (wet core scenario), and
- reactor vessel breach from a local failure or global creep-rupture.

Removal of decay heat produced by the core must take place in order to achieve adequate core cooling and prevent initiation of a severe accident. In the event that all of the safety-related and non-safety-related systems fail to remove the decay heat, the core will heat up to the point at which damage to the fuel and fuel cladding may occur. Transfer of decay heat is through the radiative, conductive, and convective heat transfer to the steam, other core materials, and non-fuel materials within the reactor. The insufficient cooling supply results in coolant boiloff and a decreasing level within the reactor vessel as the decay heat generation exceeds the heat removal rate. The coolant level within the core further decreases so that the fuel rods above the coolant level cool only by rising steam. The fuel rods begin to overheat and cladding oxidation in the presence of steam begins at high temperatures. Generation of hydrogen and additional heat occurs as the cladding oxidizes in the presence of steam. A zirconium alloy called Zircaloy makes up the fuel cladding for AP1000. The initial Zircaloy oxidation involves oxygen diffusion through a ZrO_2 surface layer. As the fuel rods continue to heat up from decay heat and the exothermic zirconium oxidation reaction occurs, the expectation is that materials within the reactor with low melting points will melt first and may form eutectics. Eutectics are mixtures of materials with a melting point lower than that of any other combination of the same components.

Zircaloy, with a melting point of 1,757 °C (3,194 °F), begins to melt during a severe accident, breaking down the protective ZrO_2 layer, which exposes unoxidized Zircaloy. Following this, local melting of the fuel rods may cause changes in the core geometry resulting in differing steam flow paths. This can lead, on the one hand, to an increase in the oxidation process as access to the unoxidized Zircaloy becomes available; on the other hand, the melt formation or changes in the steam flow path could reduce the Zircaloy surface available for oxidation and thereby decrease the overall reaction process. In some accident scenarios in which residual amounts of water remain in the bottom of the core and lower plenum, substantial steaming and oxidation can take place.

In addition to oxidation, the potential exists for the Zircaloy to interact with the UO_2 fuel, forming low-melting-point eutectics. Formation of eutectics may decrease the effective surface area for oxidation and the overall oxidation rate. The melting point of Zircaloy depends on its state and lattice structure. Zircaloy has three melting points: 1,877 °C (3,410 °F) (beta-Zr), 1,977 °C (3,590 °F) (alpha-Zr(O)), and 2,677 °C (4,850 °F) (ZrO_2). When partially oxidized Zircaloy is in contact with UO_2, an alpha-Zr(O)/UO_2-based eutectic will form with a liquefaction temperature of approximately 1,897 °C (3,446 °F). Therefore, in the presence of good fuel/cladding contact, fuel liquefaction and melt relocation will commence around this temperature. This has the potential to affect the oxidation behavior of Zircaloy-based melt.

Various severe fuel damage (SFD) test programs sponsored by the NRC indicate that the oxidation of the Zircaloy is largely controlled by the availability of a steam supply and that high rates of hydrogen generation can continue after melt formation and relocation. Some of these experiments indicate that the majority of the hydrogen generation occurred after onset of Zircaloy melting and fuel dissolution. In steam-rich experiments, oxidation took place over most of the fuel bundle length and most of the hydrogen generation occurred early. For steam-starved experiments, oxidation was limited to local regions of the fuel bundle, and the majority of the hydrogen generation occurs after the onset of Zr/UO_2 liquefaction and relocation.

Hydrogen production and accumulation during a severe accident may represent challenges to the containment in numerous ways, including deflagration, detonation, and pressurization, as hydrogen gas is non-condensible. The AP1000 containment has 64 hydrogen igniters to consume hydrogen as it is produced during a severe accident, thereby introducing the potential for hydrogen detonation events that would challenge containment integrity.

The SFD tests indicated the potential for incoherent melt-relocation as a result of non-coherent temperatures within the test bundles. This is because of the different core materials present with a wide range of melting points and eutectic temperatures. Formation of eutectics would result in a nonuniform melting and relocation process. Further differences in the melt-relocation process can be attributed to asymmetric bundle heating that can increase upon Zircaloy oxidation. This process begins when one area of the fuel bundle is initially at a temperature higher than the other areas. The higher temperature Zircaloy will consume the available steam through oxidation at a quicker rate. The oxidation reaction increases the hotter areas to even higher temperatures, which further increases the oxidation rate and the local temperatures. This autocatalytic nature of Zircaloy oxidation appears to contribute to asymmetric bundle heatup and the potential for incoherent melt relocation behavior.

As the temperature of the core increases, vaporization and release of some fission products occur. Steam and/or hydrogen then carry these fission products throughout the primary system where they are subject to deposition on the surfaces of internal components. The deposition mechanisms include condensation on the heat sinks (diffusiophoresis) , gravitational settling, and thermophoresis. The fission products that are not deposited remain airborne and are released to the containment, where the dominant removal mechanisms are gravitational settling and diffusiophoresis.

The core melt progression, including relocation and fission product release, becomes increasingly difficult to predict as it continues to degrade. The core melt could relocate into the lower reactor vessel plenum. If water is present in the lower plenum, the potential exists for in-vessel steam explosions, where molten core rapidly fragments and transfers its energy, causing rapid steam generation and shock waves. Once in the lower plenum, the potential exists to halt the core melt progression through external vessel cooling. The AP1000 is designed to flood up the reactor cavity with water from the IRWST, thereby providing cooling of the core debris through the reactor vessel.

The in-vessel core melt progression, including core degradation, relocation, and failure of the reactor vessel, contains considerable uncertainty. This uncertainty includes the following:

- the potential for in-vessel steam explosion (see Section 19.2.3.3.5.1 of this report),
- the interaction between core debris and internal vessel structures,
- the potential for external vessel cooling of core debris (see Section 19.2.3.3.1 of this report),
- the time and mode of vessel failure,

- the composition of the core debris released at vessel failure,
- the amount of in-vessel hydrogen generation,
- the in-vessel fission-product release and transport, and
- retention of fission products and other core materials in the RCS.

19.2.3.2.2 Ex-Vessel Melt Progression

The following conditions affect ex-vessel severe accident progression:

- the mode and timing of the reactor vessel failure,
- the primary system pressure at reactor vessel failure,
- the composition, amount, and character of the molten core debris expelled,
- the type of concrete used in containment construction, and
- the availability of water to the reactor cavity.

The initial response of the containment from 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 by design features, early containment failure mechanisms and bypass usually dominate risk consequences. Early containment failure mechanisms result from energetic severe accident phenomena, such as high pressure melt ejection with direct containment heating and ex-vessel steam explosions. The long-term containment pressure and temperature response from ex-vessel severe accident progression is largely a function of an interaction between molten core and concrete, known as core-concrete interaction (CCI), and the availability of mechanisms to remove heat from the containment.

At high RCS pressures, ejection of the molten core debris from the reactor vessel could occur in jet form, causing fragmentation into small particles. The potential exists for the core debris ejected from the vessel to be swept out of the reactor cavity and into the upper containment. Finely fragmented and dispersed core debris could heat the containment atmosphere and lead to large pressure spikes. In addition, chemical reactions of the core debris particulate with oxygen and steam could add to the pressurization loads. Hydrogen, pre-existing in the containment or produced during direct containment heating, could ignite adding to the loads on the containment. This phenomena is known as high pressure melt ejection with direct containment heating.

Reactor vessel failure at high or low pressure coincident with water present within the reactor cavity may lead to interactions between fuel and coolant with the potential for rapid steam generation or steam explosions. Rapid steam generation involves the pressurization of containment compartments from nonexplosive steam generation beyond the capability of the

containment to relieve the pressure so that the containment fails because of local overpressurization. Steam explosions involve the rapid mixing of finely fragmented core debris with surrounding water resulting in rapid vaporization and acceleration of surrounding water creating substantial pressure and impact loads.

The eventual contact of molten core debris with concrete in the reactor cavity will lead to CCI. Such interaction will lead to a decomposition of concrete and can challenge the containment by various mechanisms, including: (a) pressurization as a result of the production of steam and noncondensible gases to the point of containment rupture, (b) the transport of high-temperature gases and aerosols into the containment leading to high-temperature failure of the containment seals and penetrations, (c) containment liner melt-through, (d) reactor support structures melt-through leading to the relocation of the reactor vessel and tearing of containment penetrations, and (e) the production of combustible gases such as hydrogen and carbon monoxide. CCI is affected by many factors, including the availability of water to the reactor cavity, the containment geometry, the composition and amount of core debris, the core debris superheat, and the type of concrete involved.

19.2.3.3 Severe Accident Mitigative Features

19.2.3.3.1 External Reactor Vessel Cooling (ERVC)

The AP1000 design incorporates ERVC as a strategy for retaining molten core debris in-vessel in severe accidents. The objective of ERVC is to remove sufficient heat from the vessel exterior surface that the thermal and structural loads on the vessel (from the core debris which has relocated to the lower head) do not lead to failure of the vessel. By maintaining RPV integrity, the potential for large releases due to ex-vessel severe accident phenomena (i.e., ex-vessel FCIs and CCI) is eliminated. A residual challenge to containment from hydrogen combustion remains, but it diminishes with successful ERVC since combustible gas production would be limited to in-vessel hydrogen generation. ERVC will remove some decay heat through the RPV in design basis LOCAs (which result in a flooded reactor cavity as a direct consequence of the sequence), but in the absence of loss of core cooling and core debris relocation, this heat removal is insignificant and is not credited in design-basis accidents. This section provides the results of the staff's review of the ERVC strategy for the AP1000.

Background

The AP1000 design includes several features that enhance ERVC relative to operating plants, specifically: (1) safety-grade systems to provide RCS depressurization and reactor cavity flooding, (2) a "clean" lower head that is unobstructed by in-core instrument lines or other penetrations, and (3) a RPV thermal insulation system which limits thermal losses during normal operations, but provides an engineered pathway for supplying water cooling to the vessel and venting steam from the reactor cavity during severe accidents. The AP1000 design further enhances the ability to flood the reactor cavity by a containment and reactor cavity arrangement which permits the RCS inventory (breakflow) to drain to the cavity, in addition to the manually-actuated cavity flooding system.

ERVC is credited with preventing RPV failure in the AP1000 PRA on the basis of a DOE-sponsored analysis by the University of California, Santa Barbara (UCSB) using the Risk Oriented Accident Analysis Methodology (ROAAM). The UCSB analysis of ERVC, documented in DOE/ID-10460, "In-Vessel Coolability and Retention of a Core Melt", July 1995 (Peer Re-Review Version) and October 1996 (Final), concluded that thermally-induced failure of an AP600-like reactor vessel is "physically unreasonable" provided the RCS is depressurized and the RPV is submerged in water to a depth of at least the top of the debris pool. Based on AP1000-specific testing and analyses (and resulting modifications to the AP1000 insulation design), this work was extended to the AP1000 design, and, similar to the AP600 PRA, sequences with successful RCS depressurization and reactor cavity flooding are assigned zero probability of vessel breach, and sequences with either inadequate RCS depressurization or reactor cavity flooding are assumed to fail the reactor vessel and containment in the AP1000 PRA.

Staff review of ERVC centered on 3 major areas including: (1) the likelihood of achieving RCS depressurization and reactor cavity flooding in the AP1000 design, both of which are required for successful ERVC, (2) the likelihood of maintaining RPV integrity given successful RCS depressurization and reactor cavity flooding, and (3) system-related considerations and design requirements for the cavity flooding system and the RPV thermal insulation system. The results of the review are provided below.

19.2.3.3.1.1 Likelihood of Achieving Requisite Conditions for ERVC in AP1000

Both RCS depressurization and reactor cavity flooding are required for successful ERVC. Important considerations include the manner in which these conditions are defined in the PRA success criteria, the potential for the RCS to be depressurized automatically or by manual backup of ADS, and the potential for the reactor cavity to be flooded passively by gravity draining or by manual actuation of the cavity flooding system.

The AP1000 PRA defines the success criteria for ERVC as: (1) depressurization of the RCS to below 150 psi before RCS pressure boundary challenge, and (2) flooding of the reactor cavity to a level above the reactor vessel nozzle gallery (98-ft elevation) prior to the time at which core debris would relocate to the lower head, vaporize the water in the lower head, and reheat to the point of melting additional structures. Each of these critera is discussed below.

19.2.3.3.1.1.1 RCS Depressurization

RCS depressurization can occur as a result of the initiating event (e.g., a large LOCA), or operation of the safety-grade ADS. In the event that automatic actuation of the ADS does not occur, manual actuation is addressed in Emergency Response Guidelines and credited in the PRA. In the Level 1 PRA, the majority of Level 1 sequences (about 90 percent) involve events with at least partially successful RCS depressurization and relatively low RCS pressure (<1.03MPa (150 psig)) at the time of core uncovery. For high pressure core melt sequences, the potential to depressurize the RCS in the time period between the onset of core damage and challenge of the RCS pressure boundary is further evaluated in the Level 2 event trees. After credit for late depressurization, an even larger fraction of the core melt sequences (about

95 percent) are estimated to involve a depressurized RCS before the time of substantial core damage.

The RCS pressure associated with successful ERVC in the PRA (i.e., 1.03 MPa (150 psig) or less) is greater than the RCS pressure assumed in the baseline analysis in the UCSB study for AP600 (the UCSB study assumed a fully depressurized RCS). However, a supplemental structural analysis is provided in Appendix G of the UCSB report which illustrates that there is margin in the load carrying capacity of a thinned RPV (with 5 cm (1.97 in.) wall thickness) at an elevated pressure of 2.76 MPa (400 psig). The supplemental analysis considers the effect of vessel creep under high temperature and elevated pressure, and concludes that there is margin in the load carrying capacity of the vessel shell.

The pressure challenge to RPV lower head integrity for AP1000 is greater than in AP600 due to the higher decay heat level and core mass in AP1000. The higher decay heat level results in greater heat flux through the RPV lower head relative to AP600 and further thinning of the RPV wall in the region of maximum heat flux. The larger core mass results in an increased dead-load that must be carried by the thinned RPV wall. In Section 39.4 of the PRA, the applicant provided an assessment of the RPV wall thickness available to carry the internal loading in the portion of the vessel conducting heat at the peak critical heat flux, where maximum thinning occurs. The analysis indicates that the portion of the vessel wall available to carry the load (at a wall temperature less than the yield strength temperature of 900°K (1645°R)) is approximately 0.8 cm (0.31 in.) thick. Given the mass of the AP1000 core and RPV internals, and the offsetting buoyancy forces on the vessel associated with a fully-flooded reactor cavity, this wall thickness is 36 times the minimum thickness required to carry the dead load.

Although significant, this margin can be eroded by residual pressure or pressure pulses within the RCS, such as might occur during late-phase core relocation or reflood of the molten core debris pool. For example, an internal pressure of 6.89 kPa differential (1 psid) within the RPV would be roughly equivalent to the dead load on the lower head (i.e., the weight of the core debris less the buoyancy force), and a pressure of 241 kPa differential (35 psid) would be sufficient to eliminate the estimated margin to failure in the thinned wall. In response to RAI 720.45, the applicant provided additional analyses of the RCS pressures during representative severe accident sequences, and the maximum RCS pressurization that would occur during reflood of a molten debris bed. This information indicates that the RCS is essentially fully depressurized in relevant severe accident sequences due to the lack of steam generation and the available discharge area through the open ADS valves, and that the maximum RCS pressurization during reflood would be limited to about 152 kPa differential (22 psid), given the available discharge area through open ADS valves or In-containment IRWST spargers. Based on this assessment, vessel reflood is not predicted to fail the weakened vessel due to pressurization by steam.

The staff notes that the assessment of RCS pressurization during reflood is based on steaming rates from the flat plate critical heat flux and an assumption that molten fuel and coolant do not interact energetically. These assumptions are considered reasonable given the high surface temperatures of the molten debris pool and the large density differences between water and molten core debris, both of which would tend to produce film boiling. Although the potential for

energetic interactions cannot be ruled out, the likelihood of such interactions will be minimized in AP1000 by COL Action Item 19.2.5-1 regarding the severe accident management program. As part of COL Action Item 19.2.5-1, the COL applicant will develop and implement severe accident management guidance on reflooding a damaged core retained in-vessel.

The staff concludes that for sequences that are considered depressurized in the PRA (and are also successfully flooded as described below), RPV structural integrity will be maintained. Thus, the success criteria for RCS pressure as applied in the AP1000 PRA is acceptable.

19.2.3.3.1.1.2 Reactor Cavity Flooding

On the basis of an assessment of the timing of core debris relocation and associated uncertainties, the applicant rationalized that the RPV lower head would not be thermally challenged until core debris would relocate to the lower head, vaporize the water in the lower head, and reheat to the point of melting additional structures. Based on a review of accident progression analyses for AP1000, Westinghouse estimated that debris bed dryout and reheat would not occur until 70 minutes after the core exit temperature first exceeds 648.9°C (1200°F). Successful IRWST injection is necessary to meet this criterion because CMT and accumulator water inventories alone are not adequate to achieve the necessary water level. Accordingly, the long-term reactor cavity water level corresponding to successful ERVC in the PRA is approximately 32.6 m (107 ft), which completely covers the RPV hot leg and cold legs. This final level is consistent with the containment water level simulated in tests performed by the University of California in the ULPU facility, which form the basis for the exterior heat transfer coefficients employed in the ERVC analysis for AP1000.

An assessment of reactor cavity flooding rates presented in Chapter 39 of the PRA indicates that with both cavity flood (recirculation) lines open, the Elevation 98' is reached within about 30 minutes of opening the valves, and with one line open the same elevation is reached within about 50 or 65 minutes of opening the valves, depending on whether the less restrictive or the more restrictive of the two flooding lines is used. Thus, in the most limiting scenario the operator has about 5 minutes to open the cavity flood valves after high core exit temperatures signal the need for cavity flooding within emergency response guideline. The operator instructions to flood the cavity have been moved from the end of ERG AFR.C-1 (in AP600) to the entry of the procedure (in AP1000) to achieve the water depths and flooding times required for successful ERVC in AP1000. This procedure is entered when core exit temperatures exceed 648.9°C (1200°F).

In the quantification of human error probabilities, the PRA assigns a probability of 0.003 to failure to recognize the need to flood the reactor cavity and open the valves in 1 of 2 lines to flood the cavity within a 20-minute time window. This probability is reasonable for AP1000 if either: both flooding lines function (in which case 40 minutes would be available for operator action) or only the less restrictive of the two flooding lines functions (in which case 20 minutes is available for operator action). The assumed human error probability is optimistic for the most limiting situation in which only the more restrictive flooding line (5 minutes for operator action) is available. However, a sensitivity study performed by Westinghouse shows that increasing this

probability by a factor of 10 (for all flood line combinations) would increase the containment failure frequency by only about 30 percent (from 1.9E-8/y to 2.6E-8/y).

The effectiveness of reactor cavity flooding was confirmed by Westinghouse through MAAP calculations for selected sequences for each accident class in the PRA. These calculations, documented in Chapter 34 of the PRA, indicate that the cavity would be passively flooded before or at the time of onset of oxidation in many sequences (although not to a level sufficient to provide long-term cooling), and approximately 70 minutes or more typically exists to manually flood the cavity.

The staff performed limited calculations using the MELCOR code to confirm the general nature of core melt progression in the AP1000. Although these calculations revealed some significant differences in predicted behavior, the code comparisons confirm the order and approximate timing of major events in the accident progression, and the overall thermal hydraulic behavior during the accidents analyzed. Of particular note is the MELCOR calculation for the frequency-dominant sequence that would require manual actions to flood the reactor cavity (the 3BE sequence). The MELCOR calculation indicates that there would be approximately 75 minutes between the onset of rapid core oxidation and the first relocation of core debris into the lower head. The time between core exit temperatures exceeding 648.9°C (1200°F) and debris bed dryout will be substantially greater. These results confirm that there is margin implicit in the Westinghouse success criterion for cavity flooding. In view of this confirmation, the staff concludes that the Westinghouse characterization of melt progression and the time available for manual actions, which forms the basis for assessing the likelihood of successful operator action in the PRA, is reasonable and acceptable.

In the baseline PRA, adequate reactor cavity flooding is achieved in about 98 percent of the sequences. About half of the core damage events require operator actuation of the cavity flooding system to ensure successful cavity flooding, but the remaining half would adequately flood as a direct consequence of the accident progression, even without manual actions. The availability of the power sources, availability of the valves, ability of the operator to diagnose the situation, and success of the operator are all considered in the fault tree used to quantify the failure probability of cavity flooding. Since the system fault trees are linked to the containment event tree (CET), the availability of power sources is treated consistently for all sequences in the CET.

In summary, the staff concludes that the success criteria for RCS depressurization and reactor cavity flooding is appropriate, and that the safety-related systems for RPV depressurization and reactor cavity flooding provide high confidence that the requisite conditions for ERVC, i.e., a depressurized RCS and timely flooding of the reactor cavity, will be achieved in most core melt sequences. In those events where either condition is not met, the sequence is conservatively assumed to lead to containment failure in the AP1000 PRA. The staff, therefore, considers the PRA models and assumptions for estimating the likelihood of achieving the requisite conditions for ERVC, and the consequences of not achieving these conditions, to be acceptable.

19.2.3.3.1.2 Likelihood of Successful ERVC

The UCSB study for AP600 evaluated two debris configurations or debris/vessel contact modes that were considered to bound the thermal loads from all other debris configurations that can reasonably be expected to occur in the time period between the initial relocation event and the final steady state where essentially the entire core debris is contained in the lower head. One configuration was dominated by transient forced convection and jet impingement effects, and the other was dominated by natural convection in the final steady state. Analyses described in the UCSB report showed that vessel failure would not occur as a result of jet impingement. This was consistent with the staff's independent assessment of this threat. Thus, thermal loads to the vessel for the final steady state configuration were considered bounding and were analyzed in detail. Key aspects of the steady state configuration, termed the "Final Bounding State" or FIBS in the UCSB report, are: (1) fully-developed natural circulation of a homogeneous oxidic molten pool in the lower head of the RPV with an overlying metallic layer, (2) debris pool masses corresponding to relocation of essentially all of the core and most of the steel structures, (3) a depressurized RCS, and (4) heat transfer coefficients on the outside of the reactor vessel corresponding to a fully-flooded reactor cavity.

The technical treatment in the UCSB study for AP600 includes the following: (1) experimental data and correlations from tests conducted specifically to address ERVC for the AP600 design, including work carried out by UCSB to investigate boiling and critical heat flux in inverted, curved geometries (the ULPU experiments) and heat transfer from volumetrically heated pools and non-heated layers on top (the mini-ACOPO and MELAD experiments, respectively), (2) a detailed computer model to sample limited input parameters over specified uncertainty ranges, and to produce probability distributions of thermal loads and margins to departure from nucleate boiling at each angular position on the lower head, and (3) detailed structural evaluations that indicate that departure from nucleate boiling, i.e., heat flux in excess of critical heat flux (CHF), is a necessary and sufficient criterion for reactor vessel failure. The UCSB study concluded that thermally-induced failure of an AP600-like reactor vessel is "physically unreasonable" provided the RCS is depressurized and the vessel is submerged in water to a depth at least to the top of the debris pool. Additional conditions on the applicability of the UCSB conclusions are that the as-built reactor vessel thermal insulation system and RPV exterior coatings are in accordance with the system design and surface coatings evaluated in the prototypical testing carried out in the ULPU Configuration III tests, and that the insulation maintains its integrity under thermal-hydraulic loads associated with ERVC. RPV pressure loads associated with late reflood of the reactor vessel were not addressed as part of the UCSB analysis of ERVC.

The UCSB report was peer-reviewed by 17 internationally recognized experts in the fields of severe accidents, heat transfer, and structural mechanics. Numerous technical issues related to ERVC were identified and addressed as part of the peer review. The impact of these issues on the study conclusions was addressed as part of the peer review comment resolution process by performing sensitivity studies and additional evaluations to address the impact of these issues on the margins to failure. The results of the further assessments indicated that even when these issues are taken into consideration, the margins to failure are significant, and failure of the lower head is "physically unreasonable."

To assist in the NRC's evaluation of ERVC for AP600, parallel review efforts were undertaken by the NRC Office of Research (RES) and the Idaho National Engineering and Environmental

Laboratory (INEEL). The review included: (1) an in-depth review of the UCSB study and the model used to assess ERVC effectiveness, (2) an in-depth review of the peer review comments and their resolution to identify areas where technical concerns were not addressed, and (3) independent analyses to investigate the impact of residual concerns and parameter uncertainties on the margins to failure and conclusions presented in the UCSB report. The latter activity included performing steady-state analyses of the thermal loads associated with alternate debris bed configurations, including stratified intermediate states and inverted metallic and oxidic layers.

The review concluded that the UCSB study provides a comprehensive treatment of the concept of retaining the degraded core in-vessel through external cooling of the vessel wall, but identified the following as areas of concern:

- The potential to form a "stratified intermediate state" before final relocation of melt to the lower head. A stratified intermediate state, if formed, would result in a thinner metallic layer on top of the oxidic melt pool than the "final bounding state" evaluated in the UCSB study, and proportionally higher heat fluxes to the vessel wall.

- The potential for an inversion of the metallic and oxidic layers. An inversion of the layers, i.e., the metallic layer settling below the oxidic layer, would result in a different partitioning of the heat fluxes, and increased thermal loads on the bottom part of the vessel where heat removal capability CHF is at a minimum.

- The possibility of chemical interactions between the melt and the RPV wall. Such interactions could lead to thinning of the vessel wall and reduced margins to failure.

For the "final bounding state" configuration defined in the UCSB study, INEEL found that heat fluxes from the vessel remained below CHF even when peer reviewer concerns and additional parameter uncertainties were explicitly addressed in the integral solution. Reactor vessel integrity would therefore be expected to be maintained in the long term, provided the "final bounding state" can be achieved without prior vessel failure. However, INEEL also found that the "final bounding state" defined in the UCSB report does not necessarily bound all possible heat loads to the vessel. Steady-state calculations performed for several postulated alternate debris bed configurations indicate that heat fluxes can be higher than for the final bounding state and greater than CHF. Three configurations were: (1) a stratified intermediate state similar to the configuration analyzed in the UCSB study but with a thinner overlying metallic layer (Configuration A), (2) an intermediate state in which a limited amount of relocated metallic melt is trapped or sandwiched between two oxidic pools (Configuration B), and (3) a configuration in which a metallic/oxidic layer inversion occurs, resulting in a more dense heat generating metallic layer (consisting of uranium dissolved in zirconium) settling to the bottom of the vessel where CHF is at a minimum (Configuration C).

The staff concluded for AP600 that reactor vessel integrity is likely to be maintained if the requisite conditions for ERVC are met, but in view of the potential for certain hypothetical debris configurations to produce heat fluxes exceeding CHF, that RPV failure could not be ruled out for all possible core melt scenarios.

The applicability of these conclusions to AP1000 was assessed. The AP1000 decay heat level is higher than for AP600, and the RPV lower head dimensions are equivalent. Thus, the heat flux from the RPV would be greater, and the margins to RPV failure (with respect to CHF) potentially less for AP1000. To offset the potential reduction in the margin to CHF, Westinghouse has increased the CHF value by: (1) refining the RPV insulation system so as to streamline the flow between the RPV and the insulation, as discussed in Section 19.2.3.3.1.3, and (2) increasing the reactor cavity flood level associated with successful cavity flooding (as discussed in Section 19.2.3.3.1.1) to ensure that sufficient water/steam flows past the RPV are achieved, consistent with the conditions simulated in ULPU Configuration IV and V testing. These changes have been shown to achieve up to a 30-percent increase in CHF based on the results of ULPU Configuration IV testing.

Westinghouse calculations provided in Chapter 39 of the PRA indicate that with the AP1000 insulation modifications (as represented in ULPU Configuration IV testing) and with the reactor cavity adequately flooded, significant margin to RPV failure remains for the AP1000. The applicant has indicated that test results from ULPU Configuration V (with proto-typical AP1000 insulation) show a further improvement in coolability performance relative to Configuration IV. Thus, the margins to RPV failure may be even greater in the as-built AP1000 design.

In support of the staff's review for AP1000, confirmatory analyses were performed by ERI using a mathematical model for lower head thermal behavior under severe accident conditions (ERI/NRC 03-202, April 2003). This model is based on a conceptual representation of a stratified molten pool consisting of a dense metallic bottom layer of Zr-U-SS, a middle ceramic layer of UO_2-ZrO_2-M_xO_y, and a top metallic layer of Fe-Zr. Input to the model is in the form of point estimate values and probability density functions. Output from the model is provided in terms of probability distributions for the heat flux on the exterior surface of the RPV at different locations on the lower head. The following two debris configurations were evaluated:

- Configuration I - a molten ceramic (oxide) pool with an overlying molten metallic layer, and

- Configuration II - a molten ceramic pool sandwiched between a bottom heavy metallic layer and an overlying metallic layer.

These configurations are considered to be bounding in terms of their impact on the lower head integrity for AP1000. The first configuration is similar to Configuration A in the INEEL study for AP600. The second configuration is a combination of Configurations A and C in the INEEL study.

For Configuration I, one of the most important aspects is the potential for the formation of a top metallic layer thin enough to cause a significant focusing of heat on the RPV wall. For a low ceramic pool mass, the lower core support plate would not be submerged, and the amount of steel in the metallic layer would be limited, resulting in a thin metallic layer and increased heat fluxes to the RPV wall in the metallic layer region. For higher ceramic pool masses, the core support plate would be submerged, resulting in a thick metallic layer and reduced heat fluxes to the RPV wall. The quantities of core debris relocated into the lower plenum were treated in the

model using a probability density function. Results for Configuration I show a zero probability of exceeding CHF within the molten oxide region. However, the probability of exceeding CHF is about 0.15 within the metallic layer region. This probability was found to vary from 0.04 to 0.3 in sensitivity analyses examining the impact of heat transfer correlations, material properties, and the mass of debris in the lower plenum.

For Configuration II, parametric calculations were performed using point estimate mean values of the masses from Configuration I. The mass fraction of uranium in the bottom layer was fixed at 0.4 and provides a bottom layer (Zr-U-SS) density greater than that of the oxide layer, consistent with this configuration. The results of these calculations indicate that the heat fluxes from the vessel remain below CHF at all locations. Thus, the vessel would not be expected to fail if partitioning of the heavy metals from the ceramic pool were to occur.

Westinghouse does not consider a thin metallic layer in Configuration I to be applicable to the AP1000 because: (1) their analyses indicate that the lower plenum debris pool will contact the lower support plate and create a thick metal layer, and (2) in the transient stages before the debris contacts the lower support plate the debris will be either water cooled or quenched rather than a fully developed naturally circulating pool. For Configuration II, Westinghouse provided an analysis which produced results similar to the staff analysis, i.e., the heat fluxes from the vessel remain below CHF at all locations (response to RAI 720.48, Revision 1).

Since the review of the AP600 design, additional experiments relevant to in-vessel retention of molten core debris have been performed as part of programs sponsored by the Organization for Economic Cooperation and Development (OECD), in particular, the RASPLAV and MASCA programs. The RASPLAV project confirmed previous evaluations of the natural convection behavior of an oxidic corium pool that were based on simulant material. In addition, RASPLAV tests revealed that prototypic sub-oxidized corium which also contained some amount of carbon can stratify into a uranium-rich layer on the bottom and a zirconium-rich layer on the top. Other structural material in the reactor, such as boron, could also have the same influence on a sub-oxidized molten pool. The MASCA program (both small scale and confirmatory large scale) has largely confirmed the prediction that iron containing sub-oxidized corium can stratify (partition) into metallic and oxidic phases (D. A. Powers, “Chemical Phenomena and Fission Product Behavior During Core Debris/Concrete Interactions,” Proceedings of CSNI Specialists’ Meeting on Core Debris Concrete Interactions, published by Electric Power Research Institute, February 1987.) More importantly, the metallic phase may be denser than the oxidic phase and relocate to the lower part of the lower head.

Despite an increased understanding of core melt progression and lower head behavior since AP600, significant uncertainties remain. Uncertainties in the likelihood of forming various debris bed configurations are largely the result of the inherent limitations in the modeling of core melt progression/relocation and lower head debris bed behavior, and the difficulty in accurately simulating proto-typical reactor conditions in experiments. Additional experiments and detailed, transient modeling of lower head debris bed and molten pool behavior would be needed to determine and assess viable lower plenum debris configurations. The calculations would need to be dependent on realistic, validated models for debris quenching, debris bed reheating and remelting, and mixing and stratification of the newly formed molten pool. Such calculations are

considered to be beyond current severe accident analysis capabilities, and results of any such calculations would be highly speculative and be subject to considerable uncertainties.

For purposes of design certification, the staff has accepted the Westinghouse characterization of ERVC in the AP1000 PRA on the basis of the margin to vessel failure for the "final bounding state" configuration defined in the UCSB study, in conjunction with results of probabilistic and deterministic analyses of the impact of vessel failure on containment integrity. The deterministic analyses for core concrete interactions and ex-vessel FCI, described in Sections 19.2.3.3.3 and 19.2.3.3.5.2 of this report, indicate that RPV failure and subsequent melt relocation is not expected to result in early containment failure. The probabilistic assessment discussed in Section 19.1.3.2.3 of this report illustrates that if credit for successful ERVC is reduced or eliminated, containment failure frequency would increase proportionally since all RPV breaches are assumed to lead to early containment failure in the baseline PRA. Under the most limiting assumption of no credit for ERVC, the containment failure frequency would approach the core melt frequency given the pessimistic characterization of containment response to an RPV breach in the PRA. Even then, however, the containment failure frequency would remain below the general plant performance guideline of 1E-06/y for a large release of radioactive material (as proposed in the Safety Goal Policy Statement) because of the low estimated core damage frequency. The staff therefore concludes that the design of the AP1000 for ERVC is acceptable. The Westinghouse position that RPV failure is physically-unreasonable does not appear justified in light of the uncertainties in the late-phase melt progression and the melt configuration in the lower head. Nevertheless, the probability of vessel failure is judged to be small and this assumption is inconsequential from the overall risk perspective as discussed in Section 19.1.3.2.3.

19.2.3.3.1.3 System Considerations

Reactor Cavity Flooding System

The reactor cavity flooding system is comprised of two 20.3 cm (8 in.) diameter lines drawing from the IRWST gravity injection line (which connects to the IRWST sump) and discharging into the recirculation sumps at Elevation 90’ of containment. The water flows out of the recirculation sumps and eventually fills the floodable region of containment to the Elevation 107’. One motor-operated valve and one explosive valve is installed in each line. All valves are Class 1E and are powered by Class 1E dc power. The line sizing for the system is based on the design function of the lines which is to provide suction for the RNS pumps in the recirculation mode.

The containment recirculation squib valves and isolation MOVs, and the containment recirculation screens are included as risk significant SSCs within D-RAP. In-service inspection and testing programs provide surveillance and maintenance requirements on the related piping and valves. The operator action to flood the reactor cavity is specified in the first step of ERG AFR.C-1, which would be entered when core exit temperatures exceed 648.9°C (1200°F). The core exit thermocouples are used to monitor the need for cavity flooding within the inadequate core cooling (ICC) portion of the EOPs, and are also Class 1E and powered by Class 1E dc power. The staff therefore concludes that treatment of the reactor cavity flooding system in the DCD Tier 2 and ITAAC is acceptable.

Reactor Pressure Vessel Thermal Insulation System

In addition to RCS depressurization and reactor cavity flooding, several conditions must also be met in order to support ERVC, specifically: (1) the reactor vessel thermal insulation system is constructed in accordance with the final design description developed through ULPU Configuration V testing with proto-typical insulation, (2) the reactor vessel insulation system maintains its integrity under the hydrodynamic loads associated with ERVC, and is not subject to clogging of the coolant flow path by debris, and (3) RPV exterior coatings do not preclude the wetting phenomena identified as the cooling mechanism in the ULPU testing. Each of these areas is discussed below.

The RPV thermal insulation system is designed to limit thermal losses during normal operations, but also to provide an engineered pathway for supplying water cooling to the vessel and venting steam during severe accidents. The general features of the insulation system are described in DCD Tier 2 Section 5.3.5, and Chapter 39 of the PRA. Water enters the insulation system through water inlets located below the RPV lower head. From there, it flows upward and outward along the spherical lower head of the RPV where significant boiling and steam production occurs. The escaping liquid/steam mixture flows into the annular gap between the cylindrical portion of the RPV and the curved insulation panels to the top of the reactor vessel cylinderical section. It then passes through one of four steam flow paths/ducts, which are embedded in the concrete biological shield, into the vessel nozzle gallery at Elevation 98'. The coolant returns to the RCDT room via a grated opening between the vertical access tunnel and the RCDT room (approximately 9.3m^2 (100 ft^2) area), and enters the reactor cavity compartment through a passively-actuated damper installed in the doorway between the reactor cavity compartment and the RCDT room.

Key attributes of the reactor vessel insulation system include the following:

- the water inlets at the bottom of the insulation and the bouyant covers over the outlets of the 4 embedded water/steam flow paths in the shield wall, both of which change position during flood-up of the reactor cavity,

- specific RPV/insulation clearances and water/steam flow areas on which experimental facility scaling for ULPU Configuration V was based, and

- insulation panel and support members designed to withstand the hydrostatic and hydrodynamic loads associated with ERVC.

The water inlet at the bottom of the insulation is sized so that the pressure drop through the inlet is negligible during the circulation of water associated with the in-vessel retention phenomena, and would have a minimum total flow area of 0.56 m^2 (6 ft^2). Each of the four steam ducts in the biological shield wall have a flow area of 0.28 m^2 (3 ft^2) which would provide a flow area greater than or equal to the minimum flow area in the structures forming the circulation loop. On the basis of results from the ULPU Configuration V tests (with proto-typical insulation), the applicant estimates that the upper limit flow rate past the RPV would be approximately 57 kL/min (15,000 gpm). This information was provided informally, and will need

to be documented as part of the DSER Open Item 19.2.3.3-1 regarding documentation of ULPU Configuration V testing discussed below. The damper between the reactor cavity compartment and the reactor coolant drain tank (RCDT) room is normally closed to prevent air from flowing into the RCDT room during normal operation, but is designed to open passively during containment floodup to permit water to flow from the RCDT room into the reactor cavity compartment. The damper opening has a minimum flow area of 0.74 m^2 (8 ft^2), and is constructed of light-weight material to minimize the force necessary to open the door. The RPV insulation system and the damper between the reactor cavity and the RCDT room are included as risk-significant SSCs in the reliability assurance program, and important criteria associated with the design are incorporated into the ITAAC.

The AP1000 RPV insulation system is purchased equipment and not within the Westinghouse scope. The COL applicant will be responsible for completing the design of the reactor vessel insulation system. This will include the detailed design of the water inlets and outlets, RPV/insulation clearances and water/steam flow areas, and the structural analysis of the reactor vessel insulation panels and support members. General design requirements for the AP1000 insulation are provided in Section 39.10 of the PRA. Information needed to complete the final design, such as the hydrostatic and dynamic load information, will be obtained from the UPLU Configuration V test data as described below. For AP600, Westinghouse specified a set of functional requirements for the RPV insulation system on the basis of the ULPU Configuration III experiments, and performed a structural analysis that showed that the insulation design was able to meet each of the functional requirements. Thus, a design that meets the functional requirements is feasible.

Tests performed in ULPU Configuration IV focused on improvements to coolability performance (CHF) that could be achieved by streamlining the flow path between the RPV and insulation, thereby enhancing convection. The tests evaluated CHF for a curved baffle located at various positions/spacings from the vessel, and showed that a significant enhancement in CHF is possible relative to the Configuration III experiments for AP600 (see Quantification of Limits to Coolability in ULPU-2000 Configuration IV, CRSS-02.05.3, May 2002). As such, these tests provide a basis for further optimizing the insulation design.

The AP1000 insulation design was refined based on insights from the Configuration IV tests, and a proto-typical insulation design for AP1000 was evaluated as part of the ULPU Configuration V test program. The applicant has indicated that the Configuration V test results show a further improvement in coolability performance relative to Configuration IV, and also include information on transient pressure loads needed by the COL-applicant to establish the pressure loads for the structural analysis of the final insulation design. The applicant has not provided documentation of: the RPV insulation design evaluated in Configuration V, the results of the Configuration V testing, or the functional requirements for the AP1000 RPV insulation system. Such information is needed in order for the staff to conclude on the margins to lower head failure for AP1000, and the viability of Westinghouse's proposal that the COL applicant complete the RPV insulation design. This is Open Item 19.2.3.3-1.

The RCS blowdown during a LOCA may tend to carry debris created by the accident toward the reactor cavity. In response to a staff request, Westinghouse performed an evaluation of the

potential for such debris to block the ERVC flow path. On the basis of the estimate of 5,700 lpm (15,000 gpm) through the insulation, the maximum approach velocity toward the entranceway between the vertical access tunnel and the RCDT room is less than 0.3 m/s (1 ft/s). Such an approach velocity would prevent significant transport of large debris. The opening between the vertical access tunnel and the RCDT room is covered by a metal grating that will prevent any large pieces of debris from entering the RCDT room. In addition, the damper between the RCDT room and the reactor cavity compartment, as well as the entrance into the RPV insulation is elevated. Because the water level at the time of debris relocation is several meters above the bottom of the insulation, floating or submerged debris cannot be ingested into the insulation flowpath. Finally, a functional requirement will be included in the RPV insulation design to assure that the minimum flow area through each water inlet, as well as around the recirculating flow loop is met. The staff considers the potential for debris blockage of the ERVC flow path to be adequately addressed by the functional requirements of the insulation design and the related system ITAAC, and therefore the resolution of debris blockage is acceptable.

The ULPU testing included tests using prototypical RPV steel with paint applied according to Westinghouse paint application specifications. This paint is intended to protect the vessel carbon steel surface during shipment and storage, and is not expected to be removed. In the ULPU tests, the paint surface was judged to actually increase the wettability of the vessel external surface and increase the critical heat flux. Therefore it is important that Westinghouse paint application specifications for the RPV exterior be met.

Contingent upon resolution of Open Item 19.2.3.3-1 regarding documentation of ULPU Configuration V testing, the COL applicant will be responsible for completing the design of the reactor vessel insulation system. This is COL Action Item 19.2.3-1.

19.2.3.3.2 Hydrogen Generation and Control

In SECY-93-087, the staff recommended that the Commission approve the staff's position that passive plant designs must include the following provisions:

- accommodate hydrogen generation equivalent to a 100-percent metal-water reaction of the fuel cladding,
- limit containment hydrogen concentration to no greater than 10 percent, and
- provide containment-wide hydrogen control (such as igniters or inerting) for severe accidents.

These positions are codified in 10 CFR 50.34(f)(2)(ix). In its SRM, dated July 21, 1993, the Commission approved the staff's position. The issue of containment combustible gas control remains an open item, as discussed in Section 6.2.5 of this report.

19.2.3.3.3 Core Debris Coolability

CCI is a severe accident phenomenon that involves the melting and decomposition of concrete in contact with core debris. This phenomenon would occur following reactor vessel breach, if the molten core debris discharged from the RPV is not quenched and cooled. CCI can challenge the containment by various mechanisms including: (1) pressurization from non-condensible gas and steam production, (2) destruction of structural support members, and (3) melt-through of the containment liner and basemat.

In SECY-93-087, the staff recommended that the Commission approve the position that both the evolutionary and passive LWR designs meet the following criteria:

- provide reactor cavity floor space to enhance debris spreading,
- provide a means to flood the reactor cavity to assist in the cooling process,
- protect the containment liner and other structural members with concrete, if necessary, and
- ensure that the best-estimate environmental conditions (pressure and temperature) resulting from CCI do not exceed ASME Code Service Level C limits for steel containments, or factored load category for concrete containments, for approximately 24 hours.

In addition, the designs should ensure that the containment capability has margin to accommodate uncertainties in the environmental conditions from CCI. In its July 21, 1993, SRM, the Commission approved the staff's position.

The AP1000 design relies primarily on safety grade RCS depressurization and reactor cavity flooding capabilities to prevent RPV breach and CCI, but also incorporates plant features consistent with the criteria in SECY-93-087 and the EPRI URD criterion regarding debris coolability. In the unlikely event of RPV failure, these features would reduce the potential for containment failure from CCI. The AP1000 design features include the following items:

- a cavity floor area and sump curb that provides for debris spreading without debris ingression into the reactor cavity sump,
- a manually-actuated reactor cavity flood system that would cover the core debris with water and maintain long-term debris coolability, and
- a minimum 0.85 m (2.8 ft) layer of concrete to protect the embedded containment shell, with an additional 1.8 m (6 ft) of concrete below the liner elevation.

The cavity flooding system is discussed in Section 19.2.3.3.1 of this report. The reactor cavity floor area and response of the concrete basemat is discussed below.

The reactor cavity is comprised of two interconnected compartments – an octagonal shaped room below the RPV, and an adjacent room containing the normal containment sump and the RCDT. The total floor area is 48 m^2 (517 ft^2), divided approximately equally between the two compartments. A 1.5 meter (5 ft) wide tunnel, and a 0.9 meter (3 ft) wide ventilation duct connects the two volumes. The tunnel connecting the two regions of the cavity is protected by a door that serves as an HVAC barrier during normal operation. The door and ventilation ductwork are expected to be displaced by the pressurization associated with RPV breach before the arrival of core debris, thereby permitting core debris to spread within the two compartments.

The reactor cavity sump is located along the back side of the wall dividing the two compartments, and is surrounded by an 61 cm (24 in.) high, 30.5 cm (12 in.) thick concrete curb. The location of the sump (out of the line-of-sight of the RPV) and the concrete curb provide protection against entry of core debris into the sump, as discussed later. The sump is covered with a stainless steel plate that supports the reactor cavity drain pumps. A number of sleeved ½-inch drain holes pass through the curbing at floor level to permit water to drain into the sump, but these passages are sufficiently small that molten core material would quench and solidify in the passages before entering the sump.

The embedded steel containment liner beneath the reactor cavity region is ellipsoidal in shape. The minimum distance from the reactor cavity floor to the embedded steel liner (0.85 m (2.8 ft)) occurs at the end of the RCDT room furthest from the reactor vessel. The distance from the floor of the cavity sump to the steel liner is only slightly less (0.52 m (2.7 ft)) because of the ellipsoidal shape of the liner and the more central location of the sump. In the calculations discussed below, the thickness of concrete above the liner is taken to be the minimum distance of 0.85 m (2.8 ft).

The ratio of reactor cavity floor area to rated thermal power for the AP1000 design is 0.014 m^2/MW_{th}. This is less than the EPRI URD design criterion of 0.02 m^2/MW_{th} for debris coolability, which represents the EPRI estimate of what is required to adequately cool core debris. (The EPRI criterion corresponds to a debris depth of about 10-inches, which is less than the debris depth in AP1000.) The staff notes that the floor area provided in the AP1000 design, in conjunction with the reactor cavity flooding system, will promote debris coolability (via debris spreading, quenching by pre-existing water in then cavity, and long-term heat removal by the overlying water pool) but will not necessarily ensure it. Accordingly, the staff has relied on deterministic calculations described below, rather than the EPRI criterion, in judging the adequacy of the reactor cavity design for CCI.

As described in Section 19.2.3.3.1 of this report, ERVC features reduce the frequency of RPV breach in the baseline PRA to less than 1E-08/y. The staff considers reliance on the ERVC strategy consistent with Commission guidance in the SRM pertaining to SECY-93-087. In particular, under the topic of core debris coolability, the Commission stated that the staff should not limit vendors to only one method for addressing containment responses to severe accident events, but permit other technically justified means for demonstrating adequate containment response. However, in view of the complexity of the technical issues impacting the reliability of the ERVC strategy, the staff, in SECY-96-128, recommended that the Commission approve the

position that Westinghouse use a balanced approach, involving reliance on in-vessel retention of the core complemented with limited analytical evaluation of ex-vessel phenomena, to address the adequacy of the AP600 design for ex-vessel events. In its January 15, 1997, SRM, the Commission approved the staff's position. The deterministic calculations for CCI are of particular significance for AP1000 since, compared to other ALWRs, the AP1000 ex-vessel debris bed is deeper and the concrete basemat is thinner. In addition, the AP1000 design does not impose any restrictions on the type of concrete that can be used for the containment basemat and the reactor cavity walls.

The applicant performed deterministic calculations of CCI for a postulated vessel breach event. A MAAP4 analysis of CCI assuming a uniform debris bed within the AP1000 reactor cavity is provided in Appendix D of the PRA as part of the equipment survivability analysis. These calculations were performed for two different reactor cavity/basemat concrete compositions, i.e., limestone/common sand and basaltic concrete. For a basemat composed of limestone concrete (which maximizes non-condensible gas generation and minimizes concrete ablation) basemat penetration would occur after about 3 days following the onset of core damage. Containment pressure is not predicted to reach Westinghouse's Service Level C estimate (627 kPa (91 psig)) until even later. For a basemat composed of basaltic concrete (which maximizes concrete ablation and minimizes non-condensible gas generation) the predicted time of basemat melt-through is reduced to about 2 days, with containment over-pressure failure expected some time later.

The applicant performed additional, detailed calculations in which the metallic and oxidic components of the in-vessel core debris were tracked separately during the release, spreading, and CCI phases, thereby allowing evaluation of concrete ablation in different regions of the reactor cavity. These calculations are documented in Appendix B to the PRA. Westinghouse assumed an initial in-vessel core debris pool configuration consistent with the "Final Bounding State" in the DOE assessment of external reactor vessel cooling (DOE/ID-10460), i.e., essentially the entire inventory of core materials and steel structures, with the metal layer overlying the oxide pool. Westinghouse assumed the release of the entire mass of core debris in a molten state. This represents a conservative upper limit in terms of the mass of debris that could participate in CCI.

The following two vessel failure scenarios were evaluated: (1) a "hinged failure" in which a localized opening occurs near the vessel beltline immediately followed by the vessel tearing around nearly all its circumference, and the lower head hinging/swinging downward and coming to rest on the cavity floor, and (2) a "localized failure" in which a localized opening occurs near the vessel beltline (releasing molten core debris above the breach), and over time, moves downward releasing additional debris. For the localized failure mode, which involves a slow release and greater water depth than the hinged failure mode, Westinghouse used the THIRMAL code to assess the break-up and freezing of the melt as it falls through the water pool; these metal-water interactions were not considered for the hinged failure mode.

The MELTSPREAD code was used to analyze the spreading of the core debris over the various regions of the cavity floor for AP600. This permitted the metallic and oxidic components of the in-vessel core debris to be tracked separately during the release, spreading, and CCI phases.

For both RPV failure modes, the analyses show a non-uniform distribution of the melt constituents, with the debris consisting primarily of oxides (and most of the decay heat) in the region directly under the reactor, and primarily of metals at the opposite end of the reactor cavity. The equilibrium depth of the debris in the two regions of the cavity is approximately equal in the “hinged failure” case since the debris remains molten during the spreading. However, the equilibrium debris depth in the “localized failure” case is greater under the reactor than in the RCDT room because of an accumulation of solidified debris below the reactor in this scenario.

The results of the MELTSPREAD analyses for AP600, in terms of the characterization of debris composition in the two regions of the cavity, were considered applicable to AP1000 (based on the similarities in the postulated in-vessel molten pool and RPV lower head failure scenarios), and were used as input to the MAAP4 code for analysis of CCI for AP1000. Two separate MAAP analyses were performed for each RPV failure mode – the first analysis to treat the debris under the reactor vessel, and the second to treat the core debris at the opposite end of the cavity, where the sump and RCDT is located. The MELTSPREAD results were also used to assess the likelihood and impact of debris entering the reactor cavity sump in the two vessel failure scenarios considered.

The applicant evaluated the effects of CCI assuming two different reactor cavity/basemat concrete compositions, i.e., limestone/common sand and basaltic concrete. For a basemat composed of limestone concrete (which maximizes non-condensible gas generation and minimizes concrete ablation) basemat penetration would occur at about 4 days following the onset of core damage. Containment pressure is not predicted to reach Westinghouse's Service Level C estimate (627 kPa (91 psig)) until even later. For a basemat composed of basaltic concrete (which maximizes concrete ablation and minimizes non-condensible gas generation) the predicted time of basemat melt-through is reduced to about 3 days, with containment over-pressure failure expected some time later. Thus, these calculations, which assume separation of the metallic and oxidic components of the melt, result in a slightly later time of basemat melt-through than the calculations for a uniform debris bed discussed above. For both RPV failure scenarios and both concrete types, the concrete basemat in the region under the reactor vessel is eroded more rapidly than the region of the RCDT, and is the limiting location for basemat failure.

Although basemat penetration is unlikely, the Westinghouse assessment indicates that the molten core debris will reach the embedded liner (i.e., ablate through 0.85 m (2.8 ft) of concrete) within 9 to 11 hours of RPV breach with basaltic concrete, and within 11 to 13 hours of RPV breach with limestone concrete. However, in all cases, the top of the molten core debris pool is well above the embedded liner when melt-through first occurs, thereby preventing an airborne release of fission products. The staff does not consider the interface between the concrete basemat and embedded containment liner to be a viable pathway for significant airborne release of fission products to the environment in AP1000 in view of the minimal gaps, if any, between the concrete and the liner, and the considerable distance that fission products would need to travel along this pathway to reach the environment (a distance approximately equal to the radius of the containment). Accordingly, the staff's focus in assessing the

capability of the AP1000 to cope with CCI is on the time of basemat penetration rather than the time of melt-through of the embedded liner.

The MELTSPREAD calculations for the “localized failure” case indicate a maximum core debris depth of 25 cm (10 in.) in the region of the sump at any time in the transient for AP600. The core debris mass and height is greater for AP1000 but the maximum debris height will remain below the AP1000 curb height of 61 cm (24 in.). Thus, the reactor curb will prevent the entry of core debris into the sump for this scenario. Calculations for the "hinged failure" mode predict that a wave of molten core debris would be reflected off the back wall of the RCDT room and achieve a maximum height of about 63 cm (25 in) in the vicinity of the sump curb during passage of the wave for AP600. The maximum height will be greater for AP1000 and will exceed the 61 cm (24 in.) curb height temporarily. The equilibrium height of debris is about 46 cm (18 in.) based on the response to RAI 720.058. The presence of core debris deposited on the sump cover during passage of the wave is expected to result in failure of the cover and debris entry into the sump in this scenario. The applicant does not consider this situation to pose a threat to containment because the core debris entering the sump would consist primarily of the metallic component of the melt, similar to the rest of the RCDT compartment. MAAP calculations for AP1000 show that the concrete penetration on the RCDT side of the cavity (by debris composed primarily of metals) is minimal compared to the penetration on the reactor side of the cavity (by debris composed primarily of oxides). Since the distance to the liner in the sump (0.82 m (2.7 ft)) is not significantly different than the distance assumed in the CCI calculations (0.85 m (2.8 ft)), the concrete penetration on the reactor side of the cavity is still expected to be limiting.

The staff considers the applicant’s rationale regarding the significance of CCI in the cavity sump to be consistent with our expectations for the postulated failure scenarios, and reasonable. In judging the adequacy of the sump protection, the staff has also considered the following:

- The low probability of reactor vessel breach in the AP1000 design, given that the requisite conditions for in-vessel retention (RCS depressurization and reactor cavity flooding) would be achieved in over 90 percent of core damage events, and the high confidence that vessel integrity would be maintained when these conditions are achieved.

- The likelihood that considerably less core debris would be released than assumed by the applicant, particularly in events with earlier times to reactor vessel breach, such as the alternate debris bed configurations postulated in Section 19.2.3.3.1 of this report.

- The AP1000 will have no piping embedded in the concrete floor that could represent a potential path out of containment.

On these bases, the staff considers the sump protection in the AP1000 design to be acceptable.

The staff performed calculations using the MELCOR code to confirm the degree of basemat ablation for AP1000 (ERI/NRC 03-201). The calculations indicate a maximum ablation depth of

about 1.3 m (4.3 ft) for both limestone and basaltic concrete 2.5 days after accident initiation, assuming a dry reactor cavity and uniform distribution of debris within the reactor cavity. The calculations were terminated at this time. The ablation rates predicted by MELCOR are considerably lower than predicted by MAAP, partially as a result of a later time of RPV failure in the MELCOR calculation (8 hours in MELCOR versus 2 hours in MAAP). While not directly comparable to the Westinghouse calculations, the MELCOR calculations support the Westinghouse finding that basemat penetration would not occur for several days.

The staff concludes that in the event that core debris is not retained in vessel, the AP1000 design provides adequate protection against early containment failure and large releases resulting from CCI. Specifically, the AP1000 incorporates features that adequately address all criteria called out in SECY-93-087 related to core debris coolability. Although several factors in the AP1000 design mentioned earlier could tend to increase the severity of basemat melt-through, best-estimate calculations performed by Westinghouse and confirmed by NRC-sponsored calculations indicate that in the event of unabated CCI, containment basemat penetration or containment pressurization above ASME Code Service Level C limits will not occur until well after 24 hours, regardless of concrete composition. On this basis, the staff finds the AP1000 design acceptable in terms of its protection against CCI.

19.2.3.3.4 High-Pressure Core Melt Ejection

High pressure core melt ejection (HPME) and subsequent DCH is a severe accident phenomenon that could lead to early containment failure with large radioactive releases to the environment. HPME is the ejection of core debris from the reactor vessel at a high pressure. DCH is the sudden heatup and pressurization of the containment resulting from the fragmentation and dispersal of core debris within the containment atmosphere. In addition, DCH could also lead to direct attack on the containment shell.

The applicant has incorporated several features in the AP1000 design to prevent and mitigate the effects of DCH, specifically, the automatic depressurization system and reactor cavity design features.

In SECY-93-087, the staff recommended that the Commission approve the general criteria that the evolutionary and passive LWR designs provide a reliable depressurization system and cavity design features to decrease the amount of ejected core debris that reaches the upper containment. Examples of cavity design features that will decrease the amount of ejected core debris reaching the upper containment include ledges or walls that would deflect core debris and an indirect path from the reactor cavity to the upper containment. In its July 21, 1993, SRM, the Commission approved the staff's position.

One of the major features of the AP1000 design is the ADS. The ADS is an automatically-actuated, safety-grade system consisting of 4 different valve stages that open sequentially to reduce RCS pressure sufficiently so that long-term cooling can be provided from the passive core cooling system. In the event that automatic actuation fails, the ADS is initiated by operator action from the main control room using the diverse actuation system. The ADS valves are designed to remain open for the duration of any ADS event, thereby preventing repressurization

of the RCS. The performance of the ADS for design-basis accident is discussed in DCD Tier 2 Section 6.3 and Sections 5.1.3.7 and 6.3 of this report. The modeling of ADS in the PRA is described in Chapters 11 and 36 of the PRA.

The Level 1 PRA includes consideration of RCS depressurization (by automatic and manual actuation of ADS) early in an event to prevent core damage. For those sequences that proceed to core uncovery at high RCS pressure, the potential to manually depressurize the RCS before the occurrence of thermally-induced SGTR or HPME is further evaluated in the Level 2 PRA. The survivability of the ADS valves and related instrumentation within the early phase of a severe accident during which late depressurization is viable is addressed in Appendix D of the PRA and Section 19.2.3.3.7 of this report. This assessment indicates that the design basis temperature will only be exceeded for a short time preceding late actuation of the valves. Because the ADS valves will be actuated before the time of rapid cladding oxidation and high RCS blowdown temperatures, the staff concludes that the ADS valves will be available to depressurize the RCS.

As discussed in Section 19.1.3.2.1 of this report, the majority of Level 1 sequences in the baseline PRA (about 90 percent) involve events with at least partially successful RCS depressurization, and relatively low RCS pressure (<1.03 MPa (150 psig)) at the time of core uncovery. With credit for late RCS depressurization, an even larger fraction of the core melt sequences (about 95 percent) are estimated to involve a depressurized RCS at the time of RCS pressure boundary challenge. Thus, only about 5 percent of the core damage events would potentially result in DCH. In the PRA, high pressure core melt sequences (with unsuccessful late depressurization) are assumed to result in failure of the SG tubes before reactor vessel failure. This obviates the need for additional thermal-hydraulic and probabilistic analyses of the following:

- the likelihood of RCS piping versus steam generator tube over-pressure failures in ATWS events,

- the likelihood of containment failure from DCH pressure loads in high pressure core melt accidents, and

- the relative challenge and timing of creep-rupture failures in RCS piping, hot leg nozzles, pressurizer surge line, and steam generator tubes in high pressure core melt accidents

However, if such a failure does not occur and all high pressure core melt accidents result in RPV failure, the resulting frequency of HPME events would remain very small (about 1E-08/y).

The design of the reactor cavity is expected to decrease the amount of ejected core debris that reaches the upper containment. The pathways for debris transport from the AP1000 reactor cavity include the following:

- the annular openings between the coolant loops and the biological shield wall, that lead to the SG compartments,

- the area around the reactor vessel flange that leads directly to the upper compartment (blocked by a permanent refueling cavity seal ring), and

- a ventilation shaft from the roof of the RCDT room, that leads to the steam generator compartments.

Debris particles traveling along the first two paths would pass between the RPV and the cavity walls, around the boro-silicone neutron shield blocks, through the HVAC air flow slots in the RPV vessel supports, and into the nozzle gallery surrounding the upper portion of the vessel, before passing through either the annular openings between the coolant loops and the biological shield or the gap around the permanent cavity seal ring. Particles traveling along the third path would pass into the RCDT side of the reactor cavity, up into a ventilation shaft in the ceiling of the RCDT room, into a common tunnel between the two SG compartments, and into the SG compartments. In all cases, the particles would change direction and encounter obstacles before reaching the upper containment.

The applicant evaluated the containment pressure loads for a postulated RPV breach event in the AP600 design using the 2-cell equilibrium model developed by Pilch, et. al., under NRC-sponsorship for resolution of the DCH issue and used as the basis for the resolution of the technical issue concerning DCH (NUREG/CR-6338). The peak containment pressure for a postulated DCH event was estimated to be about 559 kPa (81 psig), which is below Westinghouse's estimated value for Service Level C for AP600 and is sufficiently small that the corresponding probability of containment failure is negligible (less than 0.1 percent). Although a similar calculation was not performed for AP1000, the probability of containment failure in AP600 is judged by the staff to be applicable to AP1000 based on similar reactor cavity designs in AP600 and AP1000, similar ratios of containment volume to core debris mass (0.61 m^3/kg for AP1000 versus 0.66 m^3/kg for AP600), and higher ultimate pressure capacity for AP1000 (e.g., the containment pressure corresponding to a 10^{-3} probability of failure is approximately 655 kPa (95 psig) in AP1000 versus 552 kPa (80 psig) in AP600.) The latter two factors would offset the effect of a higher core mass in AP1000.

The staff concludes that the AP1000 design provides adequate protection against early containment failure and large releases due to DCH. Specifically, the AP1000 incorporates a safety-grade depressurization system, and reactor cavity design features that are expected to decrease the amount of ejected core debris that leaves the reactor cavity in the event of a high pressure melt ejection event. These features adequately address all criteria called out in SECY-97-187 related to high pressure melt ejection. In the event of an RPV breach at high pressure, calculations performed by Westinghouse for AP600 and applicable to AP1000 indicate that the peak containment pressure will remain sufficiently small, and that the corresponding probability of containment failure is negligible. On these bases, the staff finds the AP1000 design acceptable in terms of its protection against DCH.

19.2.3.3.5 Fuel-Coolant Interactions

The containment function can be challenged by energetic FCI, also known as "steam explosions." 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, high local pressures, and the propagation of the pressure wave in the water. Section J, "Containment Performance," of SECY-93-087 indicates that the staff will evaluate the impact of FCI on containment integrity by using the containment performance goal. The purpose of this section is to perform such an evaluation for steam explosions that may occur either inside (in-vessel) or outside (ex-vessel) the AP1000 reactor vessel.

19.2.3.3.5.1 In-Vessel Steam Explosions

In-vessel steam explosion is addressed in DCD Tier 2 Section 19.34.2.2.1, and in Section 34.2.2.1 of the AP1000 PRA supporting document. The applicant claims that based on the in-vessel core relocation scenario for the AP1000, the conclusions from the in-vessel steam explosion analysis performed for the AP600 can be extended to the AP1000. The claim is based on the facts that the geometry of the AP1000 lower head is the same as AP600, and expected molten core mass flow rate, its superheat and composition to be “essentially the same” as AP600.

The AP600 in-vessel steam explosion analysis was performed using ROAAM in the report “In-vessel Coolability and Retention of a Core Melt,” DOE/ID-10460 (Reference 19.34-2 in AP1000 DCD Tier 2, and Reference 34-3 in the AP1000 PRA.) The ROAAM analysis concludes that the lower head vessel failure from in-vessel steam explosion is “physically unreasonable with very large margin to failure.”

Because of its applicability, the following is a summary of staff’s evaluation and conclusions presented in Section 19.2.3.3.5.1 of AP600 FSER, NUREG 1512.

The report “In-vessel Coolability and Retention of a Core Melt,” DOE/ID-10460 is henceforth denoted as IVR report. Other reports used in the AP600 analysis are "Lower Head Integrity Under In-Vessel Steam Explosion Loads," DOE/ID-10541, henceforth denoted as the IVSE report, and its companion reports: “Propagation of Steam Explosions: ESPROSE.m Verification Studies,” DOE/ID-10503, and “Pre-mixing of Steam Explosions: PM-ALPHA Verification Studies,” DOE/ID-10504.

Briefly, the ROAAM approach involves decomposing the in-vessel steam explosion issue into a set of contributing physical processes, quantifying these processes through a combination of "causal relations" representing best estimate physics and probability distributions representing "intangible parameters" and finally, combining the quantification of individual processes into an integral assessment of the overall issue. The physical processes are as follows:

- melt relocation into the lower plenum
- initial melt-water interactions leading to coarse breakup of melt and forming a premixture
- triggering of premixture and energetic melt-water interactions
- consequent loading of the lower head and its response

The causal relations describing these physical processes, in their respective order, are:

- melt progression (analytical treatment founded on physics)
- premixing (PM-ALPHA code and associated models)
- explosion propagation (ESPROSE.m code and associated models)
- structural loads and response (ABAQUS code)

The intangible parameters, identified in the IVSE report, are as follows:

- the location and size of the failure
- melt characteristic length scale (initial size of melt particles)
- evolution of melt length scale (breakup rate)
- trigger strength and timing

Of these intangible parameters, some were treated in a deterministic manner (e.g., failure location, trigger strength), whereas probability distributions were assigned to others (i.e., failure size, initial melt particle size, melt breakup rate, and trigger timing).

The staff noted that the usual ROAAM approach, i.e., consideration of splinter scenarios, assignment of probability distributions to intangibles, and convolution of causal relations with the probability distribution (illustrated in Figure 2.3 of the IVSE report) was not rigorously followed in this case. Three reasons were cited: (1) a unique melt relocation scenario, (2) bounding approach taken with regard to premixing and explosion calculations, and (3) non-intersecting load and fragility curves. Moreover, the IVSE report argued that the bounding approach obviated any parametric and sensitivity calculations.

Regarding melt relocation, the staff accepted the applicant's conclusion that, given AP600 geometry (i.e. relatively flat radial power profile, high aspect ratio and relatively thick core plate), the melt release would occur following a sideways growth of the crust surrounding the melt pool, breach of the reflector and the core barrel, and melt flow out of the pool into the lower plenum water. As a consequence, the staff found the calculated hole in the baffle plate and the rates of molten core relocation to be acceptable. However, the staff also acknowledged that although the downward melt relocation is less likely (because of the potential for the coolability of the blockage in the lower core region), the high level of uncertainty associated with crust failure and the limited qualitative arguments provided by Westinghouse made the staff unable to completely eliminate the downward scenario from further consideration.

Regarding quantification of premixtures (i.e. initial condition for an energetic FCI), the staff found the Westinghouse method (i.e. PM-ALPHA code) to quantify pre-mixtures as applied to the AP600 acceptable. The staff had not conducted an independent verification of the PM-ALPHA code. However, the staff reviewed the submitted information and concluded that a reasonably large assessment data base supported the applicant's use of the PM-ALPHA code for this assessment. In particular, the staff agreed that Westinghouse sufficiently demonstrated that larger melt length scales would actually produce mixtures that were much more difficult to explode and, therefore, the choice of mixing length scale was conservative.

Regarding quantification of explosion loads, the staff found that the Westinghouse approach to triggering, both timing and location, to be conservative. The staff noted that the influence of

trigger location to energetics, if discernible, is likely to be bounded by sensitivity analysis involving trigger timing. On the basis of the review of the information submitted by Westinghouse, the staff found the used methodology, as applied to AP600 and documented in DOE/ID-10503 report, and the analytical results to be acceptable.

Regarding structural failure criteria, the staff concluded that IVSE report, along with it's companion reports, DOE/ID-10543 and DOE/ID-10504, are acceptable for addressing the in-vessel steam explosions, and for determining the magnitude of in-vessel steam explosions for the sideways melt release scenario for the AP600. The staff noted that this conclusion cannot be extended to the downward relocation scenario, which the staff considered to be less likely to occur. In addition, although the staff did not review and approve Westinghouse's structural analyses, the staff believes there is an adequate safety margin to support the conclusion that (for the sideways melt release scenario) in-vessel steam explosions of sufficient magnitude to challenge the structural integrity of the AP600 lower head are of sufficiently low probability to be discounted from further consideration.

The applicant did not submit AP1000-specific in-vessel steam explosion analysis, but provided arguments in support of the assertion that AP600 analyses are extendable to AP1000. The staff did not perform an independent analysis of in-vessel steam explosions for AP1000, nor did it perform one for AP600. For AP600, the staff reviewed extensive documentation of the in-vessel steam explosion analysis provided by the applicant which supporting the argument that the lower head failure from in-vessel steam explosions was of sufficiently low probability. The staff concluded that for the range of uncertainties associated with the late phase core melt progression considered in the analysis, the argument was acceptable. For AP1000, the staff performed a review of Westinghouse's approach to analysis of AP1000 in-vessel steam explosions which is based entirely on the similarity argument between AP1000 and AP600. Because of a high degree of similarity between AP600 and AP1000 geometries, the staff believes the range of uncertainties associated with the physical processes involved in the in-vessel steam explosions is same, or very similar for both configurations. Moreover, the staff recognizes the prevailing experts' opinion that the alpha-mode failure is not risk-significant (NUREG-1524).

Based on the above, the staff accepts the applicant's position that the conclusions from the AP600 in-vessel steam explosion analysis can be extended to AP1000. The staff, however, notes that an extension of the similarity argument to in-vessel retention may not be clearly evident. As such, the likelihood of lower head failure due to high heat fluxes resulting, for example, from the focusing effect is non-negligible (see Section 19.2.3.3.1 of this report.)

19.2.3.3.5.2 Ex-Vessel Steam Explosion

Ex-vessel steam explosion is addressed in section 19.34.2.2.2 of the AP1000 DCD Tier 2, and in section 34.2.2.2 of the AP1000 PRA supporting document. As stated, the first level of defense for ex-vessel explosions is the in-vessel retention of the molten core debris. However, in the event of the lower head failure and a dry reactor cavity (i.e. cavity not flooded) the PRA analysis assumes early containment failure. The issue of ex-vessel steam explosions appears only when the vessel fails with a flooded cavity. For this case Westinghouse claims that the

conclusions from the ex-vessel steam explosion analysis performed for the AP600 can be extended to the AP1000. The claim is based on the following reasons: (i) the vessel failure modes are the same for both designs, (ii) the initial debris mass, superheat and composition are expected to be the same, and (iii) since the AP1000 vessel lower head is closer to the cavity resulting in less debris mass participating in the interaction with water, it is conservative to use the AP600 analysis.

A structural response analysis of the reactor cavity during postulated AP600 ex-vessel steam explosions was performed in the Reference 19.34-5, Appendix B to DCD Tier 2. The following is a summary of staff's evaluation and conclusions presented in Section 19.2.3.3.5.2 of the AP600 FSER, NUREG 1512.

The review was performed following the guidance given in Section J, "Containment Performance," of SECY-93-087. Therefore, within the context of the containment performance goal, the staff evaluated the impact of steam explosions on the integrity of the containment. The staff found the applicant's treatment of ex-vessel steam explosions in the PRA to be conservative.

Following the guidance given in SECY 93-087, the applicant evaluated the ex-vessel steam explosion loadings on the reactor cavity, reactor pressure vessel, and the containment liner using the TEXAS code. Two reactor vessel failure modes were considered: (1) localized creep rupture of the vessel leading to a small localized opening, and (2) global creep rupture leading to "unzipping" of the lower head (denoted as the "hinged" failure mode) at or near the transition between the hemispherical lower head and cylindrical vessel structure. The first of these modes produces a small (~3.8 kg/s), localized flow of melt out of the vessel sidewall into the cavity water pool through an equivalent 6.0 cm diameter opening, while the second produces a massive flow (15,100 kg/s) through a much larger opening (~100 cm diameter) caused by global creep rupture failure at the belt line (transition between the hemispherical and the cylindrical parts). The details of each of the assumed reactor vessel failure modes are provided in Reference B-6, DOE/ID-10523, "Analysis of Melt Spreading in an AP600-Like Cavity," of Appendix B to the AP1000 PRA. Both failures are considered at a fully depressurized RPV condition and, as such, the conclusions are valid only for that condition.

The applicant performed two baseline calculations – one each for the localized and hinged failure modes – and four sensitivity calculations for the localized failure mode only. The applicant also assessed the vertical uplift of the reactor pressure vessel resulting from the impulse loads calculated for the hinged failure mode. The conclusion was that in every case the structural integrity of the steel containment vessel would be maintained, even though in the case of hinged failure the structural integrity of the concrete cavity floor and wall would not be retained.

The staff reviewed the assumptions used in the AP600 analysis as well as the results. The staff found the selected hole sizes for both the localized failure and the hinged failure cases to be realistic and therefore acceptable. Moreover, for the localized failure case, a reasonable variation in hole sizes is not expected to change the overall conclusion (as may be evident from the sensitivity analysis) that the containment integrity would not be challenged. The staff also

verified Westinghouse's assumptions of melt temperature and superheat for the hinged failure case through an independent study, "Potential for AP600 In-Vessel Retention Through Ex-Vessel Flooding," (INEEL/EXT-97-00779).

In assessing the structural integrity of the containment due to ex-vessel steam explosions, the applicant used the loading associated with the hinged failure mode and found the containment capacity to have 20 percent margin. The staff performed an independent evaluation and found the applicant analysis acceptable. The staff also performed an evaluation of the reactor vessel uplift due to explosion loading and found the uplift did not lead to containment failure.

The staff's acceptance of the applicant's containment integrity analysis, performed for AP600, during postulated ex-vessel steam explosions were based on calculations performed by ERI, using the PM-ALPHA/ESPROSE.m and the TEXAS computer codes. The mass, composition, and temperature of the core debris were based on SCDAP/RELAP5 and MELCOR analyses for low pressure accident scenarios. Sensitivity calculations were performed to examine the impact of the lower head failure size, water subcooling, melt superheat and composition, and the degree of cavity flooding (i.e., depth of the cavity water pool). Sensitivities of the calculated loads to the variations in the uncertain model parameters (i.e., the particle diameter, the maximum rate of fragmentation per particle in ESPROSE.m, and the fragmentation rate constant in TEXAS) were also studied.

Based on the above discussion, the staff concluded that the ability of the AP600 design to accommodate an ex-vessel steam explosion was acceptable, relative to the containment performance goal.

The staff, through its contractor, ERI, performed an independent evaluation of the AP1000 ex-vessel steam explosions. The results are reported in "Analysis of in-vessel retention and ex-vessel fuel coolant interaction for AP1000", ERI/NRC 03-202. The approach used in this study consists of the specification of initial and boundary conditions; determination of the mode, the size and the location of lower head failure using detailed analyses; computer simulation of the FCI processes; and finally, an examination of the impact of the uncertainties in the initial and boundary conditions as well as the FCI model parameters on the fuel coolant interaction energetics through a series of sensitivity calculations.

The cavity design in AP600 and AP1000 are similar, but the AP1000 reactor vessel lower head is closer to the cavity floor. Based on the in-vessel retention analysis, discussed in Section 19.2.3.3.1 of this report, the base case for the ex-vessel steam explosion is assumed to involve a side failure of the vessel involving a metallic pour into the cavity water. For the AP1000 analysis, the entire reactor vessel lower head is modeled based on the insights from the AP600 study by ERI (Report ERRI/NRC 95-211, September 1998). The impulse loads on the reactor vessel are found to be similar to those on the cavity wall due to the proximity of the explosion zone to both the reactor vessel and the cavity wall. A number of sensitivity studies were also performed for AP1000. The results of the ex-vessel fuel coolant interaction analyses for AP1000 show that the impulse loads on the cavity wall remain below the calculated loads for AP600. In the AP600 analysis, the base case involved a mostly ceramic melt pour, while in the present AP1000 analysis the base case involves a metallic pour, which potentially might lead to

a larger impulse load. However, the sensitivity calculations for the most severe case of a deeply flooded cavity in AP1000, clearly show that the previously reported AP600 impulse load predictions are bounding.

The staff acknowledges that the underlying physical phenomena associated with the fuel coolant interaction issue are not fully understood and significant uncertainties remain in some areas. With that understanding, the staff accepts the extension of the conclusions from the AP600 steam explosions analyses to AP1000, based on a high degree of similarity between the two designs.

19.2.3.3.6 Containment Bypass

Severe accident containment bypass for the AP1000 includes three issues: (1) interfacing system LOCAs (ISLOCA) outside containment, (2) steam generator tube rupture (SGTR) events leading to offsite releases through the steam generator relief valves, and (3) containment integrity failure during a severe accident scenario. The evaluation of design options to minimize containment bypass from SGTR events is addressed below. Containment bypass from SGTR events is discussed in Section 5.4.2.3 of this report. ISLOCA is addressed in Section 19.2.2.1.5 of this report, and maintenance of containment integrity during severe accidents is addressed in Sections 19.2.3.3.7 and 19.2.6 of this report.

In SECY-93-087, the staff recommended that the Commission approve the position to require that the advanced plant designer consider design features to reduce or eliminate containment bypass leakage that could result from SGTR. The following design features were identified 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, and
- increased pressure capacity on the SG shell side with a corresponding increase in the safety valve setpoints.

In its July 21, 1993, SRM, the Commission approved the staff's position.

Westinghouse evaluated the following design options as part of their assessment of SAMDAs for AP1000:

- a passive safety-related heat removal system to the secondary side of the steam generators. The system would provide closed loop cooling of the secondary side using natural circulation and stored water cooling, thus preventing a loss of primary heat sink in the event of a loss of startup feedwater and passive RHR heat exchanger. The system was estimated to cost $1.3 million.

- redirecting the flow from all steam generator safety and relief valves to the IRWST (as well as a lower cost option of this design improvement, consisting of redirecting only the discharge from the first stage safety valve to the IRWST). The system would prevent or reduce fission product release from bypassing the containment in the event of a SGTR event. The system was estimated to cost $0.6 million.

- increasing the design pressure of the steam generator secondary side and safety valve setpoint to the degree that a SGTR will not cause the secondary system safety valve to open. This design change would also prevent the release of fission products that bypass the containment via the SGTR. The system was estimated to cost $8.2 million.

On the basis of the estimated CDF and risk from internal events in the AP1000 design, any potential design modifications for accident mitigation that cost more than about $500 would not be cost effective, even if the modifications were to totally eliminate all offsite consequences. If the baseline core damage frequency is increased by a factor of 100 to account for external events and other accident sequences not included in the analysis, and the design modifications completely eliminate all offsite consequences, this value rises to about $50,000. The above design changes involve a major redesign effort, pose serious design drawbacks and are prohibitively expensive. In view of the low residual risk for AP1000 and the significant costs associated with the aforementioned design changes, the staff concludes that the risk reduction offered by the design changes is not significant, and that the design changes are impractical and would excessively impact on the plant.

In Section 19.1.3.1.2 of this report, the staff concludes that preventive and mitigative features in the AP1000 design result in a reduction in the estimated CDF for SGTR sequences to about 7E-09/y. In Section 15.6.3 of this report the staff concludes that there is reasonable assurance that SGTR events pose no undue threat to the public health and safety. The staff further concludes that the three design alternatives identified in SECY-93-087 have been adequately assessed and that the criteria of SECY-93-087 have been met.

19.2.3.3.7 Equipment Survivability

The survivability of equipment, both electrical and mechanical, is needed to prevent and mitigate the consequences of severe accidents. Westinghouse addressed equipment survivability in AP1000 DCD Tier 2 Appendix 19D which contains general requirements and equipment classification. The analysis performed to determine the severe accident environmental conditions is presented in Appendix D to the AP1000 PRA supporting document.

The requirements for equipment survivability are different from equipment qualification. The latter requires that the safety-related equipment, both electrical and mechanical, must perform its safety function during design bases events. Section 3.11 and Appendix 3D of the AP1000 DCD Tier 2 define the limiting environmental design conditions for all safety-related mechanical and electrical equipment. The level of assurance provided for the equipment operability during design bases events is called "environmental qualification" or "equipment qualification."

Beyond-design-basis events can be divided into two classes: in-vessel and ex-vessel severe accidents. During the in-vessel events the core is losing its coolability leading to at least a partial fuel melt. During the ex-vessel events a reactor vessel failure is assumed, leading to a relocation of molten corium (i.e. mixture of fuel and structural materials) to the containment. Such postulated severe accidents result in environmental conditions that are generally more limiting than those from design bases events. The NRC established a criterion to provide a reasonable level of confidence that the necessary equipment will perform its mitigative function in the severe accident environment for the time span for which it is needed. This criterion is referred to as "equipment survivability."

SECY-93-087 indicated that the staff would evaluate the ALWR vendor's identification of equipment needed to perform mitigative functions and the conditions under which the mitigative systems must operate. In SECY-93-087, the staff recommended that the Commission approve the staff's position that passive plant design features provided only for severe accidents mitigation need not be subject to the 10 CFR 50.49 environmental qualification requirements; 10 CFR Part 50, Appendix B quality assurance requirements; and 10 CFR Part 50, Appendix A redundancy/diversity requirements. The staff concluded that guidance such as that found in Appendices A and B of RG 1.155, "Station Blackout," is appropriate for equipment used to mitigate the consequences of severe accidents. In the SRM dated July 21, 1993, the Commission approved the staff's position.

The applicable criterion for equipment, both mechanical and electrical, required for recovery from in-vessel severe accidents is provided in 10 CFR 50.34(f).

- In Section 50.34(f)(2)(ix)(C), the NRC states that equipment necessary for achieving and maintaining safe shutdown of the plant and maintaining containment integrity will perform its safety function during and after being exposed to the environmental conditions attendant with the release of hydrogen generated by the equivalent of a 100 percent fuel-clad metal-water reaction including the environmental conditions created by activation of the hydrogen control system.

- In Section 50.34(f)(3)(v), the NRC states that systems necessary to ensure containment integrity shall be demonstrated to perform their function under conditions associated with an accident that releases hydrogen generated from 100 percent fuel-clad metal-water reaction.

- In Section 50.34(f)(2)(xvii), the NRC requires instrumentation to measure containment pressure, containment water level, containment hydrogen concentration, containment radiation intensity, and noble gas effluents at all potential accident release points.

- In Section 50.34(f)(2)(xix), the NRC requires instrumentation adequate for monitoring plant conditions following an accident that includes core damage.

These regulations collectively indicate the need to perform a systematic evaluation of all equipment, both electrical and mechanical, and instrumentation to ensure its survivability for intervention into an in-vessel severe accident. The applicable criteria required to mitigate the

consequences of ex-vessel severe accidents are discussed in the “Equipment Survivability” sections of SECY-90-016 and SECY-93-087.

In DCD Tier 2 Appendix 19D, the applicant discusses the NRC requirements regarding equipment survivability, various phases of accidents progression (i.e. pre-core uncovery, core heatup, in-vessel severe accident phase and ex-vessel severe accident phase), instrumentation needed for monitoring accident progression and equipment required to mitigate consequences of severe accidents. The applicant had not included information regarding severe accident conditions in the DCD Tier 2. Such information, however, was provided in Appendix D to the AP1000 PRA supporting document.

The following evaluation is based on information included in both DCD Tier 2 Appendix 19D and in Appendix D to the AP1000 PRA supporting document.

The applicant defined four phases of accidents progression:

- Time Frame 0: Pre-Core Uncovery,
- Time Frame 1: Core Heatup,
- Time Frame 2: In-Vessel Severe Accident Phase, and
- Time Frame 3: Ex-Vessel Accident Phase.

The applicant claims that requirements for equipment to survive and function vary as accidents progress. During Time Frames 0 and 1 the equipment survivability is covered under the design basis equipment qualification program. During Time Frame 2 the equipment is designed to fulfill the recovery actions under the severe accident management strategies, while during Time Frame 3 the equipment and instrumentation is designed to monitor accident progression, maintain containment integrity and mitigate fission product releases to the environment. The staff concurs with this characterization.

Specifically, sufficient instrumentation should exist to inform operators of the status of the reactor and the containment at all times as the in-vessel severe accident is intended to be recoverable from and lead to safe shutdown with containment integrity maintained. The ERGs direct specific manual operator actions determined by instrumentation readings and as such all instrumentation should exist where manual operator actions are specified within the ERGs.

The applicable criteria for equipment, both electrical and mechanical, required to mitigate the consequences of ex-vessel severe accidents is discussed in the “Equipment Survivability” section of SECY-93-087. Mitigative features should be designed to provide reasonable assurance that they will operate in the severe accident environment for which they are intended and over the time span for which they are needed. In cases where safety-related equipment (equipment provided for DBAs) is relied upon to cope with severe accident situations, there should be reasonable assurance that this equipment will survive accident conditions for the period that is needed to perform its intended function. Also, sufficient instrumentation needs to be identified to inform operators of the status of the containment at all times. Of particular interest is the status of the reactor vessel integrity.

The applicant analyzed various severe accident scenarios and identified the equipment needed to perform various functions during a severe accident and the environmental conditions under which the equipment must function. The results are summarized in DCD Tier 2 Tables 19D-1 through 19D-7. The severe accidents environment conditions, i.e. pressure, temperature and radiation, in which the equipment is relied upon to function, is provided in Appendix D to the AP1000 PRA supporting document.

Of particular interest is the issue of hydrogen control, i.e. maintaining hydrogen concentration in containment below a globally flammable limit. This function is performed by hydrogen igniters. The ERGs require activating the igniters in Time Frame 1, even though a significant amount of hydrogen is not generated until Time Frame 2. The staff's analyses performed by its contractor, ERI, using the MELCOR computer program indicate that integrity of the AP1000 containment is not challenged by hydrogen burn during postulated severe accidents, as discussed in Section 19.2.6 of this report. That conclusion applies also to the case, presented by Westinghouse, of a global hydrogen burn (i.e., burn of amount of hydrogen generated by oxidation of 100 percent of the Zircaly cladding in the active fuel zone.) A potential for hydrogen detonation is eliminated by design, i.e., limiting to hydrogen concentration in the AP1000 containment to a maximum of 10 percent. In addition, the AP1000 containment is equipped with PARs, which are not credited for severe accidents. Also, previous NRC-sponsored studies of the hydrogen issues (i.e. SECY-02-080 and SECY-00-0198) indicate that combustible gas generated from severe accidents is not risk significant for large, dry containments such as AP1000. Therefore, the staff accepts the AP1000 hydrogen control measures as adequate.

In general, the applicant claims that AP1000 provides reasonable assurance that equipment, both electrical and mechanical, designed for mitigating the consequences of severe accidents, will perform their functions as intended. Based on the review of information provided in DCD Tier 2 Chapter 19 and Appendix 19D of the AP1000 PRA supporting document, as well as staff's independent severe accident analyses, the staff finds this acceptable.

19.2.3.3.7.1 Equipment and Instrumentation Necessary to Survive

The applicant considers the actions defined by the AP600 Emergency Response Guidelines, Revision 3, May 1997 (Ref. 19D-2), and WCAP-13914, "Framework for AP600 Severe Accident Management Guidance (SAMG)," Revision 1, November 1996 (Ref. 19D-1) to be directly applicable to AP1000 design. The staff performed an independent comparison between the two designs, including independent analyses of AP1000 response to various severe accident scenarios, and concurs with such an approach.

In WCAP-13914, the applicant defines a controlled, stable core state and a controlled, stable containment state. The core state can be summarized as having a process for transferring the energy being generated in the core to a long-term heat sink such as a flooded reactor cavity. The conditions associated with this state are considered indicative of a degraded in-vessel core damage accident. The containment state can be summarized as having a process for transferring the energy that is released to an intact containment to a long-term heat sink such as the PCCS. The conditions associated with this state are considered indicative of an ex-vessel severe accident.

The applicant determined that the necessary equipment and instrumentation along with the environmental conditions varied over the course of a severe accident. Therefore, Westinghouse identified four equipment survivability time frames. Time Frame 0 is defined as the period of time in the accident sequence after accident initiation and before core uncovery. Time Frame 1 is defined as the period of time after core uncovery and before the onset of significant core damage as evidenced by the rapid oxidation of the core. Time Frame 2 is the period of time in the severe accident after the accident progresses beyond the design basis of the plant and before the establishment of a controlled, stable core state (end of in-vessel relocation), or prior to reactor vessel failure. Time Frame 3 is defined as the period of time after the reactor vessel fails until the establishment of a controlled, stable containment state or the end of the sequence. The equipment and instrumentation needed for each time frame are summarized in DCD Tier 2 Tables 19D.6-3 through 19D.6-5.

The equipment listed provides the operator with the ability to (1) inject into the RCS, steam generators and containment, (2) depressurize the RCS, steam generators and containment, (3) control hydrogen, (4) isolate containment, and (5) remove heat and fission products from the containment atmosphere. The list of equipment also includes the cavity flooding system and the containment penetrations. The instrumentation was chosen so that the operator could confirm and trend the results of actions taken and that adequate information would be available for those responsible for making accident management decisions.

The staff performed an independent assessment of the list of equipment and instrumentation provided in Tables 19D.6-3 through 19D.6-5 and compared them to the more extensive lists required by RG 1.97 and 10 CFR 50.34(f) to ensure that the equipment and instrumentation provided is sufficient. The staff concludes that the equipment and instrumentation needed to perform and monitor the mitigative functions necessary during a severe accident are adequate.

19.2.3.3.7.2 Severe Accident Environmental Conditions

The severe accident environmental conditions are discussed in Appendix D to the AP1000 PRA supporting document.

The radiation exposure inside the containment for a severe accident is estimated by considering the dose in the middle of the AP1000 containment with no credit for the shielding provided by internal structures. The instantaneous gamma and beta dose rates are provided in Figures D.1 and D.2, respectively. The source term is based on the emergency safeguards system core thermal power rating of 3,468 MWt, which includes a 2 percent power uncertainty.

The radionuclide groups and elemental release fractions are consistent with the accident source term presented in NUREG-1465, "Accident Source Terms for Light-Water Nuclear Power Plants," February 1995. The timing of the release is founded on NUREG-1465 assumptions. Westinghouse assumes an initial release of activity from the gaps of a number of failed fuel rods at 10 minutes into the accident, which is based on an NRC approved leak-before-break approach. Over the next 30 minutes, from 10 to 40 minutes into the accident, 5 percent of the core inventory of the noble gases, iodine and cesium is assumed to be released to the containment. During the early in-vessel release phase, the fuel as well as other structural

materials in the core reach sufficiently high temperatures that the reactor core geometry is no longer maintained and fuel and other materials melt and relocate to the bottom of the reactor vessel. The in-vessel phase is estimated to last 1.3 hours. The ex-vessel release phase begins when molten core debris exits the reactor pressure vessel and ends when the debris has cooled sufficiently that significant quantities of fission products are no longer being released. The ex-vessel phase is assumed to last 2 hours. The late in-vessel period continues for an additional 8 hours. Ultimately, the total fraction of radionuclides core inventory released to the containment includes 100 percent of noble gases, 75 percent of cesium and iodine, and 30.5 percent of tellurium. The staff finds the timing and duration for the early in-vessel, late in-vessel, ex-vessel and the late in-vessel release phases consistent with NUREG-1465, and, therefore, acceptable.

Evaluation of containment thermal-hydraulic conditions following selected severe accidents was performed by the applicant using the MAAP4.04 computer code. Five cases were analyzed:

(1) IGN - DVI line break with vessel reflood, cavity flooding, and igniters,
(2) IVR - same as IGN but no vessel reflood,
(3) NOIGN - 4-inch DVI line break with vessel reflood, cavity flooding, and no ingniters,
(4) CCI - large LOCA with igniters, no vessel or cavity reflood, and
(5) GLOB - global burning of hydrogen from 100-percent cladding reaction.

The timing for each case is presented in Table D-6. The key elements relate to the equipment survivability time frames, as defined above.

The staff, through its contractor at ERI performed an independent analysis of the AP1000 response to various severe accident scenarios. The selection of the accident scenarios was based on their contribution to the total Core Damage Frequency (CDF). Four scenarios were selected that constitute about 56 percent of the total AP1000 CDF. These scenarios are:

(1) 3BE - DVI line break with PRHR unavailable (29 percent of CDF),
(2) 3BR - Hot Leg Large Break LOCA (18 percent of CDF),
(3) 3D - Spurious ADS actuation (stage 1/2/3) (9 percent of CDF), and
(4) 1A - Transient initiated by loss of MFW (0.6 percent of CDF)

For equipment survivability the most important parameter is temperature. The two sets of analyses are not directly comparable since the risk dominant scenarios, selected by staff, are not the worst-case scenarios from the point of view of equipment survivability. Such an approach is acceptable because of inherent analytical uncertainties associated with current state of knowledge of the involved physical phenomena. However, if these uncertainties are imposed on both analyses and global hydrogen burning is not considered, the range of calculated environmental conditions are similar. For example, comparing two DVI line break cases, the maximum containment dome temperature in the IGN case is about 540°K (512°F), while in the 3BE case the temperature reached about 520°K (476°F).

The applicant's GLOB case represents a bounding hydrogen combustion case, burning the mass of hydrogen produced from 100 percent oxidation of the active fuel zone cladding in the core. The oxidation produced 788 kg (1710 lb) of hydrogen, and an instantaneous maximum containment temperature (Figure D-45 in Appendix D to AP1000 PRA) was about 1300°K (1880°F), while a "steady state" temperature was below 500°K (440°F). For comparison, the maximum amount of hydrogen produced in the NRC analyses (case 1A) was 621 kg (1368 lb), and maximum containment dome temperature was below 440°K (332°F).

Based on the confirmation provided in the AP1000 PRA supporting document and the independent analysis performed by the NRC's contractor (ERI) the staff concludes that the thermal hydraulic profiles predicted above by MAAP are acceptable approximations of the environmental conditions for which mitigative features and instrumentation, identified in this section, must survive.

19.2.3.3.7.3 Basis for Acceptability

In SECY-93-087, the staff recommended that the Commission approve the general criteria that the staff evaluate the ALWR vendor's review of the various severe accident scenarios analyzed and identify the equipment needed to perform its function during a severe accident and the environmental conditions under which the equipment must function. In its July 21, 1993 SRM, the Commission approved the staff's position.

The staff has performed this evaluation and concluds that the equipment and instrumentation identified by the applicant in DCD Tier 2 Tables 19D-3 to19D-5, and the applicable environments described in Appendix D to the AP1000 PRA supporting document meets the above guidance of SECY-93-087 and 10 CFR 50.34(f) as delineated in Section 19.2.3.3.7 of this report. Reasonable assurance that the equipment and instrumentation identified in this section will operate in the severe accident environment for which they are intended and over the time span for which they are needed is provided by the environmental qualification ITAAC and because of a COL Action Item. Specifically, the COL applicant referencing the AP1000 certified design will perform a thermal response assessment of the as-built equipment used to mitigate severe accidents to provide additional assurance that this equipment can perform its severe accident functions during environmental conditions resulting from hydrogen burns. This assessment is COL Action Item 19.2.3.3.7-1.

19.2.3.3.8 Containment Vent Penetration

Use of a containment vent to prevent containment over-pressure failure is a means of mitigating the consequences of a severe accident. In SECY-93-087, the staff indicated that the need for a containment vent for the passive plant designs would be evaluated on a design-specific basis, and that if acceptable analyses indicate that a vent would not be needed to meet the severe accident criteria, such as the Commission's containment performance goal discussed in Section 19.2.4 of this report, the staff would not propose to implement a vent requirement.

The staff relied on the evaluation of the containment performance goal in Section 19.2.4 of this report for determining the need for inclusion of a containment vent. As discussed therein, for

the most likely severe accident challenges, containment pressure would remain below Service Level C as a result of successful retention of core debris in-vessel, and operation of PCS. Accordingly, containment venting will not be required for the more likely severe accident sequences since they do not result in over-pressure failure.

The staff identified two situations in which venting would eventually be required, specifically, events involving either failure of PCS or RPV failure followed by unmitigated CCI. However, these events are much less likely, and do not contribute appreciably to containment failure frequency, as discussed below.

In the event of PCS failure, containment pressure would eventually reach Service Level C, necessitating containment venting (see Section 19.1.3.2.2). In the baseline PRA, the frequency of core damage events involving failure of PCS water delivery is estimated to be about 3E-13/y. With air cooling only, containment pressure is estimated to reach Service Level C at about 24 hours. In the AP600 PRA, PCS failure was dominated by blockage of the PCS annulus drain lines, which was estimated to have a probability of 1E-04. This failure mechanism is not modeled in the AP1000 PRA, but the staff estimates that given the same failure probability as assumed in AP600 this mechanism would result in a containment failure frequency of about 2E-11/y for the AP1000. Containment pressurization will initially be limited by PCS water delivered to the containment shell. However, following depletion of PCS water inventory (at approximately 72 hours) containment pressure will increase and eventually exceed Service Level C due to blockage of the air cooling path.

In the event of RPV failure followed by unmitigated CCI, containment pressure (due to non-condensible gas build-up) would reach Service Level C after about 3 days or later depending on the type of concrete used in the basemat (see Section 19.2.3.3.3). The frequency of core damage with RPV failure and relocation of core debris to the reactor cavity is 5E-09/y in the baseline PRA, on the basis of an assumption that RCS depressurization and reactor cavity flooding always result in successful retention of molten core debris in-vessel. As discussed in Section 19.2.3.3.1, the staff's review of ERVC supports this assumption for the core debris configuration considered in the related ROAAM analysis, but uncertainties in the likelihood of retaining a molten core in-vessel are large. Under the most limiting assumption of no credit for ERVC, the frequency of events that result in reactor vessel failure would approach the core melt frequency. However, the frequency of events that require containment venting would be somewhat less than this since the reactor cavity would be flooded in these sequences, potentially resulting in quenching of the core debris and termination of CCI.

The frequency of events that would necessitate containment venting is on the order of 1E-08/y founded on the PRA for internal events, and the time at which venting would be required would be 24 hours or later. This frequency could increase substantially if ERVC is not effective in preventing RPV failure. However, even with no credit for ERVC, the frequency of events requiring venting would be on the order of 1E-07/y and well below the 1E-06/y general plant performance guideline for a large release of radioactive material. The staff concludes that the containment performance goals regarding large release frequency and CCFP are met without a containment vent, and therefore, a containment vent is not required for the AP1000 design.

Although containment venting capability is not required to meet the containment performance goals it may be beneficial to depressurize the containment in a controlled manner under certain conditions during a severe accident. Westinghouse considered the impact of venting the AP1000 through penetrations with effective sizes of 10, 15, 25.4, and 45.7 centimeters (4, 6, 10, and 18 inches) in diameter. The results of the analysis show that over-pressure failure can be successfully mitigated using any of these vent sizes. Westinghouse did not specify the particular line(s) that could be used to vent the AP1000 containment. However, given the range in line sizes that would be effective for venting, and the relatively low pressure requirements associated with venting, a number of different penetrations might be used. The COL applicant, as part of COL Action Item 19.2.5-1 regarding accident management, will identify the specific penetration(s) for containment venting, and will develop and implement severe accident management guidance for venting containment using the framework provided in WCAP-13914, Revision 3.

19.2.3.3.9 Non-Safety-Related Containment Spray

Performance of numerous risk assessment studies over the past 20 years show that the risk to the public from severe accidents is usually dominated by accidents that result in early containment failure commensurate with a significant release of radioactive material. Many design features have been added to the AP1000 design to reduce this risk. Examples include allowing for depressurization of the reactor coolant system, controlling hydrogen generation, and cooling of molten core debris in-vessel. The large passively-cooled AP1000 containment provides significant benefit to cope with severe accident challenges because the failure modes of the containment heat removal system are independent of the scenarios that could lead to containment challenges and of the vulnerabilities associated with reliance on human actions. While the use of passive systems enhances the safety of the plant during early containment challenges, the ability to intervene and provide control over the course of a severe accident has significant benefit in terms of accident management. For existing plants an internal containment spray system and other features can accomplish this. However, the AP1000 relies solely on enhanced natural processes for aerosol fission product removal. The state-of-the-science for evaluating the effectiveness of natural removal processes in harsh environments has uncertainty levels that are greater than those for current operating plants that do not credit these processes.

The concept of passive safety systems is appealing because the design relies primarily on gravity. Passive safety system designs are also attractive because they minimize the need for support systems and reduce reliance on human actions. However, there are uncertainties regarding the performance of passive safety systems. Net driving forces are small compared to active systems. For example, the reliability and functionality of check valves can no longer be taken for granted in passive designs. While a sticking check valve in an active system can be easily overcome by the forces developed by a pump, there is less assurance that the low driving head developed by gravity injection in a passive design will similarly overcome a sticky check valve. In addition, the parallel flow paths existing in the AP1000, combined with the low driving heads, make calculation of flow distributions more uncertain. Although the staff is confident that, within the design basis, the testing program data and conservatisms inherent in

design basis analyses bound these uncertainties, the uncertainties become much more significant when considering severe accidents.

In the unlikely event that a severe accident in the AP1000 occurs, the cause is likely to be some combination of events and passive system failures that had not been specifically evaluated or assessed. Assuming the failure of the passive core cooling system features, the containment becomes the primary mitigation system to protect public health and safety. As with other passive systems, there are large uncertainties associated with the passive nature of the containment system design. Heat transfer and fission product removal from the AP1000 containment atmosphere is dependent upon mass condensation onto cool surfaces, predominantly the walls inside containment. Given a severe accident, the long-term buildup and distribution of non-condensible gases within the containment and their effects (as a result of stratification and increasing concentration gradients within the inner containment boundary layer) cannot be assessed with existing analytical tools.

In view of the uncertainties associated with the reliance on passive systems in mitigating severe accidents Westinghouse included a containment spray function as part of the AP1000 fire protection system design. The spray system is described in Section 6.5.2 of DCD Tier 2. This design feature is not safety-related and is not credited in any accident analysis including the dose analysis provided in Section 15.6.5 of DCD Tier 2. Existence of the non-safety spray system introduces additional possibility for operator intervention as part of the design's accident management strategy.

The possibility of inadvertent actuations of the containment spray system is evaluated in Section 6.2.1.1, "External Pressure Analysis," of this report.

The staff finds that the containment spray system proposed by Westinghouse provides the following benefits and, thereby, satisfies the staff's recommendation in SECY-97-044:

(1) the capability for site personnel upon recognition of elevated radiation levels in the containment atmosphere to quickly and substantially remove aerosol fission products following activation,

(2) mixing the containment atmosphere following a severe accident, especially the boundary layer inside the containment shell, and

(3) short term pressure reduction upon injection because of the heat capacity of the subcooled spray water.

19.2.4 Containment Performance Goal

The containment performance goal (CPG) is intended to ensure that the containment structure has a high probably of withstanding the loads associated with severe accident phenomena, and that the potential for significant radioactive releases from containment is small. The CPG includes both a deterministic goal that containment integrity be maintained for approximately 24 hours following the onset of core damage for the more likely severe accident challenges, and a

probabilistic goal that the CCFP be less than approximately 0.1 for the composite of all core damage sequences assessed in the PRA.

In SECY-93-087, the staff recommended that the Commission approve the following deterministic containment performance goal for the passive ALWRs:

> The containment should maintain its role as a reliable, leak-tight barrier (for example, by ensuring that containment stresses do not exceed ASME Service Level C limits for metal containments or factored load category for concrete containments) for approximately 24 hours following the onset of core damage under the more likely severe accident challenges and, following this period, the containment should continue to provide a barrier against the uncontrolled release of fission products.

In discussions during the Commission meeting on this subject, the staff informed the Commission that it also intends to continue to apply the probabilistic containment performance goal of 0.1 CCFP in implementing the Commission's defense-in-depth regulatory philosophy and the Commission's policy on Safety Goals. (The 0.1 CCFP goal had been proposed by the staff for evolutionary designs in SECY-90-016, and approved by the Commission in its SRM of June 26, 1990.)

In the SRM dated July 21, 1993, the Commission approved the staff's position to use the deterministic CPG in the evaluation of the passive ALWRs as a complement to the CCFP approach, subject to the staff's review and recommendations resulting from public comments on the "Advance Notice of Proposed Rulemaking on Severe Accident Plant Performance Criteria for Future ALWRs." In SECY-93-226, "Public Comments on 57 FR 44513 - Proposed Rule on ALWR Severe Accident Performance", the staff provided the Commission with a summary of public comments received regarding the ANPR, and recommendations regarding policy issues raised in these comments. On the basis of a review of these comments and experience gained from the evaluation of the evolutionary reactor designs, the staff concluded that use of both a deterministic and probabilistic containment performance goal should be pursued for the passive reactor designs. Accordingly, the staff has considered both the deterministic and probabilistic CPGs in assessing the performance of the AP1000 containment.

19.2.4.1 Deterministic Containment Performance Goal

The staff used the deterministic containment performance criteria to confirm that an acceptable level of containment performance has been achieved. For purposes of this evaluation, containment failure was defined as events in which the containment fails to maintain its role as a reliable, leak-tight barrier for approximately 24 hours following the onset of core damage, or following this period, fails to continue to provide a barrier against uncontrolled release of fission products. Containment was assumed to fail if any of the following conditions occur (even if the conditions occur after 24 hours):

- internal pressure exceeds the value associated with ASME Code Service Level C Limits
- the containment is bypassed, such as in SGTR and ISLOCA events

- the containment fails to isolate
- containment seal materials fail as a result of over-temperature
- molten core debris melts through the concrete basement into the subsoil

Controlled venting of containment would not constitute containment failure provided venting occurs after approximately 24 hours following onset of core damage.

On the basis of the Level 2 PRA results, the more likely severe accident challenges are defined by sequences in which the RCS is fully depressurized, the reactor cavity is flooded, the reactor vessel is reflooded and intact, the containment is isolated, and the PCS and hydrogen igniter systems are operable. (Such sequences represent more than 90 percent of the core damage frequency). Each of these sequence characteristics is directly attributable to corresponding safety-grade features incorporated in the AP1000 design, and the very low contribution of station blackout sequences to core damage frequency. The peak containment pressure for these sequences would be on the order of 207 kPa (30 psig), and the long-term pressure would be on the order of 69 kPa (10 psig) to 138 kPa (20 psig).

All relevant severe accident challenges were evaluated for the these sequences, including hydrogen combustion, high pressure melt ejection, temperature-induced creep rupture of steam generator tubes, fuel-coolant interactions, and core-concrete interactions. These phenomena do not contribute to containment over-pressure or over-temperature failure because of operation of the safety systems incorporated in the AP1000 design. Specifically, operation of the hydrogen igniter system produces peak hydrogen burn pressures well below Service Level C, and eliminates the potential for deflagration-to-detonation transitions. RCS depressurization eliminates high pressure melt ejection and temperature-induced SGTR challenges, and terminates fission product releases to the environment in SGTR and ISLOCA events. Reactor cavity flooding, in conjunction with RCS depressurization, provides reasonable assurance that core debris will be retained within the reactor vessel, thereby preventing ex-vessel FCIs, core concrete interactions/basemat melt-through, and long-term over-pressurization of containment. The operation of PCS, in conjunction with reactor cavity flooding, maintains containment pressure below Service Level C and containment temperature below levels where over-temperature failure would be a concern. Finally, core damage events involving failure of containment isolation account for less than one percent of the total core damage frequency in the baseline PRA.

For the less likely events in which these safety-grade systems do not operate, the probability of containment failure from the associated severe accident phenomena is assessed in the Level 2 PRA and in separate deterministic calculations of each phenomena described elsewhere in Section 19.2 of this report, i.e., hydrogen combustion (Section 19.2.3.3.2), high pressure melt ejection (Section 19.2.3.3.4), ex-vessel FCI (Section 19.2.3.3.5.2), and core concrete interactions (Section 19.2.3.3.3). The results of these assessments indicate that the containment is generally capable of withstanding the challenges from these phenomena, with a small attendant probability of containment failure. The probability of containment failure is addressed below in the context of the probabilistic containment performance goal. The contribution of the various phenomena to the overall containment failure frequency is described further in Section 19.1.3.2.2 of this report.

On the basis of the availability of the severe accident mitigation design features in the majority of the core damage sequences, and the ability of the containment to accommodate the corresponding severe accident loads, the staff concludes that the AP1000 containment will maintain its role as a reliable, leak-tight barrier for the more likely severe accident challenges, in accordance with the deterministic containment performance goal.

19.2.4.2 Probabilistic Containment Performance Goal

The staff used the probabilistic containment performance criteria to confirm that an acceptable level of containment performance has been achieved, and to identify important contributors to containment failure. For purposes of calculating containment failure frequency, containment failure was defined as above, with the exception that containment over-pressure failure was on the basis of a plant-specific containment failure probability distribution (containment fragility curve) rather than the Service Level C Limit. Using this approach, the probability of containment failure reflects best-estimate structural capabilities and associated uncertainties rather than the more conservative assumption that containment failure occurs whenever Service Level C is exceeded. A general plant performance guideline of 1E-06/y for a large release of radioactive material (as proposed in the Safety Goal Policy Statement) and a conditional containment failure probability goal of 10 percent (as discussed above) were used as points of reference for the probabilistic assessment. As described in Section 19.1.3.2, essentially all of the containment failure frequency (99 percent) is the result of either containment bypass, containment isolation failure, or early containment failure. Thus, containment failure frequency and large early release frequency are equivalent in this application.

The containment failure frequency for internal events is 1.9E-08/y in the baseline PRA, which is nearly two orders of magnitude below the large release guideline. The corresponding CCFP is 8.1 percent, which is below the CCFP goal. In Section 19.1.3.2.4 the staff discusses the results of the probabilistic assessment and supporting sensitivity analyses. Through these analyses the staff concludes that for reasonable variations in Level 2 input assumptions and CET split fractions, increases in the containment failure frequency and CCFP are limited to a factor of about 3, and the containment failure frequency remains below 1E-07/y. Also, modest changes in the containment failure probability distribution used in the analysis would not noticeably impact the containment failure frequency since the bulk of the containment failures in the existing analyses are driven by the frequency of events with failure of RCS depressurization or reactor cavity flooding, rather than the frequency at which containment pressure loads exceed the containment pressure capability.

The staff concludes that the AP1000 containment design satisfies the Commission's probabilistic containment performance goal. Specifically, the estimated containment failure frequency in the baseline PRA is well below the large release guideline of 1E-06/y. The conditional containment failure probability is below the CCFP goal of 10 percent in the baseline PRA. Although the CCFP goal is exceeded in several sensitivity cases, these increases are modest, and the corresponding containment failure frequencies remain well below 1E-06/y. In view of the approximate nature of the containment performance goal, the recognition that PRA results contain considerable uncertainties, and the fact that under more realistic modeling

assumptions a large fraction of the containment failures reflected in the calculated CCFP in the baseline PRA would actually involve late basemat melt-throughs (or no containment failures) rather than early releases to the atmosphere, the staff concludes that the AP1000 design satisfies the Commission's goals for both large release frequency and CCFP.

19.2.5 Accident Management

Accident management (AM) encompasses those actions taken during the course of an accident by the plant operating and technical staff to (1) prevent core damage; (2) terminate the progress of core damage if it begins and retain the core within the reactor vessel; (3) maintain containment integrity as long as possible; and (4) minimize offsite releases. AM, in effect, extends the defense-in-depth principle to plant operating staff by extending the operating procedures well beyond the plant design-basis into severe fuel damage regimes, and by making full use of existing plant equipment and operator skills and creativity to terminate severe accidents and limit offsite releases.

On the basis of PRAs and severe accident analyses for the current generation of operating plants, the NRC staff concluded that the risk associated with severe accidents could be further reduced through improvements to utility accident management capabilities. Although future reactor designs such as the AP1000 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, focus, and overall importance 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 relieve the operators of the need for rapid decisions, and permit a greater reliance on support from outside sources. For longer times after an accident (several hours to several days), human intervention and accident management will continue to be needed.

The nuclear power industry initiated a coordinated program on accident management in 1990. This program involves the development of three major products as follows: (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, a plant-specific accident management plan has been implemented at each operating plant as part of an industry initiative.

For both operating and advanced reactors the overall responsibility for AM, including development, implementation, and maintenance of the accident management plan, lies with the nuclear utility, since the utility is ultimately responsible for the safety of the plant and for establishing and maintaining an emergency response organization capable of effectively responding to potential accident situations. However, the development and implementation of accident management in future reactors involves both the reactor designer and the plant

owner/operator, particularly in view of the fact that many of the design details are still to be developed (such as balance of plant equipment and final piping layout). The plant designer is responsible for developing the technical bases for the plant-specific accident management program or plan, whereas the owner/operator is responsible for developing and implementing the complete accident management plan, including those areas beyond the purview of the plant designer, such as the content and techniques for severe accident training, and the delineation of decision making responsibilities at a plant specific level.

In DCD Tier 2 Westinghouse identifies COL item number 19.59.10-4 for the COL applicant to develop and submit an accident management plan. This was previously identified as COL Action Item 19.2.5-1. The plan will provide a commitment to perform a systematic evaluation of the plant's ability to deal with potential severe accidents, and to implement the necessary enhancements within the detailed plant design and organization, including severe accident management guidelines and training. General areas that will be addressed in the plan include the following five items: (1) accident management strategies and implementing procedures, (2) training in severe accidents, (3) guidance and computational tools for technical support, (4) instrumentation, and (5) decision making responsibilities.

All AP1000 PRA insights and COL action items that fall within the scope of accident management should be specifically addressed as part of the COL applicant's accident management plan, including:

- development of detailed guidance and procedures for the use of the severe accident features in the AP1000 design, including the ADS (manual actuation after core uncovery), the hydrogen igniter system, the reactor cavity flood system, the containment spray system, and containment venting.

- development of guidance and procedures on protection of fission product barriers, including:

    - filling the SGs, and avoiding SG depressurization if water is not available, in order to prevent a thermally-induced SGTR,

    - depressurizing the RCS and maintaining a secondary side water level covering the SG tubes in order to mitigate fission product releases from a SGTR event,

    - using the containment spray system and associated water sources for containment fission product scrubbing in events with intact or vented containments, and

    - using containment venting to control fission product releases.

- development of guidance and procedures for actions that are expected to be taken in the longer-term (post-72 hours), including:

    - using the ancillary ac diesel generators to power the post-accident monitoring system, main control room lighting, and the PCS recirculation pumps,

- aligning and using the PCS recirculation pumps to refill the PCCWST from a mobile water source using power from the ancillary diesel generators,

- changeover of the main control room habitability system from air bottles to circulation using diesel-powered ancillary fans,

- water makeup to the spent fuel pool and containment, and

- reflooding a damaged core which is retained in-vessel.

- development of guidance and procedures for actions that may need to be taken in events during shutdown operations, such as actions to flood the reactor cavity.

- evaluation of information needed to implement the accident management guidelines, and plant instrumentation that could be used to supply the needed information considering instrumentation availability and survivability under severe accident conditions.

The applicant has developed a framework to guide the COL applicant in the development of plant-specific AM guidance for the AP1000 design. This guidance, documented in WCAP-13914, Revision 3, includes a discussion of the anticipated structure for the decision making process, the goals that must be accomplished for severe accident management, a summary of possible strategies for AP1000 severe accident management, and potential adverse impacts of AM strategies. The COL applicant is expected to follow the recommendations provided in WCAP-13914, Revision 3 in developing their plant-specific AM guidance. This is COL Action Item 19.2.5-1.

The staff will review the accident management plan at the COL stage to assure that the evaluation process and commitments proposed by the COL applicant provide an acceptable means of systematically assessing, enhancing, and maintaining AM capabilities, consistent with staff expectations. This plan should be developed on the basis of 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. As previously discussed this is COL Action Item 19.2.5-1.

19.2.6 Conditional Containment Failure Probability Distribution

This evaluation is based on Revision 0 which was not changed in Revision 2 of Chapter 42 of the AP1000 PRA.

19.2.6.1 Background

The containment structure for a standard plant design is required to have a high probability of withstanding the loads associated with severe accident phenomena, and that the potential for significant radioactive releases from containment is small. The containment performance requirement includes both a deterministic goal that containment integrity be maintained for

approximately 24 hours following the onset of core damage for the more likely severe accident challenges, and a probabilistic goal that the CCFP be less than approximately 0.1 for the composite of all core damage sequences assessed in the PRA.

In the deterministic approach for ensuring containment structural integrity against severe accident internal pressure, a design limit is established. This limit is the pressure at which Service Level C stress limit of the ASME Code is reached. The AP1000 containment structure has several failure modes, and the mode that yields the lowest capacity is the deterministic capacity. Amongst the various containment failure modes, there are two buckling failure modes, one is a local buckling and the other is a global buckling. It should be noted that at Service Level C a factor of safety of 1.67 applies to the local buckling capacity in accordance with the ASME Code Case N284; whereas, a factor of safety of 2.5 applies to the global buckling mode in accordance with ASME Code Section III, Subsection NE, paragraph 3222. How the applicant used the factors of safety associated with the two buckling modes is further evaluated below.

The probability distribution of containment failure is generated to evaluate containment fragility due to internal pressure from various accident scenarios. The applicant has used an approach similar to that used in the AP600 design. The applicant developed the CCFP distribution from various failure modes determined by structural calculations, and assumed that the failure modes are independent of each other. Chapter 42 of the AP1000 PRA, describes the limiting containment failure modes as:

- General yielding of the cylindrical shell,
- Buckling of the ellipsoidal upper head,
- Buckling of 16-ft. diameter equipment hatch covers, and
- Yielding of personnel airlocks

Other containment failure modes (e.g., yielding of the ellipsoidal head, piping penetrations, mechanical penetration bellows, functional loss of containment due to ovalization of the equipment hatches) were not developed further, because general yielding of the cylindrical part of the containment shell occurs at a substantially lower internal pressure. The staff agrees with this determination.

19.2.6.2 Deterministic Containment Capacity

The evaluation of ultimate capacity of the AP1000 containment is presented in DCD Tier 2 Section 3.8.2.4.2. In this section, the applicant evaluates the containment capacity at Service Level C limit by examining various parts of the containment structure, cylindrical shell, top and bottom heads, equipment hatches and covers, personnel airlocks, and mechanical and electrical penetrations. At Service Level C, the applicant determined that the capacity of the ellipsoidal head is 627 KPa (91 psig) at 149°C (300°F) and the capacity of the equipment hatch covers is 558 KPa (81 psig) at 149°C (300 °F) using NE 3222. Using Code Case N284, the capacity of the equipment hatch covers was determined to be 834 KPa (121 psig) at 149°C (300°F). The staff has always maintained that the provisions of Code Case N284 apply to local buckling cases only. The equipment hatch cover buckling is a global buckling phenomenon and

therefore, the use of Code Case N284 is not appropriate. The Service Level C capacity of the AP1000 containment structure should be the lowest value, 558 KPa (81 psig) at 149°C (300 °F). In Section 42.3.1 of the PRA, the applicant states, “The 90 psig [620 KPa] is the Service Level C containment failure pressure at 300°F.” The staff does not agree with this assessment. The applicant should address why 558 KPa (81 psig) at 149°C (300 °F) is not the limiting severe-accident pressure for the AP1000 containment. This is Open Item 19.2.6-1

19.2.6.3 Probabilistic Model

The applicant used the best estimate of the failure pressure from each failure mode with its associated random and modeling uncertainties in the development of the probability distribution. The applicant considered the Gaussian, Gamma, Gumbel, lognormal and Weibull distributions, and selected the lognormal distribution. The lognormal distribution is considered a reasonable distribution since the statistical variation of many material properties can be represented well by this distribution, provided one is not primarily concerned with extreme tails of the distribution. The engineering calculations to determine the strength of the containment is multiplicative, since the capacity changes due to material properties or the thickness of the shell are multiplicative. In addition, a distribution of a random variable consisting of products and quotients of several variables tends to be lognormal even if the individual variable distributions are not lognormal. The pressure capacity for a given failure mode is described by $P = P_m \cdot M \cdot S$, where (1) P_m is the median pressure capacity representing the internal pressure Level for which there is a 50 percent probability of failure, (2) M is a lognormally distributed random variable having a unit median value and a logarithmic standard deviation, $ß_M$, representing the uncertainty as a result of analytical modeling, and (3) S is also a lognormally distributed random variable having a unit median value and the logarithmic standard deviation, $ß_S$, representing the uncertainty associated with the material properties. Therefore, since the pressure capacity is a random variable which is the result of the product of several other random variables, the pressure capacity is well represented by a lognormal distribution. The staff finds that the use of lognormal distribution for the containment pressure capacity is reasonable and acceptable.

The use of a lognormal distribution requires a determination of the median values of failure pressures from various containment failure modes and consideration of variabilities of the associated parameters. The applicant used the best estimate failure capacity values for each of the containment failure modes using the expected material yield stress to arrive at the median values of CFP at 204°C (400°F) and 166°C (331°F). The best estimate capacity takes into account the expected behavior of the containment structure using realistic natural properties; therefore, it is appropriate to use this value as the median capacity.

The applicant has considered three sources of uncertainty that can influence the median value of the containment failure pressure (CFP). These are geometric properties, structural analysis, material properties and gross errors. However, the applicant did not incorporate the effect of uncertainty from geometric properties because of the insensitivity to the CFP of the geometric property. The overall uncertainty in the containment strength is generally insensitive to variations in geometric properties such as fabrication and erection tolerances on plate thickness, size, and dimensions, except for the buckling mode of failure (L. Greimann and F. Fanous, "Reliability of Containments under Overpressure," Pressure Vessel and Piping

Technology, 1985, pp. 835 - 856). With respect to the buckling failure mode, the use of knockdown factors incorporates the uncertainty in the CFP. The applicant has determined CFP values that have a conservative bias; therefore, the use of median values without an explicit consideration of uncertainty from geometric properties would tend to overstate the CFP. The staff finds the approach used by the applicant acceptable.

From the staff's previous reviews of standard designs, modeling uncertainties have been found to have a significant effect in the probability of the containment structure failure. NUREG/CR-2442 recommends that the coefficient of variation (COV) be 0.12 for all practical instances of modeling error. The applicant has used a value of 0.12 for the consideration of structural uncertainty. The value of the COV used by the applicant is acceptable.

In order to consider uncertainty in the material property value, the applicant used a value of 0.11 as the COV which is consistent with two references, (1) "Reliability of Containments under Overpressure," by L. Greimann and F. Fanous, Pressure Vessel and Piping Technology, 1985, pp. 835 - 856, and (2) "Development of a Probability Based Load Criterion for American National Standard A58," National Bureau of Standards Special Publication 577, US Government Printing Office, Washington, DC, 1980. Therefore, the use of this value of the COV for material property variation is acceptable because it is based on recommendations of two studies.

Gross errors in construction and design are not quantifiable, or predictable by reliability methods. Gross design and construction errors can lead to catastrophic results. Careful attention is paid to quality assurance in nuclear power plant design and construction. In addition, the containment structure is subject to a structural integrity test prior to placement in service. the applicant did not explicitly consider uncertainty due to construction and design error in developing its containment fragility curves. The approach used by Westinghouse is consistent with the current practice.

19.2.6.4 Containment Fragility Evaluation

As discussed in the background section, the applicant considered four failure modes for which the best estimates of failure pressures are calculated using realistic material properties as described below. In each case, the best estimate value is used as the median value along with coefficients of variations of 0.11 and 0.12 for material property and modeling uncertainty respectively.

19.2.6.4.1 Cylindrical Shell Capacity

The median capacity value for the shell is calculated as 1.01 MPa (147 psig) at 166°C (331°F) and 0.93 MPa (135 psig) at 204°C (400°F) using realistic material property and nominal design thickness. Therefore, the staff finds the median capacity value acceptable.

19.2.6.4.2 Buckling of Ellipsoidal Upper Head

The median capacity value for the buckling of the ellipsoidal head is calculated as 1.14 MPa (166 psig) at 166°C (331°F) and 1.1 MPa (159 psig) at 204°C (400°F) using realistic material property, nominal design thickness, and appropriate analytical method for the prediction of buckling. Therefore, the staff finds the median capacity value acceptable.

19.2.6.4.3 Buckling of the Two 4.87 m (16 ft) Diameter Equipment Hatch Covers

The calculated critical buckling pressure for the equipment hatch covers is 1.45 MPa (211 psig) at ambient condition, as discussed in DCD Tier 2 Section 3.8.2.4.2.3. In Section 42.4.3 of the AP1000 PRA, it is shown that a factor of 1.5 was used as a multiplier to the calculated buckling pressure at ambient condition of 38°C (100°F), based on the test head data. Using the multiplier of 1.5 and adjusting for the reduction in material strength due to temperature, the applicant has calculated the median capacity value for the buckling of the two 4.87 m (16 ft) diameter equipment hatch covers as 2.14 MPa (311 psig) at 166°C (331°F) and 2.05 MPa (297 psig) at 204°C (400°F). However, as noted in DCD Tier 2 Section 3.8.2.4.2.2, one of the test results shows a reduction of 0.79 and the other test result shows a factor of 1.0 on the predicted BOSOR-5 value. Therefore, the staff considers that the use of the multiplier of 1.5 is not justified. Consequently, the staff does not agree with the values shown in Tables 42-1 and 42-2 of the PRA. This is Open Item 19.2.6-2.

19.2.6.4.4 Yielding of Personnel Airlocks

The applicant estimates the failure pressure of the personnel airlock to be at least 2.07 MPa (300 psig). Therefore, the applicant considers the contribution of the personnel air locks to the CCFP to be negligible. The staff agrees with this assumption because the capacities of the personnel airlocks far exceeds the capacity .related to other failure modes.

19.2.6.5 Overall Probability Distribution

The applicant has used the estimated median and COV values for the above failure modes, as shown in Tables 42-1 and 2 of the PRA for two sets of temperatures, 204°C (400°F) and 166°C (331°F), respectively. The applicant has developed the CCFP at the corresponding temperatures considering the above failure modes as independent. It is not clear whether or not the contribution to the CCFP from each equipment hatch has been taken as independent as well. Contributions to the CCFP from the equipment hatches are at least two orders of magnitude less than other contributions at 1.38 MPa (200 psig) internal pressure, and much less than that at lower internal pressures. Consequently, the influence of equipment hatch failure mode on the overall CCFP is negligible. Nevertheless, Chapter 42 of the PRA should be revised to clarify the approach used by the applicant. This is Open Item 19.2.6-3.

19.2.6.6 Conclusion

Using the lower value of 558 KPa (81 psig) at 149°C (300 °F) as the deterministic capacity of the containment structure, the probability of failure is less than 9.6E-5.

Therefore, subject to the resolution of the three identified open items, 19.2.6- 1, 19.2.6-2 and 19.2.6-3, the staff concludes that the analysis methodology and the procedures used by Westinghouse are appropriate and acceptable for the deterministic and probabilistic analyses of the AP1000 containment function in protecting public health and safety.

19.3 Shutdown Evaluation

19.3.1 Introduction

As part of the design certification process for the AP1000 design, the NRC has determined, in accordance with SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," issued April 2, 1993, that concerns about shutdown operations should be satisfactorily addressed before the final design approval on the ALWR is issued. The NRC requested the ALWR applicants to perform a systematic assessment of the shutdown risk issue to address concerns identified in NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," as they are applicable to the plant design. The assessment should include:

- an evaluation of risks associated with shutdown and low-power operation, (including design specific vulnerabilities, weaknesses, and consideration of fire and floods with plant in Modes other than full-power), and

- a demonstration that these risks have been considered, and that the design features that minimize shutdown and low-power risk probability have been incorporated.

The applicant has performed its systematic evaluation of the shutdown operations and provided the results of its evaluation in DCD Tier 2 Appendix 19E, "Shutdown Evaluation." The applicant evaluated the AP1000 design for risks associated with plant conditions in Mode 4 (safe shutdown), Mode 5 (cold shutdown) and Mode 6 (refueling). The applicant concluded that the AP1000 is designed to mitigate all design-basis events that can occur during shutdown modes, and the risk of core damage as a result of an accident that may occur during shutdown modes is acceptably low.

The staff based its review of this submittal on insights from NUREG-1449 and a PRA of shutdown and low-power operating modes for PWRs to screen for important accident sequences. The purpose of the staff’s review is to ensure that the AP1000 design has appropriately addressed the shutdown risk concerns on the basis of experience with operating plants, including appropriate vendor guidelines for COL applicants, in areas of outage planning and control, fire protection, and instrumentation. The staff reviewed design improvements to ensure that insights from shutdown operation experiences are appropriately addressed, and that the design improvements reduce the likelihood of core damage and enhance public health and safety. Also, the staff evaluated vulnerabilities that may result from new design features; decay heat removal capability using the RNS; treatment of fires and floods with the plant in modes other than full-power; safety analyses for shutdown operations; related technical findings discussed in NUREG-1449; and the effectiveness of the RTNSS proposed by the design certification applicant. The staff’s evaluation is provided as follows.

19.3.2 Design Features That Minimize Shutdown Risk

The applicant describes the AP1000 design features that minimize shutdown risk in DCD Tier 2 Apendix 19E, "Shutdown Evaluation." These features are discussed in the following sections of this report.

19.3.2.1 Decay Heat Cooling System

The AP1000 design includes a redundant RNS, which is used to perform normal plant cooldown. The detailed RNS design is discussed in DCD Tier 2 Section 5.4.7, "Normal Residual Heat Removal System." The RNS is a non-safety-related defense-in-depth system, that consists of two mechanical trains of decay heat removal. Each train includes a pump, a heat exchanger and the system piping and valves, and is located in the auxiliary building. The two RNS trains share a common suction line from the RCS and a common discharge header that splits inside containment to return flow to the RCS via the two DVI lines. In the event that a loss of RNS cooling occurs during shutdown operations, an alternate core cooling capability is provided by a passive safety-related injection system, using the IRWST, that injects water into the RCS via the DVI line. Other alternative core cooling capabilities, as discussed in DCD Tier 2 Section 6.3, "Passive Core Cooling System," and Appendix 19E, can be achieved using the accumulators, the CMTs and PRHR.

The IRWST is available for long-term RCS makeup. The actuation of the IRWST injection path relies on a low-2 CMT water level signal, which is available in Modes 3, 4 and 5 with the RCS intact. When the RCS is open, the IRWST can be actuated on a low hot-leg level signal.

The accumulators are available for safety injection, until Mode 3. When the RCS pressure is reduced below the normal accumulator pressure, the accumulator valves are isolated to block the accumulator injection.

During shutdown, the CMTs are available in Modes 3 through 5, until the RCS pressure boundary is open and pressurizer water level is reduced. Because the RCS temperature and pressure, and the low steam line pressure signals are blocked in Mode 3 prior to cooling and depressurizing the RCS, the actuation of the CMTs during a loss of inventory event relies on a low pressurizer level signal in Mode 3 through 5. In Mode 5 with the RCS open for reduced inventory operations, the low pressurizer level signal is blocked prior to draining the RCS, and therefore, the CMTs are not available and the RCS makeup is provided by the IRWST.

The PRHR is available for decay heat removal in Modes 1 through 5, with the RCS intact. The PRHR is actuated on a CMT actuation signal. In Modes 5 and 6 with the RCS open, the decay heat removal is provided by feeding water from the IRWST and bleeding from the ADS.

In DCD Tier 2 Section 16.1 "Technical Specifications", the TSs specify the limiting conditions for operation (LCOs) for the above safety related systems. In DCD Tier 2 Section 13.5.1, "Combined License Information Item," the applicant includes insights from DCD Tier 2 Appendix 19E, "Shutdown Evaluation," which indicates that the COL applicant will address plant procedures for normal and abnormal operations; emergency operation; refueling and outage

planning; alarm response; maintenance; inspection; test and surveillance, as well as administrative controls. This is COL Action Item 19.3.2.1-1.

19.3.2.2 Onsite Power Systems

The AP1000 onsite power systems (OPS) arrangement includes the following power supply sources:

- The preferred power supply is from the high-voltage switchyard through the plant main stepup transformers and two unit auxiliary transformers. Each unit auxiliary transformer supplies power to about 50 percent of the plant loads.
- A maintenance source is provided through a reserve auxiliary transformer.
- Two non-safety-related onsite standby diesel generators are furnished with their own support subsystems.
- A Class 1E dc power and uninterruptible power supply system provides reliable power for the safety-related equipment required for the plant instrumentation, control, monitoring, and other vital functions needed during shutdown operations.

19.3.2.3 Decay Heat Removal Capabilities During Shutdown and Mid-Loop Operations

The applicant has incorporated into the AP1000, design features that address issues related to low-power and shutdown operations, especially during mid-loop operations. These design features include the following: (1) RNS self-venting path, (2) RCS loop piping offset, and (3) RNS step-nozzle connection. These design features are discussed integrally in the shutdown operation discussions of the AP1000 design.

19.3.2.3.1 RNS Self-Venting Path (DCD Tier 2 Section 19E.2.4.2.2)

While the RCS water level is lowered to within the hot-leg (mid-loop) to allow maintenance and testing activities, the risk of losing decay heat cooling increases, as a result of the increased likelihood of vortexing at the RNS pump suction. Also, air entrained in the RNS piping may hinder the ability to provide adequate shutdown cooling during mid-loop operation. In addressing this concern, the applicant designed the RNS piping, to each respective pump suction, in a continuously downward sloping path from the RCS hot-leg, thereby creating a self-venting path with no high point areas and no loop seals. The staff considers that the RNS self-venting path design is an improvement in the AP1000 design to minimize the potential air entrainment of the RNS during mid-loop operation, and therefore, the staff concludes that the design is acceptable.

19.3.2.3.2 RCS Piping Offset Layout (DCD Tier 2 Sections 19E.2.1.2.1 and 19E.2.3.3.1)

The layout of the RCS hot-leg piping and the SG channel head allows the hot-leg to be drained to a level that is much higher than existing operating plants for nozzle dam installation. The

AP1000 RCS hot-leg and cold-legs are vertically offset, and this piping offset provides a higher margin of operation to prevent vortex formation in the RNS pump suction during mid-loop operation. The TSs specify (DCD Tier 2 Chapter 16, Table B 3.0-1) that ADS first-, second- and third-stage valves be open and fourth-stage valves be operable, whenever the CMTs are blocked, during shutdown conditions, with the reactor vessel upper internals in place. In accordance with Items 10.c and 22.c of TS Table 3.3.2-1, the IRWST injection valves and fourth stage ADS valves are required to open on the RCS hot-leg low level signal. The TS requirements establish an RCS vent path that precludes inadvertent repressurization of the RCS during shutdown conditions in the event of a loss of decay heat removal, and also allow the IRWST to inject water into the RCS following a sustained loss of decay heat removal. The staff finds that the layout of the RCS hot-leg piping provides a large margin of available water in the RCS that will minimize the potential loss of RNS cooling, during mid-loop operation due to air entrainment. Also, the availability of the ADS, for RCS venting, minimizes inadvertent repressurization of the RCS and allows the IRWST injection to the RCS. Therefore, the staff concludes that the applicant's design improvement for the RCS piping layout is acceptable.

19.3.2.3.3 RNS Step-Nozzle Connection (DCD Tier 2 Section 19E.2.1.2.3)

One of the design features, that prevents air binding of the RNS pump during mid-loop operation, is the step-nozzle connection to the RCS hot-leg. The step-nozzle connection substantially reduces the critical RCS hot-leg level at which a vortex can occur in the RNS pump suction line, because it reduces the fluid velocity in the hot-leg step-nozzle, and limits the amount of air entrainment into the pump suction, should a vortex occur, to no greater than 5-percent, while continuing to provide decay heat cooling. The applicant relies on the test data and analysis included in a test report, APWR-0452, "AP600 Vortex Mitigation Development Test for RCS Mid-Loop Operation," dated July 6, 1994, to support the adequacy of the AP1000 step-nozzle design. The report describes the scaled tests and analysis, which investigate the vortex behavior at the RNS line and hot-leg junction, during mid-loop operation.

In RAI 440.122, the staff requested that the applicant justify how the report, APWR-0452, is applicable to the AP1000 design. In a letter dated October 18, 2002, the applicant responded to RAI 440.122 by stating that the test program and data analysis of APWR-0452 resulted in a correlation between the Froude number for the RNS flow conditions in the RNS step-nozzle and the critical vortexing water level in the hot-leg, with respect to the bottom of the hot-leg inside diameter. The critical vortexing water level is that hot-leg level below which the vortex will cause air to be entrained in the water flowing to the pump. Since the applicant confirmed that the Froude number resulting from the AP1000 flow rate is within the valid range for the correlation, it indicated that the correlation can be applied to the AP1000. The correlation shows that the normal mid-loop hot-leg operating level is greater than the predicted critical vortexing level. Also, the test data and analysis demonstrate that the step-nozzle prevents the vortex from being drawn down to the RNS pumps, and that the pumps can continue to operate when the water level in the hot-leg drops below the critical vortexing water level. Since the applicant confirmed that the AP1000 RNS step-nozzle size and flow conditions are within the range of the scaled RNS flow testing conditions, the staff determines that the APWR-0452 report is applicable to the step-nozzle design for the AP1000. Therefore, the staff concludes

that a step-nozzle is an improvement in the AP1000 design to minimize the potential air entrainment of the RNS pumps during the mid-loop operation, and its design is acceptable.

19.3.2.4 Containment

During shutdown operations, the applicant identified the need for the containment and containment cooling to maintain cooling water inventory, following a loss of the RNS. Following loss of the RNS, the RCS will heat up and release steam to the containment environment. If the containment is closed and sufficient cooling is provided through the containment shell to condense the steam, the condensate will eventually drain back to the RCS, providing a long term decay heat removal path. A closed containment, also known as containment closure, for shutdown operations, is not the same as containment integrity normally associated with power operations. For example, containment closure relies upon a single barrier in each penetration, and leak testing of the containment or the containment penetrations is not required.

In DCD Tier 2 Section 19E.2.6, the applicant committed to providing the ability to achieve containment closure, during shutdown operations, for events that may result in a steam release to the containment. Containment closure consists of the ability to establish a single pressure resistant barrier in penetrations providing a direct release path to the atmosphere, before the time that steam would be released to the containment. The pressure resist barriers will have a design pressure equivalent to the containment design pressure of 508.12 kPa (59 psig). If the large equipment hatches are open during shutdown operations, a self-contained power source will be provided to ensure that the hatch can be closed when needed. In addition, when the decay heat is greater than 9 MWt, the PCS will be available. For the reasons set forth above, the staff finds the proposed containment-related aspects of the AP1000 design, needed to maintain cooling water inventory during shutdown operations, to be acceptable.

19.3.2.5 Reactor Cavity Seal

Current plants use temporary reactor cavity seals to flood the refueling cavities. Failure of these seals can divert water to the reactor pit, and subsequently to the reactor floor drains which may result in a loss of shielding and fuel cooling during spent fuel assembly movement. The AP1000 design has incorporated a permanently welded seal ring between the vessel flange and the refueling cavity floor. This refueling cavity seal is part of the refueling cavity and is seismic Class I. The applicant also stated in DCD Tier 2 Section 19E.2.8 that the cavity seal is designed to accommodate the thermal transients associated with the reactor vessel flange. The AP1000 permanent seal eliminates the failure mechanism that exists with temporary pneumatic seals for some current plants.

In addition, the applicant stated that there are a total of five piped connections to the refueling cavity at levels below what is necessary for fuel movement, and that during refueling these connections will be isolated by valves and/or flanges that will be locked and maintained under administrative control. The staff find this response acceptable to address this issue.

19.3.2.6 Spent Fuel Pool Cooling

The staff reviewed the spent fuel pool cooling and purification system (SFPCPS) in accordance with Standard Review Plan (SRP) Section 9.1.3, "Spent Fuel Pool Cooling and Cleanup System." The staff's acceptance of the SFPCPS design is contingent on whether the design complies with the requirements of GDC 2, "Design Bases for Protection Against Natural Phenomena;" GDC 4, "Environmental and Dynamic Effects Design Bases;" GDC 5, "Sharing of Structures, System, and Components;" GDC 44, "Cooling Water;" GDC 45, "Inspection of Cooling Water System;" GDC 46, "Testing of Cooling Water System"; GDC 61, "Fuel Storage and Handling and Radioactivity Control;" GDC 63, "Monitoring Fuel and Waste Storage," and 10 CFR Part 20, "Standards for Protection Against Radiation," Paragraph 20.1101(b), as discussed in Section 9.1.3 of this report.

The AP1000 spent fuel cooling system is a non-safety-related system. The system is not required to operate to mitigate design-basis events. In the event the spent fuel cooling system is unavailable, spent fuel cooling is provided by the heat capacity of the water in the pool. Connections to the spent fuel pool are made at an elevation to preclude the possibility of inadvertently draining the water in the pool to an unacceptable level. In the event of loss of normal spent fuel pool cooling, a 7-day supply of makeup water is available.

The spent fuel pool cooling system consists of two mechanical trains of equipment. Each train consists of one spent fuel pool pump, one spent fuel pool heat exchanger, one spent fuel pool demineralizer, and one spent fuel pool filter. The two trains of equipment share common suction and discharge headers. In addition, the spent fuel pool cooling system comprises piping, valves, and instrumentation necessary for system operation.

Either train of equipment can be operated to perform any of the functions required of the spent fuel pool cooling system, independently of the other train. One train is continuously cooling and purifying the spent fuel pool while the other train is available for water transfers or IRWST purification, or is aligned as a backup to the operating train of equipment.

Both trains are designed to process spent fuel pool water. Each pump takes suction from the common suction header and discharges directly to its respective heat exchanger. The outlet piping branches into parallel lines. The purification branch is designed to process approximately 20 percent of the cooling flow, while the bypass branch passes the remaining 80 percent of the cooling flow. Each purification branch is routed directly to a spent fuel pool demineralizer. The outlet of the demineralizer is routed to a spent fuel pool filter. The outlet of the filter is then connected to the bypass branch, which forms a common line that connects to the discharge header.

The staff completed its review of the spent fuel cooling system and concluded that the design is acceptable, and has provided an evaluation in Section 9.1.3 of this report.

19.3.3 Temporary RCS Boundaries

In Section 6.7 of NUREG-1449, the NRC discusses instances in which the failure of temporary RCS boundaries (such as nozzle dams installed in the hot-leg and cold-leg penetrations to SGs, temporary plugs for neutron instrument housing, and freeze seal, which is used to

temporarily isolate fluid systems) can lead to a rapid non-isolable loss of reactor coolant. In RAI 440-123, the staff requested that the applicant address the concern with respect to failure of temporary boundaries in the AP1000.

In a letter dated October 2, 2002, responding to the RAI, the applicant indicated that the AP1000 uses passive safety systems to provide the safety-related means for protecting the plant during all modes of operation including shutdown and refueling. The passive safety systems are designed to either automatically mitigate events that occur during shutdown, or are available for manual actuation. The AP1000 TSs identify when the various portions of passive safety systems are required to be available.

In addition, the applicant provided the following information for the design features that reduce risks associated with temporary RCS boundaries for the AP1000:

- SG nozzle dams (DCD Tier 2 Section 19E.2.1.2.6)

  SG nozzle dams are often used to isolate SGs during refueling outages to allow maintenance and inspection of the SG tubes. The nozzle dams will fail if the RCS pressure exceeds the nozzle dam design pressure without a pressure vent/release pathway, thus, creating a direct RCS drain path to the containment through an open SG primary manway. In DCD Tier 2, Revision 1, the applicant indicated that the AP1000 nozzle dams are designed to withstand to a RCS pressure of 275.8 kPa (40 psia), compared to that of the AP600 pressure of 220.6 kPa (32 psia). In RAI 440.110, the staff requested the applicant to discuss the analysis used to determine the design pressure of the nozzle dam. In a letter dated October 2, 2002, the applicant responded by indicating that the design pressure of the nozzle dam bracket and nozzle dam was determined to be able to withstand the RCS pressures that would occur during a loss of RNS cooling event. The event was analyzed with the NOTRUMP code for the AP1000. The analysis performed was consistent with the analysis approach used in the AP600 loss of RNS cooling analysis presented for the AP600 in WCAP-14837, Revision 3, "AP600 Shutdown Evaluation Report."

  The initial conditions were assumed to be at Mode 5 with the RCS open through the ADS stage 1 through 3 valves. Following the loss of RNS cooling, the RCS pressure increases. During the transient, the operator action is credited to manually open the ADS-4 valves at 1.3 hours into the transient, when the RCS vessel inventory is reduced to the bottom of the hot-leg. The assumption of the operator action and the associated time is consistent with Item 10.c of DCD Tier 2 Section Table 3.3.2-1 that specifies CMT actuation when the RCS water decreases to the bottom of the hot-leg, and therefore, is acceptable.

  The result of the analysis shows that the maximum pressure is 303.4 kPa (44 psia). The applicant revised the design pressure for the SG nozzle dam from 275.8 kPa (40 psia) to 344.8 kPa (50 psia). Since the assumptions used in the analysis are representative of the reduced inventory operating conditions, and the revised design pressure bounds the maximum calculated RCS pressure for the AP1000, the staff

concludes that the revised design pressure for the SG nozzle dam is adequate and acceptable.

- Elimination of temporary plugs for nuclear instrumentation

  The AP1000 does not contain removable bottom mounted nuclear instruments that require temporary plugging during shutdown and refueling. The AP1000 design uses a fixed incore system with penetration through the top head, rather than the bottom head.

- Elimination of temporary plug related to the excore detectors

  Current plants remove the excore detectors from above the excore housing through the floor of the refueling cavity. During refueling operations, these holes are plugged to facilitate flooding of the refueling cavity. The AP1000 design eliminates these temporary plugs by designing the excore instrumentation to be inserted from below the excore housings.

- Reduced reliance on freeze seals

  Freeze seals are used for repairing and replacing components such as valves, pipe fittings, pipe stops and pipe connections when it is impossible to isolate the area of repair any other way. Industrial experience indicates that some freeze seals have failed in nuclear power plants and resulted in significant events. In addressing the issue of freeze seals failure, the AP1000 design reduces the potential applications of freeze seals by reducing the number of lines that connect to the RCS and by providing the ability to perform inservice tests (ISTs) on many valves that connect to the RCS pressure boundary. The IST program reduces the requirements for disassembling RCS pressure boundary valves to perform operability tests. The use of freeze seals during a forced outage typically occurs in cold shutdown (Mode 5). During Mode 5, the PXS is required by the TSs (DCD Tier 2 Chapter 16, Table B 3.0-1) to be available, and therefore, the PXS can respond to a loss of coolant through a failed freeze seal.

The staff finds that the reduction of RCS penetrations, the ability to perform ISTs, the use of fixed incore system, and higher nozzle dam design pressure will reduce the risks associated with the loss of temporary RCS boundaries. Therefore, the staff concludes that the design relative to temporary RCS boundaries is acceptable.

DCD Tier 2 Section 13.5, "Plant Procedures," contains COL information items requiring plant procedures to be prepared for each plant. However, the COL applicant should develop plant specific guidelines that would reduce the potential for loss of RCS boundary and inventory when using freeze seals. This COL information is not specified in the DCD. Therefore, this is Open Item 19.3.3-1 and COL Action Item 19.3.3-1.

19.3.4 Instrumentation and Control During Shutdown Operations (DCD Tier 2 Section 19E.2.1.2.2)

In NUREG-1449, the NRC discusses inadequate instrumentation and incomplete operating procedures, especially during periods of reduced inventory operations that have contributed to several loss of shutdown cooling events at operating plants. Consequently, the staff has recommended that PWRs of advanced designs include enhanced instrumentation capabilities to enable the operator to continuously monitor key plant parameters during reduced inventory operations. Also, the operator must be able to detect the onset of a loss of decay heat cooling early enough that mitigation actions can be taken to restore shutdown cooling capability. As a minimum, this instrumentation should be available to provide visible and audible indications of abnormal reactor vessel level, temperature, and RNS heat removal performance.

The applicant addressed the instrumentation and control systems in DCD Tier 2 Section 19E.2.1.2.2 and the response to RAI 440.121, in a letter dated October 2, 2002. The staff's evaluation is discussed below.

19.3.4.1 Level Instrumentation (DCD Tier 2 Section 19E.2.1.2.2)

The AP1000 utilizes two redundant safety-related RCS hot-leg level channels, one located in each hot-leg. These two channel are independent of each other. One level tap is connected to the bottom of the hot-leg, and the other tap is on the top of the hot-leg bend leading to the SG. The level tap for the instrument in the hot-leg, with the RNS step-nozzle suction connection, is located between the reactor vessel and RNS step-nozzle suction line. Indication of the water level channels is retrievable in the main control room. These channels generate the alarms on the low hot-leg water level. They also provide signals for the following protection functions: (1) isolation of letdown on the low level signal (in accordance with Item 28.a of TS DCD Tier 2 Chapter 16 Table 3.3.2-1), (2) actuation of IRWST injection on the empty hot-leg level signal (in accordance with Item 22.c of TS Table 3.3.2-1), and (3) actuation of fourth-stage ADS valve on empty hot-leg level signal (in accordance with Item 10.c of TS Table 3.3.2-1.)

The letdown isolation system assists the operators when draining the RCS to a mid-loop level. If the operators fail to isolate the letdown, the letdown isolation channels send a signal to close the letdown valves and stop the draining process. In the event that a loss of the RNS cooling occurs and the RCS water level drops to the bottom of the hot-leg, the passive safety-related IRWST and fourth-stage ADS are automatically actuated to inject water into the RCS to maintain core cooling depressurization. In addition, the operators can manually initiate IRWST injection if the automatic function is not available.

The applicant indicated that the accuracy and response time of the hot-leg level instruments are designed to be consistent with the standard engineering safety features actuation discussed in DCD Tier 2 Section 7.3, "Engineered Safety Reactors." In RAI 440.126, the staff requested that the applicant address concerns of noncondensible gases in the water level instrument discussed in NRC Information Notice (IN) 92-54, "Level Instrumentation Inaccuracies Caused by Rapid Depresurization." In a letter dated October 2, 2002, the applicant responded stating that the NRC IN 92-54 issues were addressed in the layout of the instrument lines. In addressing issues related to non-condensible gases, the hot-leg level instrument lines are downward sloping from the hot-leg, the length of the lines are minimized, and the lines do not include large condensing pots. In addition, the hot-leg instrumentation is used primarily for

shutdown operations when the RCS is at low pressure. During these conditions, there are low levels of dissolved gases in the fluid in the instrument lines, and thus, the quantity of the non-condensible gases which could be released is small. Therefore, the accuracy of the hot-leg level measurement is not significantly affected by the non-condensible gases during the period of the intended use.

In the AP1000, draining the RCS to mid-loop condition is achieved in a controlled manner as discussed in DCD Tier 2 Section 19E.2.1.2.4 and the reduced-inventory operations are limited to the low RCS drain rates discussed in DCD Tier 2 Section 19E.3.1.3.5. Because of the low RCS drain rates and the step-nozzle design (discussed in Section 19.3.3 of this report), the RCS level perturbation and the amount of air-entrainment are small during the mid-loop operation. Therefore, the reliability of an accurate level indication is high. Also, the offset design of the AP1000 RCS hot-leg and cold-leg piping provides additional margin for mid-loop operation as compared with the hot-leg centerline.

As shown in DCD Tier 2 Figure 19E.2-1, the AP1000 includes a nonsafety-related independent pressurizer level transmitter that provides water level indication during startup, shutdown and refueling operations. The upper level tap is connected to an ADS valve inlet header, above the top of the pressurizer. The lower level tap is connected to the bottom of the hot-leg. This configuration provides level indication for the entire pressurizer and a continuous reading as the level decreases to mid-loop levels during shutdown operations.

Based on its review discussed above, the staff finds that the additional water level margin and the reliable hot-leg level indication, with aid of the pressurizer level indication, reduce the potential for loss of RNS from air-entrainment into the pump suction during mid-loop operation. The low hot-leg level signal and automatic isolation prevents the operator from over-draining the RCS coolant during a draindown process. Water injection from the IRWST provides and maintains core cooling in the event of a loss of RNS. The staff, therefore, concludes that the AP1000 level instrument design is acceptable.

19.3.4.2 Temperature Instrumentation (DCD Tier 2 Section 19E.2.1.2.2)

The AP1000 includes two safety-related hot-leg wide-range thermowell-mounted RTDs, one in each hot-leg, and at least two incore thermocouples that are used to measure RCS temperature. The incore thermocouples are used to measure core exit temperature, which is indicative of the RCS temperature, and they are only available when the reactor vessel head is in place. This capability is no longer available when the reactor vessel head is detensioned, and the instruments are disconnected in preparation for refueling activities. In this condition, the RCS temperature is measured by the RCS wide-range hot-leg RTDs. In a letter dated October 2, 2002, the applicant responded to RAI 440.121 by indicating that the hot-leg RTDs are mounted below the mid-plane of the hot-leg piping to provide information to the operators during all operating modes. These wide-range detectors can indicate the full-range of RCS temperatures from shutdown through power operation. For shutdown conditions including mid-loop operations, the wide-range RTDs provide a backup indication of the RCS coolant temperature when the RNS is operating, because the RNS heat exchanger inlet and outlet temperatures, and the RNS pump flow indications will show adequate RCS cooling. In the event that the RNS pumps become inoperable and the RNS detectors become ineffective, the wide-range RTDs can be used as an indication of core condition.

Based on its review, the staff finds that the RCS RTDs and the incore thermocouples are used in the current operating PWRs for the RCS temperature measurement. Therefore, the staff concludes that they are acceptable for indication of the RCS temperature and the core conditions during shutdown operations.

19.3.4.3 Instrumentation Monitoring RNS Performance (DCD Tier 2 Section 19E.2.4.2.1)

Several instruments are available to monitor the RNS performance. As described in DCD Tier 2 Section 5.4.7, the following system parameters are monitored for system performance: (1) RNS pump flow/discharge pressure, (2) RNS heat exchanger inlet/outlet temperature, (3) RNS valve status, and (4) RCS wide range pressure.

As described in DCD Tier 2 Section 19E.2.4.2.1, the AP1000 RNS pumps are located at the lowest elevation in the auxiliary building in order to maximize the available net positive suction head (NPSH) for the RNS pumps. The RNS pumps can be restarted and operated following a temporary loss of RNS cooling event. In RAI 440.113, the staff requested that the applicant discuss the NPSH requirements for the RNS pumps. In a letter dated October 2, 2002, the applicant reponed to RAI 440.113, by stating that the minimum NPSH requirement for the RNS pump is approximately 3.05 m (10 ft), at the design flow. The required NPSH provides the pumps with capability to operate during most mid-loop conditions, without throttling the RCS flow. If the RCS is at the mid-loop level and saturated conditions, some throttling of a flow control valve is necessary to maintain the adequate NPSH for the RNS pumps.

Based on its review, the staff concludes that the available instrumentation and the NPSH requirements are adequate for the operator to monitor the performance of the RNS.

19.3.5 Technical Specifications (DCD Tier 2 Section 19E.5)

In NUREG-1449, the NRC has indicated that current standard technical specifications (STS) for PWRs are not sufficiently detailed to address several risk-significant RCS configurations during shutdown and refueling operations. The safety margin that is available during these modes of operation is significantly influenced by the time it takes to uncover the core following an extended loss of residual heat removal capability. The staff found that the conditions that affect this safety margin include the decay heat level, the initial reactor vessel water level, the status of reactor vessel head, the number and size of openings in the cold-legs, the existence of hot-leg vents, and availability of alternate methods of decay heat removal in case of a loss of decay heat removal systems. The applicant discusses the TS provisions including specifications for shutdown operations in DCD Tier 2 Section 16.1. The shutdown specifications are summarized in AP1000 TS DCD Tier 2 Table B 3.0-1. For events that occur in Mode 4, safe shutdown, the TSs specify that the full complement of passive safety-related systems be available to mitigate an event. For events that occur in Mode 5, cold shutdown conditions with the RCS pressure boundary intact, the passive safety-related ADS, CMT and PRHR HX, as well as IRWST injection, must be available. The accumulators, however, are not required to be available.

For events that occur in Mode 5, with the RCS pressure boundary open and the plant in reduced inventory conditions, the PRHR HX, accumulators, and CMTs are not effective. The ADS first-, second- and third-stage valves are open and the fourth-stage valves are required to be operable. The IRWST gravity injection, containment recirculation paths and containment closure capability must be available. Since the TSs LCOs for shutdown operations are assumed in the safety analysis, discussed in Section 19.3.6 of this report, and the results of the analysis are acceptable, the staff concludes that the shutdown TSs are acceptable. However, TSs do not include the RNS in the AP1000 in shutdown modes.

The requirements of 10 CFR 50.36 specify the contents of TSs. Specifically, 10 CFR 50.36(c)(2)(ii) indicates that a TS LCO must be established for each item meeting one or more of the specified criteria. These criteria are: (1) installed instrumentation that is used to detect, and indicate in the control room, a significant abnormal degradation of the RCS pressure boundary (RCPB); (2) initial plant conditions that are assumed in a design-basis transient or accident analysis; (3) SSC that is used for mitigating consequences of a design-basis transient or accident; and (4) an SSC which PRA has shown to be significant to public health and safety.

The staff finds that the RNS does not meet any of the criteria specified in 10 CFR 50.36(c)(2)(ii) for inclusion of a TS LCO, i.e., it is not an installed instrumentation used to detect and indicate a significant abnormal degradation of the RCPB (criterion 1), not a process variable, design feature, or operating restriction that is an initial condition of a design-basis transient or accident analysis (criterion 2), not an SSC that is part of the primary success path and which functions or actuates to mitigate a design-basis transient or accident (criterion 3), and not an SSC which PRA has shown to be significant to public health and safety. Therefore, the staff concludes that the applicant's proposal of not including a TS LCO for the RNS is acceptable.

In Section A of SECY-94-084, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety-Related Systems (RTNSS) in Passive Plant Designs," dated March 28, 1994, the staff discussed the processes used (1) to develop insights regarding the importance of non-safety-related systems to the overall safety of the passive ALWR design, and (2) to determine what, if any, additional regulatory controls should be implemented for those non-safety-related systems determined to be important to safety. In Chapter 22 of this report, the staff discusses the RTNSS process in detail.

The applicant's evaluation of the RTNSS implementation is discussed in WCAP-15985, "AP1000 Implementation of the Regulatory Treatment of Non-Safety-Related Systems Process." The RTNSS evaluation in WCAP-15985 identifies the non-safety-related systems requiring regulatory controls for operations during mid-loop conditions. These systems include the RNS and supporting fluid and ac electrical systems, which are controlled through the short-term availability controls described in DCD Tier 2 Section 16.3.

The staff reviewed the applicant's AP1000 investment protection short-term availability controls for the RNS and supporting SSCs, discussed in DCD Tier 2 Section 16.3. The proposed administrative controls specify that for Modes 1, 2 and 3, one train of the RNS injection should be operable. If one required train is not operable, the operator should restore the train to operable status within 14 days. For Mode 5 with RCS pressure boundary open, or Mode 6 with upper internals in place or RCS cavity level less than full, the proposed controls specify that both RNS pumps should be operable for RCS cooling. If one RNS pump is found inoperable, the operator is requested to initiate actions to increase the RCS water inventory above the core within 12 hours and remove the plant from the applicable Modes 5 and 6 within 72 hours. The proposed administrative controls discussed above for the RNS in the Modes 5 and 6 conditions are also proposed for the RNS supporting systems such as the component cooling water, service water and on-site ac power systems when any of the systems does not fully meet its associated operability conditions. As discussed in this section above, since the RNS is a non-safety-related system and is not credited in a design-basis transient or accident analysis, the TS LCO is not needed for the RNS. The administrative controls for the RNS and the associated supporting systems are proposed for defense-in-depth to enhance the operability of the RNS for the residual heat removal and reduce the risk in a loss of core cooling during shutdown conditions. Therefore, the staff concludes that the administrative controls are acceptable.

19.3.6 Transient and Accident Analysis (DCD Tier 2 Section 19E.4)

The applicant discussed applicable DCD Tier 2 Chapter 15 non-LOCA and LOCA transients postulated to occur in shutdown operations in DCD Tier 2 Section 19E.4. The applicant identified the limiting case for each event category discussed in DCD Tier 2 Chapter 15 and evaluated for shutdown operations the effects of plant control parameters, neutronic and thermal hydraulic parameters, and engineered safety features on plant transient response such as departure from nucleate boiling ratio (DNBR), peak pressure and peak cladding temperature. For those cases that are bounded by the corresponding cases presented in DCD Tier 2 Chapter 15, the applicant provided supporting rationales. For those cases that are more

limiting than the corresponding DCD cases, the applicant provided the results of quantitative analyses for the staff to review. The following discussion documents the staff's evaluation.

19.3.6.1 Feedwater System Malfunctions (DCD Tier 2 Section 19E.4.2.1)

Feedwater system malfunctions can result in a decreased feedwater temperature or an increased feedwater flow. Both events decrease RCS temperature, which causes power to increase, because of the effects of the negative moderate coefficient of reactivity. The analyses of the feedwater system malfunction, initiated from Modes 1 and 2, are discussed in DCD Tier 2 Sections 15.1.1 and 15.1.2. Protection against feedwater system induced cooldown events is provided by the protection and safety monitoring system, through the automatic reactor trip and main feedwater system isolation. The protection functions are available in all modes of operation during which the feedwater system is in operation.

The increase in feedwater temperature event is less severe as the power level is decreased. Normal operating feedwater temperature decreases as plant power level deceases. As a result, if a feedwater malfunction suddenly reduces the feedwater temperature, the maximum change in feedwater temperature occurs when the plant is operating at full-power. Also, the increased feedwater flow event is the worst case when the plant is at full-power (Mode 1) conditions. In Modes 2 and below, feedwater entering the SG is routed through the startup feedwater control valves, which restrict feedwater flow to be less than the flow through the main feedwater control valves. Therefore, an increase in feedwater flow event caused by an inadvertent opening of a main feedwater control valve in Modes 2 and below is not likely. The assumption of a failed open startup feedwater control valve in Modes 2 and below results in a relatively slow transient because of a lower feedwater flow rate.

The events that occur from the Modes 1 and 2 conditions, as discussed in DCD Tier 2 Sections 15.1.1 and 15.1.2, bound the events initiated from the shutdown modes because of the following:

- higher feedwater temperature increases and higher feedwater flow rates, caused by the feedwater system malfunctions, occur at higher power level conditions, and

- the protection functions are available in all modes during which the feedwater system is in operation

The staff has reviewed the analysis for the limiting feedwater system malfunction events and provided its evaluation in Sections 15.2.1.1 and 15.2.1.2 of this report.

19.3.6.2 Excessive Increase in Secondary Steam Flow (DCD Tier 2 Section 19E4.2.2)

Excessive load increase events decrease RCS temperature, which causes an increased power because of the effects of the negative moderate coefficient of reactivity. The excessive load increase event, initiated from full-power conditions, is discussed in DCD Tier 2 Section 15.1.3. Since the initial power at Mode 2 is low, the event results in a lower power level than that from full-power conditions. In Modes 3 through 6, the excessive load increase event may be

considered to be a simple steam release, because there can be no load when the turbine is off-line and the core is subcritical. The steam release events initiated from Modes 3 through 6 are bounded by Mode 2 because the initial RCS temperatures and pressures are reduced and the core is subcritical. Therefore, the excessive load events at low powers and shutdown modes are bounded by the cases initiated from full-power conditions. The staff has reviewed the analysis for the limiting excess load initiated from full-power, and provided its evaluation in Section 15.2.1.3 of this report.

19.3.6.3 Steamline Breaks (SLBs) (DCD Tier 2 Section 19E.4.2.3)

The steam released from a steamline break causes a decrease in the RCS temperature, and in the presence of a negative MTC, the decreased RCS temperature results in a positive reactivity addition. If the resulting positive reactivity is greater than the negative reactivity from the inserted control rod worth and from the borated water injected from the CMTs, the core may return to criticality for a post-trip core with the most reactive rod cluster control assmbly (RCCA) stuck in the fully withdrawn position. Thus, leading to high local power levels and causing the concern of low DNBRs. In DCD Tier 2 Sections 15.1.4 and 15.1.5, the applicant shows that if the event occurs in Mode 2, it results in a more severe post-trip transient than that initiated from Mode 1, because the decay heat level for Mode 1 is higher and reduces the effect of cooldown.

A SLB initiated from Modes 3 and 4 is not worse than that from Mode 2, because the pressure, temperature, and steam flow through the affected SG are less limiting. Automatic safeguards actuation signals are available through Mode 3, until the RCS is borated to meet shutdown margin requirements at cold shutdown 93 °C (200 °F) and safeguards signals are blocked (in accordance with Note (a) to item 1 of DCD Tier 2 Table 3.3.2-1 and TS LCO 3.1.1.) Both CMTs continue to be available for automatic actuation on low-2 pressure level or manual actuation through Mode 4 with the RCS not being cooled by the RNS (in accordance with TS LCO 3.5.2). In Mode 4, with the RNS in operation, and in Mode 5, with the RCS intact, one CMT is available for actuation (in accordance with TS LCO 3.5.3). The RCS temperatures in Modes 5 and 6 are low (below 93 °C (200 °F)), and the cooldown effect resulting from the SLB is insignificant. Therefore, the SLB initiated from Mode 2 bounds the cases at full-power and shutdown modes. The staff has reviewed the analyses for the limiting SLB initiated from Mode 2 conditions, and provided its evaluation in Sections 15.2.1.4 and 15.2.1.5 of this report.

19.3.6.4 Inadvertent PRHR HX Operation (DCD Tier 2 Section 19E4.2.4)

Inadvertent actuation of the PRHR HX causes an injection of relatively cold water into the RCS, and produces a positive reactivity addition in the presence of a negative MTC. The analysis of this event for Modes 1 and 2 is discussed in DCD Tier 2 Section 15.1.6. The PRHR HX heat transfer rate is a function of the heat exchanger's inlet temperature and flow rate. PRHR HX heat transfer rate is higher with high flow rates and high inlet temperatures. The maximum heat removal rate occurs when the plant is at full-power with forced RCS flow. At plant full-power conditions, the PRHR HX heat removal rate is approximately 10 percent of full-power. At hot zero-power conditions with natural circulation, heat removal by the PRHR HX is about 1.5 percent to 2 percent of full-power. With the maximum heat removal rate, the event which occurs at the full-power condition results in a higher power than that from Mode 2.

In Mode 3, the cooldown caused by the actuation of the PRHR HX, results in the cold-leg temperature decreasing below the low T_{cold} safeguards signal setpoint. This actuates a reactor trip, initiates boration by the CMTs, and trips all the RCPs. When the RCPs trip, natural circulation flow begins in the RCS and the PRHR HX loop. During the natural circulation flow conditions, the heat removal capability of the PRHR HX decreases to about 1.5 percent of full-power, and the severity of the transient decreases. With the RCS in natural circulation, the cooldown rate is slow. Boration by the CMTs will bring the core subcritical again if the criticality occurs. In Modes 3, the safeguards signals may be blocked to allow plant cooldown and depressurization. However, prior to blocking the safeguards signals, the RCS is borated to the shutdown margin requirements at cold shtudown (93 °C (200 °F)) (in accordance with Note (a) to item 1 of DCD Tier 2 Table 3.3.2-1 and TS LCO 3.1.1.) In Mode 3 with safeguards signals blocked or in Mode 4, because the reactor is subcritical, the event produces lower power increases than that from Mode 1. For Modes 5 and 6, the cooldown effect resulting from the inadequate PRHR HX operation is insignificant because the initial RCS temperatures are low. Therefore, the inadvertent actuation of the PRHR HX initiated from full-power conditions is the limiting case. The staff has reviewed the analysis for the limiting case, and provided its evaluation in Section 15.2.1.6 of this report.

19.3.6.5 Decreased Heat Removal by the Secondary System (DCD Tier 2 Section 19E.4.3)

The consequences of a decrease in heat removal by the secondary system in Modes 1 and 2 are discussed in DCD Tier 2 Section 15.2. The following seven events are analyzed: (1) loss of load, (2) turbine trip, (3) inadvertent closure of main steam isolation valves, (4) loss of condenser vacuum, (5) loss of ac power, (6) loss of normal feedwater, and (7) feedwater system pipe breaks. These events are characterized by rapid reductions in heat removal capability of the SGs. The loss of heat removal capability results in a rapid rise in the SGs' secondary system pressure, and temperature and a subsequent increase in the RCS pressure and temperature. Reactor trip and actuation of secondary and primary safety valves mitigate the effects of the primary to a secondary power mismatch during these events. The severity of these events is increased if the primary to a secondary power mismatch is increased. The occurrence of the events at full-power produces a greater and more rapid power mismatch than at lower power or operations below Mode 2 because of a higher initial power and a higher decay heat level. Therefore, the worst cases for the events discussed above are initiated from full-power conditions.

For operations other than Mode 1, the loss of load and turbine trip events, listed above, are not considered credible because the turbine is off-line and the transients resulting from a turbine related fault cannot occur.

A loss of condenser vacuum (LOCV) or inadvertent MSIV closure (IMSIVC) events may occur during Mode 2 through 4, because the plant may dump steam to the condenser to remove decay heat in these modes of operation. Their transient responses are bounded by the turbine trip analysis from full-power because the power mismatch is low. Decay heat can be removed by the SGs through SG safety valves, which are available through Mode 4 (in accordance with TS LCO 3.7.1,) and it can also be removed with the PRHR HX, which is available through Mode 5 with the RCS intact (in accordance with TS LCOs 3.5.4 and 3.5.5.)

During a loss ac power event, the low SG level signal trips the reactor. Following the reactor trip, the PRHR HX is activated to remove decay heat. Automatic PRHR HX on the low SG level is available in Modes 1 through 3 and Mode 4 without the RNS in operation to cool the RCS (in accordance with item 13.c of TS Table 3.3.2-1). The most limiting case, for the loss of ac power event, is initiated from full-power because of a higher decay power level at full-power conditions. For operations in Mode 4 or 5 with the RNS in operation, the plant response to a loss of ac power is the same as the loss of RNS cooling event (see Section 19.3.6.20 of this report.)

For a loss of normal feedwater (LONF) or the feedwater line break (FLB) events, the low SG low level signal trips the reactor. Following the reactor trip, the PRHR HX is activated to remove decay heat. Automatic PRHR HX on the low SG level is available in Modes 1 through 3 and Mode 4, without the RNS in operation to cool the RCS. The most limiting cases for both LONF and FLB events are initiated from full-power, because of a higher decay power level at full-power conditions. In Mode 4 with the RNS aligned and in Modes 5 and 6, the feedwater system is not used. Therefore, the LONF and FLB events will not cause a heatup of the RCS.

The staff has reviewed the analyses for the limiting cases for the decreased heat removal by the secondary system events, and provided its evaluation in Section 15.2.2 of this report.

19.3.6.6 Decrease in Reactor Coolant Flow (DCD Tier 2Section 19E.4.4)

The consequences of a decrease in RCS flow in Modes 1 and 2 are discussed in DCD Tier 2 Section 15.3. The following four events are analyzed: (1) partial loss of forced RCS flow, (2) complete loss of forced RCS flow, (3) reactor coolant pump shaft seizure, and (4) reactor coolant pump shaft break. For these events, a decrease in the RCS flow can reduce heat removal from the primary to the secondary system, and cause a heatup in the RCS. The RCS heatup results in an increase in the RCS pressure and a decrease in the DNBRs during the low RCS flow conditions. The occurrence of the event at full-power produces a greater and more rapid heatup than at lower power, or operations below Mode 2. In addition, below Mode 2, when the core is subcritical, forced RCS flow is not needed because margin-to-DNB is not an issue. Therefore, the cases initiated from full-power are the limiting cases, resulting in a maximum peak RCS pressure and a minimum DNBR. The staff reviewed the analyses for the limiting events, and provided its evaluation in Section 15.2.3 of this report.

19.3.6.7 Uncontrolled RCCA Bank Withdrawal from a Subcritical Condition (DCD Tier 2 Section 19E.4.5.1)

An uncontrolled RCCA bank withdrawal from a subcritical condition causes power to increase. An increase in power results in a decrease in DNBR, if it is not terminated by a reactor trip. The analysis of this event for Mode 2 is discussed in DCD Tier 2 Section 15.4.2. In the analysis, the most limiting operating conditions specified by the TSs were used to bound the event from Modes 2 through 5. The assumptions related to the limiting operating conditions include: (1) the power range (low setting) high neutron flux is credited for the reactor trip to delay the trip, (2) the flow from three reactor coolant pumps are credited to calculate the minimum DNBR,

and (3) the RCS temperature at Mode 2 is used to calculate the minimum DNBR and core kinetics feedback.

LCO 3.3.1 of the AP1000 TSs specifies the source range high neutron flux trip to be in operation in Modes 3, 4 and 5 when the reactor trip breakers are closed. If the reactor trip breakers are open, then a RCCA withdrawal event is precluded from occurring. The source-range high neutron flux trip is available in Mode 2 when power is below the P-6 interlock. In these circumstances, the source-range high neutron flux trip will be available to terminate the event, by tripping any withdrawn and withdrawing RCCA, before any significant power level can be attained. The analysis in DCD Tier 2 Section 15.4.2 takes credit of the power range (low setting) high neutron flux, instead of the souce-range high neutron flux, to trip the reactor. The staff concludes that this is a conservative assumption because it delays the trip, resulting in a higher increase in power level. Therefore, the staff finds this acceptable.

LCO 3.4.4 of the AP1000 TSs specifies that all four RCPs are operating whenever the reactor trip breakers are closed in Modes 1 through 5. The DCD Tier 2 Section 15.4.2 analysis assumes the flow from three RCPs, instead of all four RCPs as specified by the TSs, to calculate the minimum DNBR. The assumption of using the flow from three RCPs is within the operating conditions of Modes 1 through 5. The staff concludes that this is a conservative assumption, because it results in a lower calculated DNBR. Therefore, the staff finds this acceptable.

The staff has reviewed the limiting case discussed above, and provided its evaluation in Section 15.2.4.1 of this report.

19.3.6.8 Uncontrolled RCCA Bank Withdrawal at Power (DCD Tier 2 Section 19E.4.5.2)

The analysis for this event is discussed in DCD Tier 2 Section 15.4.2. This event is not applicable to Mode 2 and below because this event occurs only at power.

19.3.6.9 RCCA Misalignment (DCD Tier 2 Section 19E.4.5.3)

The following three events are considered RCCA misalignment: (1) one or more dropped RCCAs, (2) statistically misaligned RCCA, and (3) withdrawal of a single RCCA. The analyses of these events for full-power conditions are discussed in DCD Tier 2 Section 15.4.3. These events result in core radial power distribution perturbations. The radial power changes cause the calculated DNBRs to decrease. When the reactor is in any of the subcritical modes, the dropped RCCA event, and misaligned RCCA event, will not result in any power transient in the absence of a critical neutron flux. Also, LCO 3.1.1 of the AP1000 TSs specifies the required shutdown margin that is determined based on the rodded core, with the most reactive RCCA stuck out. As a result of the TS requirements, no single RCCA withdrawal, initiated from the subcritical modes, will insert enough reactivity to cause the core to become critical. Therefore, the RCCA misalignment events discussed above are significant only at power, and the severity increases at higher power. For operations below Mode 2, while the reactor is subcritical, the events do not result in a significant decrease in DNBRs, and are bounded by Mode 1 conditions.

The staff has reviewed the analyses for the limiting events initiated from full-power, and provided its evaluation in Section 15.2.4.3 of this report.

19.3.6.10 Startup of an Inactive Reactor Coolant Pump at Incorrect Temperature (DCD Tier 2 Section 19E.4.5.4)

Starting an idle RCP increases the circulation of cold water into the core from the stagnant RCS loop. This results in an increase in positive reactivity in the presence of a negative moderator coefficient, and thus, causes the power level to increase. This event is precluded from occurring during at-power modes by TS 3.4.4, that specifies four RCPs in operation in Modes 1 and 2. Startup of an inactive RCP, while in any of the subcritical modes, will have relatively small effect upon the core temperature because there will be a small or no temperature difference between the RCS loops.

19.3.6.11 Chemical and Volume Control System Malfunction (DCD Tier 2 Section 19E.4.5.5)

Chemical and volume control system (CVS) malfunctions result in a decrease in boron concentration in the reactor coolant. The analyses of the boron dilution event in Modes 1 through 6 are provided in DCD Tier 2 Section 15.4.6. The staff has reviewed the analyses for the CVS malfunction events and provided its evaluation in Section 15.2.4.6 of this report.

19.3.6.12 Inadvertent Loading of a Fuel Assembly in an Improper Position (DCD Tier 2 Section 19E.4.5.6)

Fuel loading errors may result in a core power shape exceeding its design values. The core power shape changes cause the calculated DNBRs to decrease. When the reactor is in any of the subcritical modes, the fuel loading error events do not affect the calculated DNBRs. The severity of the fuel loading error events increases as the power level increases. Therefore, the results discussed in DCD Tier 2 Section 15.4.7 for Mode 1 at full-power conditions, bound the results for Mode 2 and the subcritical modes. The staff has reviewed the analysis for the limiting event initiated from full-power conditions, and provided it evaluation in Section 15.2.4.7 of this report.

19.3.6.13 RCCA Ejection (DCD Tier 2 Section 19E.4.5.7)

RCCA ejections in Modes 1 and 2 are the most limiting cases. LCO 3.1.1 of the AP1000 TSs specifies the maintenance of adequate shutdown margin for Modes 3 through 5. The required shutdown margin is determined by assuming that the most reactive RCCA is fully withdrawn from the core. Ejection of a single RCCA, initiated from subcritical conditions, would not cause the core to be critical. The staff has reviewed the analysis for the limiting cases initiated from Modes 1 and 2, and provided its evaluation in Section 15.2.4.8 of this report.

19.3.6.14 Inadvertent Actuation of the CMTs (DCD Tier 2 Section 19E.4.6)

The analysis of the inadvertent actuation of the CMTs is performed with the plant initially in full-power conditions (Mode 1), and is discussed in DCD Tier 2 Section 15.5.1. The full-power case

described in the DCD is the CMT malfunction caused by the inadvertent opening of the discharge valves to one CMT. This event results in the maximum amount of stored energy in the RCS, and in the maximum core decay heat. The analysis performed for the full-power case shows that the pressurizer will not be overfilled with water, and the loss of reactor coolant does not occur. When the reactor is at part-power, or in the subcitical modes, the amount of the stored energy and decay heat will be significantly reduced, and the increase in water inventory in the pressurizer is bounded by the full-power case.

For the case with actuation of CMTs, initiated by a spurious "S" signal, the reactor is tripped and the PRHR HX is actuated at the time of the event initiation. The CMTs begin injecting cold, borated fluid into the RCS. The injected fluid expands as it is heated in the RCS by decay heat. The expansion is counteracted by decay heat removal through the PRHR HX. The severity of the expansion is increased with higher decay heat power levels. Therefore, the case initiated from full-power conditions bounds the cases initiated from part power, or any subcritical modes with respect to the fluid expansion that causes the pressurizer to overfill with water.

The staff has reviewed the analysis for the limiting case initiated from full-power conditions, and provided its evaluation in Section 15.2.5.1 of this report.

19.3.6.15 CVS Malfunction (DCD Tier 2 Section 19E.4.6)

Malfunctions in the CVS increase water inventory in the RCS. The analysis of CVS malfunction is performed with the plant initially in Mode 1, and is discussed in DCD Tier 2 Section 15.5.2. In the full-power analysis, a worst combination of makeup boron concentration, feedback conditions, and plant system interactions is used for the limiting case. For this case, the CVS malfunction can cause a slight boration of the RCS. As a result, the core power decreases, which in turn causes actuation of an "S" signal on low cold-leg temperature. The "S" signal is generated before the pressurizer water increases to the high-2 pressurizer level signal (that actuates isolation of the CVS makeup and terminates the transient). The "S" signal actuates the CMTs and PRHR. However, the reactivity effects of the CVS malfunction, that causes an "S" signal for the full-power cases, does not occur at shutdown because the core is subcritical with a sufficient shutdown margin. In shutdown modes, the CVS malfunction results in the pressurizer water level increasing to the high-2 level setpoint. Item 16.c of TS Table 3.3.2-1 specifies that the CVS be isolated on the high-2 pressurizer level signal when the plant is in Modes 1 through 3 and Mode 4, prior to operating on the RNS. Because the isolation of the CVS makeup flow occurs earlier and the CMTs are not actuated (resulting in a smaller increase in the RCS inventory), the events initiated from operations at shutdown modes are bounded by the full-power case. In Modes 4 through 6 when the RNS is in operation, low-temperature overpressure protection (LTOP) of the RCS pressure boundary is provided by the RNS relief valve. A discussion of the LTOP analysis is included in DCD Tier 2 Section 5.2.2 and Section 5.2.2.2 of this report.

The staff has reviewed the analysis for the limiting case, and provided its evaluation in Section 15.2.5.2 of this report.

19.3.6.16 Inadvertent Opening of Pressurizer Safety Valves or the ADS Valves

(DCD Tier 2 Section 19E.4.7.1)

The analysis of inadvertent opening of pressurizer safety valves or ADS valves, with the plant initially at full-power conditions, is discussed in DCD Tier 2 Section 15.6.1. During the transient, the RCS pressure decreases rapidly. These depressurization events, which occur at power, result in deceased DNBRs. For subcritical modes, violation of DNB safety limits is not of concern because of low decay power levels. Therefore, the events discussed in DCD Tier 2 Section 15.6.1 bound these same events initiated from operating modes other than full-power conditions. The staff has reviewed the analysis for the limiting case initiated from full power, and provided its evaluation in Section 15.2.6.1 of this report.

19.3.6.17 Failure of Small Line Carrying Primary Coolant Outside Containment (DCD Tier 2 Section 19E.4.7.2)

The analyses of radiological consequences for breaks of small lines carrying primary coolant outside containment are discussed in DCD Tier 2 Section 15.6.2. The analysis performed for Mode 1 is bounding because the coolant temperature and iodine concentrations at Mode 1 bound those that would exist in the other modes. The staff has reviewed the analysis for the limiting case initiated from Mode 1, and provided its evaluation in Section 15.2.6.2 of this report.

19.3.6.18 Steam Generator Tube Rupture in Lower Modes (DCD Tier 2 Section 19E.4.7.3)

The analyses of the SGTR events, with the plant initially at full-power conditions, are discussed in DCD Tier 2 Section 15.6.3. At full-power conditions, the SGTR event results in maximum offsite doses. The offsite doses drop significantly at lower power levels and in lower modes of operation because the break flow from the primary to secondary sides and the steam release from the faulted SG, (major factors to determine dose releases), are less limiting. In DCD Tier 2 Section 15.6.3, the applicant indicates that an analysis at full-power is performed to demonstrate margin to SG overfill and thus, to assure that the SG safety valves can reseat after opening. The dose calculations for the SGTR event are based on the assumption that the SG safety valves will reseat after opening.

The applicant indicates, in DCD Tier 2 Section 19E.4.7.3, that the margin to the SG overfill would be maintained for SGTR events initiated at lower power levels, even with a higher initial SG inventory corresponding to the lower initial power level. The staff notes that margin to SG overfill depends on parameters such as initial SG water inventory, time to actuate the PRHR HX for cooling and depressurization, and time for termination of the CVS flow. In the absence of a quantitative analysis for SG overfill, it is not clear that the margin to SG overfill can be maintained for SGTR events. In RAI 440.185, the staff requested that the applicant perform an analysis to show the adequacy of the AP1000 design for SG overfill prevention during a SGTR event, in shutdown modes. The analysis should include the following cases, which were analyzed for the AP600 design: (1) Mode 3 with the RCS at no-load conditions, (2) Mode 4 with the RCS at 215 °C (420 °F) and 13.3 MPa (1900 psig), and (3) Mode 4 with the RCS at 157 °C (350 °F) and 7 MPa (1000 psig). In a letter dated April 1, 2003, the applicant responded by performing an analysis for the cases requested in RAI 440.185.

Case 1 bounds the highest RCS pressure and temperature that may exist during shutdown modes.

Case 2 represents the lowest expected RCS temperature that may exist while the accumulators are aligned. At the RCS temperature of 215 ^{0}C (420 ^{0}F), the initial pressure of 13.3 MPa (1900 psig) is the maximum RCS pressure, based on the required primary to secondary pressure differential specified in operating procedures. The low RCS temperature will reduce the effectiveness of the PRHR HX, and the highest RCS pressure will maximize the leakage flow from the primary to the secondary sides. Both assumptions minimize the margin to SG overfill.

Case 3 represents the lowest RCS temperature where a credible SGTR is postulated. The initial pressure of 7 MPa (1000 psig) is the maximum expected RCS pressure that may exist when the RCS temperature is at 157 ^{0}C (350 ^{0}F).

The results of the analysis shows that although the initial mass of water in the SG is higher in lower modes, (PRHR HX actuation may be delayed until the low pressurizer level setpoint is reached and accumulator injection may occur), the margin to SG overfill is maintained. Since the values used for input parameters are at zero power level and initial conditions consistent with lower modes of operation, and the results show that the consequences of the SGTR events are bounded by the DCD results for the SGTRs at full-power conditions, the staff concludes the SGTR analysis is acceptable.

19.3.6.19 Loss-of-Coolant Accident Events in Shutdown Modes
(DCD Tier 2 Section 19E.4.8.1)

The analyses of LOCAs are performed with the plant initially at full-power conditions, and are discussed in DCD Tier 2 Section 15.6.5. With other parameters being the same as assumed for LOCAs at full-power conditions, the reduction in decay heat levels associated with shutdown modes would make all LOCA events less limiting than those analyzed at full-power conditions. However, as the plant proceeds through shutdown mode of operation, various accident mitigating system components are removed from service. One particularly significant action is to isolate the accumulators at 6.9 MPa (1000 psig). During the AP600 review, the staff found that the LOCA analyses in shutdown modes are bounded by the DCD Tier 2 Section 15 LOCA analyses initiated from full-power conditions. As demonstrated by the DCD Tier 2 Section 15 LOCA analyses for full-power conditions, the AP1000 provide a similar level of protection as the AP600 passive safety systems . Furthermore, in a letter dated December 2, 2002, the applicant responded to RAI 440-119 by analyzing the double-ended cold-leg guillotine (DECLG) break, which is identified in DCD Tier 2 Section 15.6.5.4A as the limiting large break LOCA (LBLOCA) event. The analysis is performed assuming the LOCA event initiated from Mode 3 conditions.

During Mode 3 operations, the accumulators are allowed to be removed from the service by the TSs once the pressurizer pressure has been reduced to less than 6.9 mPa (1000 psig). Before the accumulators are disabled, the consequences of a postulated LOCA event in Mode 3 are less limiting than for full-power cases discussed in DCD Tier 2 Section 15.6.5 because of the lower decay heat levels. In the LOCA analysis initiated from Mode 3 conditions, the applicant assumed that the initial pressurizer pressure and hot-leg temperature are 6.9 mPa (1000 psig)

and 218 °C (425 °F), respectively. The accumulators are assumed to be isolated. The temperature of 218 °C (425 °F) is the highest expected hot-leg temperature when the pressure is 6.9 mPa (1000 psig), and the accumulators are removed from service.

The decay heat level is determined at 2.78 hours after reactor shutdown. The cooldown time of 2.78 hours is based on the time estimated to cool down the plant from full-power operation to 218 °C (425 °F), at a cooldown rate of 27.8 °C (50 °F) per hour. The cooldown time assumed in the analyses is shorter than the expected time to reach the point to isolate the accumulators during a plant outage. Selection of an earlier time after shutdown will be non-limiting relative to the DCD Tier 2 Section 15.6.5 analyses, because the accumulators remain available. The required 10 CFR Part 50, Appendix K decay heat, and the maximum peaking factors specified in TS (or the core operating report) are used in the analysis.

For consideration of the worst LBLOCA single failure, the limiting fault is a failure of one CMT discharge valve to open. The LOCA analysis performed in Mode 3 bounds the events that occur during both Modes 3 and 4 because after accumulator isolation, and before RNS operation, the decay power drops to the Mode 3 LOCA analysis conditions, and there is no reduction in safety-related systems that are available to mitigate the event.

The applicant used the NRC-approved WCOBRA/TRAC code (as discussed in Chapter 21 of this report) to analyze the LBLOCA case initiated from Mode 3 conditions. The results show that for the limiting LBLOCA case, the maximum peak cladding temperature (PCT) is 771 °C (1420 °F), and all of the 10 CFR 50.46 acceptance criteria are met. The values used for the input parameters are representative of the Mode 3 conditions. Therefore, the staff concludes that the analysis is acceptable.

19.3.6.20 Loss of RNS Cooling

During shutdown modes of operations, the RNS is used to remove decay heat when the RCS temperature and pressure are reduced to less than or equal to 178 °C (350 °F) and 3.1 mPa (450 psig), respectively. A loss of electrical power event can result in a loss of flow through the RNS, and a subsequent loss of RNS cooling event. For the AP1000 application, the applicant stated in DCD Tier 2 Section 19E4.8.1 (Revision 1) that the results of the loss of RNS for the AP1000 plant are similar to the AP600 plant response, and the availability of the accident mitigating system components in shutdown modes is the same for both the AP600 and AP1000. However, the staff noted that the Chapter 15 loss of cooling analysis was performed at Modes 1 and 2. During the shutdown modes conditions, the AP1000 plant response to accidents may be different from the AP600 plant response. In RAI 440.119, the staff requested the applicant to provide an analysis demonstrating that the equipment available during shutdown, as prescribed by the AP1000 TSs, are sufficient to protect the plant from a loss of RNS cooling event during shutdown. In a letter dated December 2, 2002, the applicant responded by providing the results of the additional analysis for the AP1000 in the DCD Tier 2 Sections 19E.4.8.2 and 19E.4.8.3 (Revision 3), for the staff to review. The analysis determined the plant response to the two loss of RNS cooling events (one event is initiated from Modes 4 and 5 with the RCS intact, and the other event is initiated from Mode 5 with the RCS open). The analysis assumes that both loss of RNS cooling events are caused by a loss of offsite

power, that results in a loss of flow through the RNS. An NRC-approved NOTRUMP code (as discussed in Chapter 21 of this report) is used for the analysis. The analysis of both loss of the RNS cooling events is discussed as follows.

19.3.6.20.1 Loss of RNS Cooling in Mode 4 and Mode 5 with RCS Intact (DCD Tier 2 Section 19E 4.8.2)

For a loss of RNS cooling in Mode 4 and Mode 5 with RCS intact, the analysis used an initial decay heat corresponding to the decay heat level at four hours after reactor shutdown. This cooldown time is based on an expected cooldown rate of 27.8 °C (50 °F) per hour, to cool the RCS to the entry conditions for the RNS operation with the RCS temperature and pressure assumed to be 178 °C (350 °F) and 3.1 mPa (450 psig), respectively. The main steam system is assumed to be unavailable for heat removal. The plant conditions for the analysis are assumed to bound the events that occur during both Modes 4 and 5. To bound Mode 5 with the intact RCS, only three of the fourth-stage ADS valves (in accordance with TS LCO 3.4.12) are assumed to be operable. For consideration of the worst single failure, one of three available fourth-stage ADS valves is assumed to fail to open on demand. The RNS relief valve setpoint is assumed to be 5.6 mPa (832.7 psia), with corresponding relief capacity of 41L/s (650 gpm). Both CMTs are assumed to be available. In accordance with the specifications of TS LCO 3.5.3, only one CMT is available. In a letter dated April 2, 2003, the applicant responded to RAI 440.119 by performing the loss of RNS cooling case with CMT available in Mode 4. The results of the analysis show similar plant response for cases with one CMT, or two CMTs available. Since the assumptions discussed above are more limiting than Mode 5 conditions, the analysis of the loss of RNS in Mode 4 is applicable to the loss of RNS cooling in Mode 5 with the RCS intact. Two cases were analyzed: Case 1 allows for automatic safety system actuation on a low pressurizer level signal late in the event, and Case 2 assumes that the operator takes actions to actuate the CMT and PRHR HX 1800 seconds after the loss of RNS cooling.

Case 1 - Automatic Safety System Actuation

The sequence of the event is discussed in DCD Tier 2 Table 19E.4.8-2. Following the loss of RNS cooling, the core decay heat generation results in an increase in the reactor coolant temperature and the RCS pressure. The pressure increases to the RNS relief valve setpoint and opens the relief valve. Since the reactor coolant released through the relief valve is not sufficient to remove the core decay heat, the core outlet temperature continues to increase until it reaches the saturation temperature, at the relief valve setpoint. The generation of steam in the core causes the system pressure to increase above the RNS relief setpoint, and the pressurizer level to continue to increase. As the boiling front moves lower and lower into the core, more steam generation occurs and the pressure continues to increase. Once the entire core length is boiling, the upper plenum mixture level is within the hot-leg perimeter. When steam begins to flow through the relief valve along with liquid, the system pressure begins to decrease. The pressurizer level also decreases as the water drains from the pressurizer into the RCS hot-leg. The low pressurizer level signal causes the CMT actuation, which, in turn, opens the PRHR HX isolation valves. The CMT flow injection results in a decrease in the CMT level. As the CMT level decreases, the ADS valves begin to open. The actuation of ADS fourth-stage valves opens the IRWST injection line valve. The vapor and liquid flow through the

ADS valves reduces the pressure to the point where the IRWST injection begins. The CMT and IRWST injection reverses the decrease in the core and downcomer water level.

The staff finds that the NRC-approved NOTRUMP code is used for the analysis; the input parameters used in the analysis are representative of the plant conditions at Modes 4 and 5 with RCS intact; and the results show that the calculated core mixture water level remains above the top of the active fuel during the event, thus avoiding fuel failure. Therefore, the staff concludes that the analysis is acceptable.

Case 2 - Manual Safety System Actuation

For the case where operator actions are taken, the CMT and PRHR isolation valves are assumed to open 1800 seconds following the transient. The sequence of the event is also discussed in DCD Tier 2 Table 19E.4.8-2. Initially, the decay heat is greater than the PRHR capacity and the RCS pressure increases to the RNS relief valve setpoint. A small amount of the RCS inventory is vented through the valve. In the later part of the transient, the decay heat matches the PRHR capacity, and the RCS pressure slowly decreases to the relief valve setpoint and terminates the flow through the relief valve. The analysis shows that no significant loss of RCS inventory occurs and the ADS is not actuated. Therefore, the staff concludes that the analysis is acceptable.

19.3.6.20.2 Loss of RNS Cooling in Mode 5 with RCS Open
(DCD Tier 2 Section 19E.4.8.3, Revision 3)

For a loss of RNS cooling in Mode 5 with the RCS open, the RNS is initially operating in Mode 5 at 24 hours after reactor shutdown, with the ADS stage 1, 2, and 3 valves open (meeting TS 3.4.13), and one of the IRWST injection paths available (meeting TS 3.5.7). The initial RCS temperature and pressurizer pressure are assumed to be at 70.5 °C (160 °F) and at atmospheric pressure plus the elevation head in the IRWST, respectively. The SG is assumed to be unavailable for heat removal. To be consistent with the TS, both CMTs and PRHR are assumed to be not available. Two of the fourth-stage ADS valves are assumed operable (meeting TS 3.4.13). For the consideration of the worst single failure, one of two available fourth-stage ADS valves is assumed to fail to open on demand.

The sequence of the event is discussed in DCD Tier 2 Table 19E.4.8-3. Following the loss of RNS cooling, the core decay heat generation results in an increase in the reactor coolant temperature. The core outlet temperature increases until it reaches the saturation temperature. The RCS is vented to the IRWST through ADS stages 1, 2, and 3, resulting in the RCS inventory decreasing to the bottom of the RCS hot-legs. In accordance with Items 10.c and 22.c of TS Table 3.3.2-1, a low RCS hot-leg level signal opens the fourth-stage ADS valves, and opens the IRWST flow path to permit IRWST injection when the downcomer pressure is sufficiently low. The IRWST injection reverses the decrease in the core and downcomer water level.

The staff finds that the input parameters used in the analysis are representative of the plant conditions during Mode 5 with RCS open, and the results show that the calculated core mixture

water level remains above the top of the active fuel during the event, thus avoiding fuel failure. Therefore, the staff concludes that the analysis is acceptable.

For a loss of the RNS during mid-loop operations, the applicant performed an analysis to determine the time until core uncovery. The analysis shows that the plant response to the loss of RNS cooling during the mid-loop conditions is similar to the plant response to the loss of RNS cooling in Mode 5 with RCS open. The analysis shows that the operator has at least 100 minutes from the loss of RNS cooling until the occurrence of core uncovery, to manually actuate the IRWST and ADS stage-4 valves. Since the analysis for mid-loop operations shows that the operator has sufficient time to align IRWST and ADS stage-4 valves to prevent core uncovery from occurring, the staff concludes that the analysis is acceptable.

The applicant confirmed that the analysis of a loss of the RNS performed in Mode 5 bounds events that may occur during Mode 6, with the upper internals in place, because of the higher heat power levels. In Mode 6, the water in the refueling cavity provides a large heat sink. Following a loss of the RNS, the water in the refueling cavity can heat up and begin to boil in several hours. The applicant stated that, before boiling occurs, the operators are required to close containment. If no operator actions are taken, the water in the refueling cavity could fall below the top of the core within several days. The applicant stated that, before this time, the operators are required to align the IRWST injection and eventually containment recirculation to provide long-term cooling. In the AP600 ERG, the applicant provides guidance for the required operator actions to close containment, align IRWST injection, and establish containment recirculation for removal of the decay heat. The staff concludes that the analysis, (confirming that results of a loss of the RNS during Mode 6 with upper internals in place is bounded by that of Mode 5 conditions), is acceptable for the following reasons:

- the same ERG guidance for AP600 will be used for AP1000 for accident mitigation, and

- a sufficient operator time (several days for Mode 6 vs. 100 minutes for the Mode 5 Mid-loop operations conditions) is available to preclude core uncovery by manually actuating the IRWST and ADS stage-4 valves.

19.3.6.21 Effects of PWR Upper Internals

In NUREG/CR-5820, "Consequences of the Loss of the Residual Heat Removal System in Pressurized Water Reactors," the NRC analyzed a loss of residual heat removal event, with the vessel upper intervals in place, to determine whether it would be possible to uncover the core because of a lack of coolant circulation flow. Such conditions could occur during the flooding of the refueling pool cavity while preparing for fuel shuffling operations. Under these conditions, the vessel upper internals may provide sufficient hydraulic resistance to natural circulation flow between the refueling pool and the reactor, and may prevent the refueling water from cooling the core if the residual heat removal cooling is lost. In RAI 440.125, the staff requested the applicant to address this NUREG/CR-5820 issue and show that the AP1000 design is adequate to preclude pressurization of the RCS in Mode 6, following the loss of the RNS event.

In a letter dated October 18, 2002, the applicant responded to RAI 440.125 that the AP1000 ADS valves are required to be available in Mode 6 until the refueling cavity is filled, and the upper internals are removed. Specifically, TS 3.4.13 specifies that all ADS stages 1-3 be open, and two paths of ADS stage 4 valves be operable in Mode 6 until the reactor vessel upper internals are removed. When the refueling cavity is flooded in Mode 6 by transferring water from the IRWST to the refuel cavity, the ADS vent path allows refueling cavity water to flow down through the upper internals into the core. The open ADS flow paths, in the pressurizer, vent steam generated in the core following a loss of RNS heat removal.

The TS 3.4.13 related to ADS venting function is also applicable in Mode 5 with the RCS pressure boundary open, or with pressurizer level less than 20 percent. In addition, as discussed in DCD Tier 2 Sections 19E.4.8.5.2 and 19E4.8.5.3, and Section 19.3.6.20 of this report, the analyses of the loss of the RNS for Modes 4 and 5, and Mode 6 with upper internals in place, show that the ADS valves and IRWST flow path provide sufficient venting and injection flow capacity to avoid the core uncovery during a loss of the RNS event. Also, the AP1000 ADS valves and the IRWST path are required by TS to be available in Mode 6 until the upper internals are removed. In addition, the ERGs provide guidance for the operator to align the required ADS and IRWST valves in a loss of RNS cooling event. Therefore, the staff concludes that AP1000 design is adequate for avoiding the RCS pressurization and core uncovery in Mode 6 with the upper internals in place, following a loss of the RNS event.

19.3.7 Outage Planning and Control

The technical findings of NUREG-1449 support the determination that a comprehensive program for planning and controlling outage activities would reduce risk during shutdown, by reducing the frequency of precursor events. The staff realizes that the ultimate responsibility for outage planning and control is within the scope of the plant owners and considers this a COL action item.

DCD Tier 2 Section 13.5.1 requires the COL applicants to develop plant procedures for normal and abnormal operations; emergency operation; refueling and outage planning; alarm response; maintenance; inspection; test and surveillance, as well as administrative controls. This is COL Action Item 19.3.7-1.

The staff will review the COL applicants' outage planning and control program, and the COL applicants will have to appropriately address the factors that improve low-power and shutdown operations. As a minimum, these factors will include the following important elements:

- an outage philosophy which includes safety as a primary consideration in outage planning and implementation,

- separate organizations responsible for scheduling and overseeing the outage; provisions for an independent safety review team that would be assigned to perform final review and grant approval for outage activities,

- control procedures which address both the initial outage plan and all safety-significant changes to schedule,

- provisions to ensure that all activities receive adequate resources,

- provisions to ensure defense-in-depth during shutdown and ensure that margins are not reduced; an alternate or backup system must be available if a safety system or a defense-in-depth system is removed from service, and

- provisions to ensure that all personnel involved in outage activities are adequately trained; this should include operator simulator training to the extent practicable; other plant personnel, including temporary personnel, should receive training commensurate with the outage tasks they will be performing.

This COL information is not specified in the DCD. Therefore, this is Open Item 19.3.7-1 and COL Action Item 19.3.7-2.

19.3.8 Fire Protection

The fire protection program should address protection of safe shutdown functions, specifically decay heat removal, during shutdown and refueling operations. This is to ensure that adequate protection is provided for systems necessary to remove decay heat and maintain the RCS below saturation conditions.

The staff reviewed the AP1000 fire protection design for shutdown and refueling operations against applicable portions of Section 9.5-1 of the SRP Branch Technical Position (BTP) Chemical Engineering Branch (CMEB) 9.5-1 and NUREG-1449. In addition, in response to RAI 720.038, the applicant provided WCAP-14837, "AP600 Shutdown Evaluation Report" to the NRC staff. Although this WCAP provides a description of the AP600 fire protection design, the same features in place to minimize the occurrence of a fire in shutdown conditions, are applicable to the AP1000 fire protection design.

NUREG-1449 provides the NRC's evaluation, findings and other relevant information regarding fire protection during shutdown and refueling operations. In addition, BTP CMEB 9.5-1, Section C.7.a.(2), "Refueling and Maintenance," states that shutdown and refueling operations in containment may introduce additional hazards such as contamination control materials; decontaminations supplies; wood planking; temporary wiring; welding; and flame cutting (with portable compressed-gas fuel supply). Possible fires would not necessarily be in the vicinity of fixed detection and suppression systems. Therefore management procedures and controls are necessary to ensure adequate fire protection for transient fire loads. In addition, adequate self-contained breathing apparatus should be provided near the containment entrances for firefighting and damage control personnel. The portions of the SRP that are applicable pertain to administrative controls.

In Section 3.5 of the AP600 Shutdown Evaluation Report, the applicant specifies that the Fire Protection Analysis demonstrates the ability to achieve or maintain safe-shutdown conditions

following a fire in any fire area that occurs during shutdown modes. In Section 2.1.3.2 of the AP600 Shutdown Evaluation Report, the applicant defines plant shutdown as "the operation that brings the reactor plant from no-load operating temperature to cold shutdown conditions." Plant shutdown (Modes 3-6) consists of two distinct cooldown stages. The first cooldown stage consists of lowering the RCS temperature from 287.8 °C (550 °F) and no-load operation (Mode 3) to RCS temperature of 176.7 °C (350 °F) and 3.1 MPa (450 psig) (Mode 4). One of the SGs transfers heat from the RCS to the steam supply system. The steam supply system transfers heat to the condenser. This heat removal process will continue to remove heat as long as a vacuum is maintained in the condenser. In the event that a fire damages this heat removal process and the RNS, or its support equipment, the PRHR heat exchanger will be available to remove decay heat. Should a fire occur inside containment, the PRHR system is provided with fire protection features that provide reasonable assurance that one passive shutdown path will be available.

The PRHR will be available during Modes 4 and 5 with the RCS closed. If loss of RNS occurs during Mode 4, the PRHR will maintain the reactor in a stable shutdown condition for a long period of time. If loss of RNS occurs during Mode 5 with the RCS closed, the RCS will reheat to 215.6 °C (420 °F). The PRHR is available to maintain the reactor at stable shutdown conditions and allow sufficient time for operators to recover RNS. The IRWST gutter isolation air-operated valves (V130 A/B) will be closed to direct IRWST condensate from the containment shell gutters back to the IRWST. In this configuration, PRHR will remove decay heat from the RCS for a long period of time.

The applicant incorporated design features in the AP1000 plant that limit fire damage to the RNS system. This was accomplished by separating the redundant RNS components. RNS pumps and their associated cabling are located in separate fire areas. RNS pump A is located in fire area 1200 AF 01 and RNS pump B is located in fire area 1204 AF 01. RNS support equipment includes the component cooling water system and the service water system. In the event the component cooling water system, the service water system, and the fire protection water supply system are not available, a water connection is provided for fire truck pumpers to supply water to the secondary side of the RNS heat exchangers. This configuration will allow RNS to continue to remove decay heat without the component cooling water system, the service water system, or the fire protection water supply system.

In SECY 94-084, the staff specifies that although these systems (RNS pumps and associated cabling) are not safety-related, a high level of confidence exists that active systems that have a safety role will be available when challenged. Therefore, applicants are to maintain the integrity of these fire protection features (such as fire barriers, sprinkler systems, location of storage and amount of transient combustibles). Applicant’s administrative controls of combustibles procedures are to include limitations on the amount of combustibles in areas with redundant RNS cabling to ensure survivability of these systems. This is COL Action Item 9.5.1-1(j) (refer to Section 9.5.1 of this report). In addition, as stated in the response to Question 3, Item b of RAI 720.038, the control of combustibles is minimized through the use of noncombustible structural materials in plant buildings and the control of transient combustible materials.

The second cooldown stage is initiated at RCS temperatures less than 176.7 °C (350 °F) (Mode 4) using RNS pumps and their support equipment to continue plant cooldown. At RCS temperatures below 93.3 °C (200 °F) and 0 Pa (0 psig) (Mode 5), the RCS may be opened for refueling or other maintenance activity. In the event that the RNS system is lost because of a fire in this plant configuration, IRWST can supply water for decay heat removal. Containment will be closed and if boiling occurs in the RCS, the steam will be condensed on the inner containment shell, and drained back into IRWST. In this configuration, the plant will remain in a stable condition until RNS can be placed back into service.

Based on the applicant meeting the guidance of NUREG-1449, the applicable portions of the SRP, and SECY-94-084 as it pertains to the RNS pumps and associated cabling, the staff concludes that the AP1000 fire protection design for shutdown and refueling operations is acceptable.

19.3.9 Operator Training and Emergency Response Guidelines (DCD Tier 2 Section 19E.3.3)

The staff determined in Chapter 2 of NUREG-1449 that it is important to have adequate procedures that give detailed guidance concerning responses to a loss of reactor vessel inventory or shutdown cooling capability. Also, the alternate strategies for recovery are important to reduce risk during shutdown conditions.

DCD Tier 2 Section 18.9 indicates, (as stated by the applicant in its response to RAI 440-109), that WCAP-14690, "Designer's Input To Procedure Development for the AP600," Revision 1, issued June 1997, provides input to the COL applicant for development of plant operating procedures, including information on development and design of the AP600 ERGs and emergency operating procedures (EOP). The applicant indicated that the WCAP-14690 is directly applicable to AP1000. DCD Tier 2 Sections 19E.1.2 and 19E.3.3 indicate that the AP600 ERGs are applicable to the AP1000 ERGs, including shutdown operations.

In RAI 440.109, the staff requested that the applicant provide acceptable bases addressing the applicability of the AP600 ERGs to the AP1000. In a letter dated December 2, 2002, the applicant responded to RAI 440.109 by indicating that the design goal of the AP1000 is to make the necessary changes in the AP600 to accomplish the higher power output. As a result, the AP1000 contains larger system components such as the reactor vessel, SG and RCPs, as well as containment and turbine island. The capacity of the passive safety systems and active nonsafety-related systems are increased, as necessary, to maintain the required safety and operating margins. The configuration of the passive safety systems is the same for both the AP600 and AP1000 designs, and the role of the passive safety systems in mitigating the consequences of accidents are the same. The AP600 ERGs use both nonsafety-related systems and the passive safety systems to maximize the protection of the plant for design basis and beyond design basis accidents. The application of the AP600 ERGs for the AP1000 is similar to the implementation of the Standard ERGs for Westinghouse operating plants. Because the Westinghouse ERGs are symptom-orientated, the functional guidance included in the ERG has been applied to a range of plant designs that functionally perform in a similar manner. For the existing plants, the low-pressure ERGs have been applied to Westinghouse 2-loop, 3-loop or 4-loop plants that contain a range of nuclear steam supply system and balance

of plant system design features. Since the AP600 and AP1000 designs are similar in functional performance and the AP600 ERGs are a symptom-oriented guidance, the staff finds that the use of the AP600 ERGs as a guidance for the development of the AP1000 EOP including shutdown operations is consistent with the current licensing practice. Therefore, the staff concludes that it is acceptable.

19.3.10 Flood Protection

In NUREG-1449, the NRC stated that the safety significance of flooding or spills during shutdown depends on the equipment affected by the spills and that such spills are most often caused by human error. In DCD Tier 2 Section 3.4.1, the applicant discusses the flood protection measures that are applicable to the AP1000 plant for postulated external flooding and internal flooding from plant system and component failures.

All safety-related systems for the AP1000 design are housed in the seismic Category I containment and auxiliary buildings. Seismic Category I structures are located such that the land slopes away from the structures. This assures that external flood water will drain away from the building and prevent pooling near the building. In addition, the actual grade is a few inches lower than building entrances to prevent surface water from entering doorways.

The AP1000 design minimizes the number of penetrations through exterior walls below grade. Penetrations below the maximum flood level will be watertight and any process piping penetrating an exterior wall below grade either will be embedded in the wall or will be welded to a steel sleeve embedded in the wall. Exterior walls are designed for maximum hydrostatic loads, as are penetrations through the wall.

One of the acceptable methods of flood protection incorporates a special design of walls and penetrations. The AP1000 walls are reinforced concrete designed to resist the static and dynamic forces of the design-basis flood and incorporate water stops at construction joints to prevent in-leakage. Penetrations are sealed and also capable of withstanding the static and dynamic forces of the design-basis flood. The AP1000 design has incorporated these protective features.

Redundant safety-related systems and components are physically separated from each other, as well as from non-safety-related components. Therefore, the failure of a system or component may render one division of a safety-related system inoperable, while the redundant division is available to perform its safety function. Other protective features used to minimize the consequences of internal flooding include:

- structural enclosures
- structural barriers
- curbs and elevated thresholds
- leakage detection systems
- drainage systems

The flood sources that were considered in the internal flooding analysis included:

- high-energy piping (breaks and cracks)
- moderate-energy piping (through-wall cracks)
- pump mechanical seal failures
- storage tank ruptures
- actuation of fire suppression systems
- flow from upper elevations and adjacent areas

In the DCD, the applicant identifies seven compartments inside containment that are subject to full or partial flooding. These are the reactor vessel cavity, two SG compartments, a vertical access tunnel, the chemical and CVS compartment and two PXS compartments (PXS-A and PXS-B). Of these compartments, only the two PXS compartments contain safe-shutdown equipment. The PXS-A and PXS-B compartments, and the CVS compartment inside containment, are physically separated and isolated from each other by a structural wall so that flooding in one compartment cannot cause flooding in the other compartment. Inside these compartments, all the automatically actuated containment isolation valves (CIVs) are located above the maximum flood height with the exception of one normally closed CIV for the spent fuel pit cooling system in PXS-A and three normally closed CIVs for the RNS in PXS-B. However, these CIVs are not required for safe shutdown operation and will not fail open under flooded conditions.

In the DCD, the applicant identifies safety-related equipment in the auxiliary building that require flood protection on a room-by-room basis, depending on the relative location of the equipment. The auxiliary building is separated into RCAs and nonradiologically controlled areas (NRCAs). On each floor, structural walls and floor slabs 0.61 to 0.91 m (2 to 3 ft) wide areas separate these areas. The structures are designed to prevent floods which may occur in one area from propagating to another area. The NRCA is divided into a mechanical equipment and an electrical equipment area. The electrical equipment area is further divided into an area housing Class 1E electrical equipment and non-Class 1E electrical equipment.

The safe-shutdown equipment located in the NRCA is associated with the protection and safety monitoring system (instrumentation and control cabinets), the Class 1E dc system (Class 1E batteries and dc electrical equipment), and containment isolation. NRCAs are also designed to provide maximum separation between Class 1E and non-Class 1E electrical equipment. The AP1000 design minimizes water sources in those portions of the NRCA housing Class 1E electrical equipment.

The MCR and the RSW are also located in the NRCA. The MCR and RSW are adequately protected from flooding as a result of limited sources of flood water, pipe routing, and drain paths.

The AP1000 flooding protection scheme provides separation of the equipment and cabling for each of the four divisions of safe-shutdown equipment by using 3-hour fire-rated structural barriers. Areas containing safety-related equipment are physically separated from one another and from areas that do not contain safety-related equipment by sealed 3-hour fire-rated

barriers, with no openings in the barriers. This defense-in-depth feature results in a small probability that flooding would affect more than one safety-related system or division. In addition, the design minimizes location of potential flood sources in safety-related equipment areas to the extent possible.

Flood detection and mitigation capability is provided in the AP1000 design and is maintained during shutdown, even when parts of the automatic systems are rendered unavailable for preventive maintenance and testing. This is because compensatory measures are expected to be taken to maintain the detection and mitigation capability.

In a letter dated March 28, 2003, the applicant responded to RAI 720.038 by providing an evaluation of plant risk associated with internal floods at shutdown. The objective of this study was to confirm that the design incorporates adequate capability to achieve safe shutdown following these events, by showing that the associated plant risk is sufficiently small. Deterministic criteria were used to screen out any areas in which the risk from flooding is clearly insignificant, on the basis of the lack of flood initiation sources or absence of equipment important to safe shutdown, as modeled in the internal events PRA. Because the plant is already in shutdown, an initiating event for the shutdown analysis was considered an event leading to a threat to equipment needed for the normal decay heat removal function.

Based on the staff's preliminary review of this letter, it appears to have errors in the calculated CDF for two of the eight sequences. The applicant needs to address these errors and the staff needs to complete its review. This is Open Item 19.3.10-1.

The results from the shutdown flooding study appear to confirm that the inherent design characteristics of the AP1000 provides an effective barrier against potential internal flooding hazards. This is true even considering several conservative assumptions used in the study, such as assuming total system failure for non-safety-related fluid systems if they are affected by flooding in any area, and taking no credit for operator actions to mitigate the consequences of flooding.

The analysis identified eight internal flooding scenarios at shutdown. The total calculated contribution to CDF from internal flooding during safe shutdown is estimated to be between 3.22E-9 and 3.98E-9 per year. The correct value will be identified as part of Open Item 19.3.10-1.

The results of the internal flooding analyses are provided in DCD Tier 2 Section 19.59.6.1. The CDF from internal flooding during at power events is 8.82E-10 per year, with a large early release fraction (LERF) of 7.14E-11 per year. The CDF from internal flooding events during low-power and shutdown events is stated to be 3.33E-9 per year, with a LRF of 5.37E-10 per year.

The results of the AP1000 study for internal flooding show that the AP1000 design is adequate, such that internal floods during shutdown do not represent a significant risk contribution. The results also show that safe shutdown following internal floods can be achieved, and an acceptably low level of risk attained, using only safety-related equipment. Therefore, the staff

concludes that the AP1000 design provides adequate flood protection for systems and components required to achieve and maintain safe shutdown, and is acceptable, pending resolution of Open Item 19.3.10-1.

19.4 Consideration of Potential Design Improvements Under Requirements of 10 CFR 50.34(f)

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." For AP600, the applicant provided an evaluation of potential design improvements (Severe Accident Mitigation Design Alternatives) in Appendix 1B of the SSAR. The details of this evaluation, which included a design description and estimated risk reduction and costs for each alternative, and estimated offsite exposure for each of the major release categories, formed the basis for the staff's review. A similar evaluation was not provided in DCD Tier 2 Appendix 1B or in the PRA for AP1000, but was submitted in response to RAI 720.060.

Based on a review of the RAI response, the staff determined that the applicant's evaluation did not address a number of items called out in the RAI and had several additional deficiencies, as summarized below:

- the cost benefit methodology appears to be based on an outdated guidance document (NUREG/CR-3568, 1983), rather than the current guidance for regulatory analysis contained in NUREG/BR-0184 (1997) and NUREG/BR-0058 (2000).

- replacement power costs were omitted. These averted onsite costs need to be included consistent with SECY-99-169.

- the CDF and population dose values used in the evaluation only reflect internal events. The contribution to CDF and population dose from shutdown and fire events should also be included.

- the RAI requested an explanation of how insights from the AP1000-specific PRA and supporting risk analyses for external and shutdown events, including importance analyses and cutset screening, were used to identify potential plant improvements. This was not addressed in the response.

- the RAI requested justification that the potential improvements identified through a systematic process (as suggested above) are included within the set of 15 SAMDAs identified in Appendix 1B of the AP1000 DCD. This was not addressed in the response.

In a revised RAI response dated March 31, 2003, the applicant provided an updated evaluation addressing these concerns. The staff has not completed of its evaluation of SAMDAs for AP1000. Therefore, this is Open Item 19.4-1.

Table 19.1.1 Comparison of Core Damage Frequency Contributions by Initiating Event (Internal Events and Power Operation).

Initiating Event	AP1000 (CDF/yr)	Operating PWRs (CDF range/yr) IPE results [NUREG-1560]
LOCAs (Total)	2.1E-07	1E-6 to 8E-5
- Large	4.5E-08	
- Spurious ADS Actuation	3.0E-08	
- Safety Injection Line Break	9.5E-08	
- Medium	1.6E-08	
- Small	1.8E-08	
- CMT Line Break	4.0E-09	
- RCS Leak	3.0E-09	
Steam Generator Tube Rupture (SGTR)	7.0E-09	9E-9 to 3E-5
Transients	8.0E-09	5E-7 to 3E-4
Loss of Offsite Power/Station Blackout	1.0E-09	1E-8 to 7E-5
Anticipated Transient Without Scram (ATWS)	5.0E-09	1E-8 to 4E-5
Interfacing System LOCA	5.0E-11	1E-9 to 8E-6
Vessel Rupture	1.0E-08	1E-7
Total	2.4E-07	4E-6 to 3E-4

Table 19.1-2 Level 1 Accident Class Functional Definitions and Core Damage Frequencies

Accident Class	Definition	RCS Pressure at Uncovery	CDF	% of Total CDF
1A	Core damage with RCS at high pressure following transient or RCS leak	>1100	5.01E-9	2.1
1AP	Core damage with no depressurization following small LOCA and RCS leak with passive RHR operating, or intermediate LOCA	~1100	1.48E-9	0.6
3A	Core damage with RCS at high pressure following ATWS or main steamline break inside containment	>1100	4.43E-9	1.8
3BR	Core damage following large LOCA with full RCS depressurization, but accumulator failed	~0	4.63E-8	19.2
3BE	Core damage following large LOCAs or other event with full depressurization	~0	8.06E-8	33.4
3BL	Core damage at long term following failure of water recirculation to RPV after successful gravity injection	~0	2.40E-8	9.9
3C	Core damage following vessel rupture	~0	1.0E-8	4.2
1D	Core damage with partial depressurization of RCS following transient	<150	5.97E-8	24.8
3D	Core damage following LOCA (except large) with partial depressurization			
6E	Core damage following SGTR or ISLOCA. Early core damage (loss of injection)	Sequence Specific	9.52E-9	4.0
6L	Core damage following SGTR. Late core damage (loss of recirculation)			
TOTAL			2.41E-7	100.0

Table 19.1-3 Conditional Containment Failure Probability by Accident Class

Accident Class	CCFP (%)
1A	40.9
1AP	42.1
3A	92.2
3BR	0.2
3BE	4.4
3BL	2.4
3C	10.3
3D/1D	5.7
6E/6L	43.1
Weighted Average*	8.1

*Weighted on the basis of core damage frequencies provided in Table 19.1-2

Table 19.1-4 Containment Release Categories and Associated Frequencies

Containment Release Category	Frequency	% of CDF	% of LRF
Intact Containment (IC)	2.2E-7	91.9	NA
Early Containment Failure (CFE)	7.5E-9	3.1	38
Intermediate Containment Failure (CFI)	1.9E-10	<0.1	1
Late Containment Failure (CFL)	3.5E-13	<0.1	<0.1
Containment Isolation Failure (CI)	1.3E-9	0.6	7
Containment Bypass (BP)	1.1E-8	4.4	54
Total	2.4E-7	100	100

Table 19.1-5 Contribution to Risk from Various Release Categories, as Reported by Westinghouse (72 Hour Mission Time)

Containment Release Category	Frequency	P-Rem/Event	P-Rem/y	% Risk
Intact Containment (IC)	2.2E-7	8.8E2	1.9E-4	1
Early Containment Failure (CFE)	7.5E-9	9.4E5	7.0E-3	52
Intermediate Containment Failure (CFI)	1.9E-10	8.9E5	1.7E-4	1
Late Containment Failure (CFL)	3.5E-13	5.8E5	2.0E-7	--
Containment Isolation Failure (CI)	1.3E-9	2.1E6	2.9E-3	21
Containment Bypass (BP)	1.1E-8	3.1E5	3.3E-3	24
Total	2.4E-7		1.3E-2	100

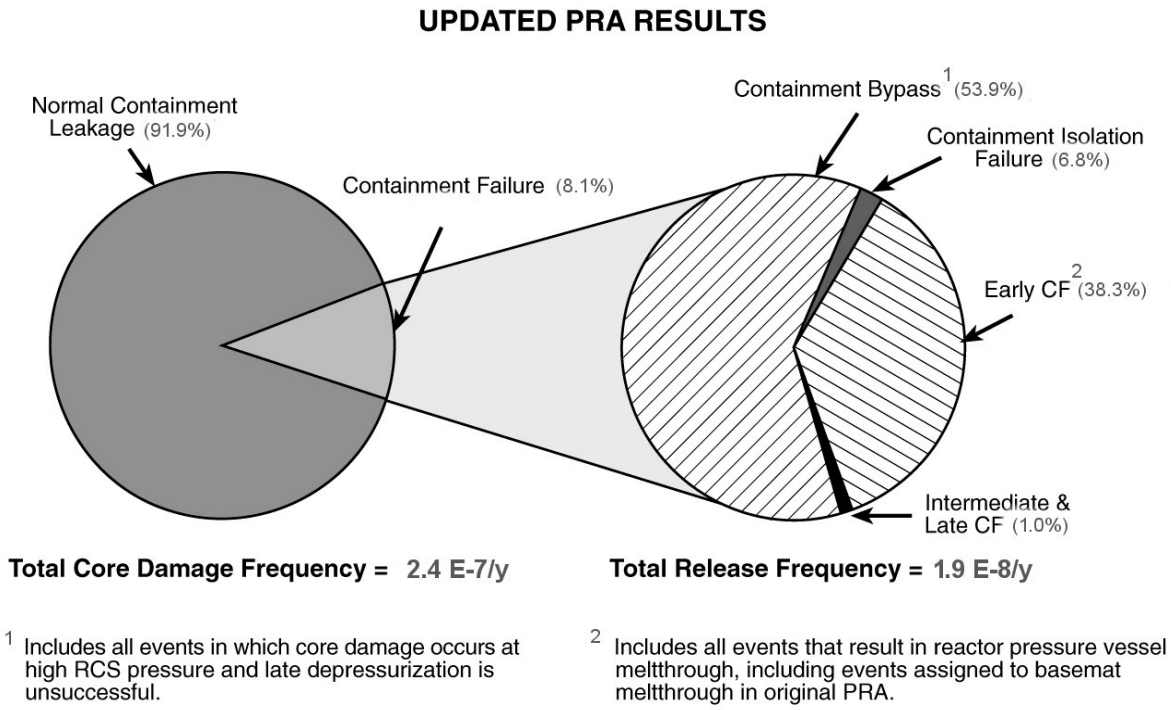
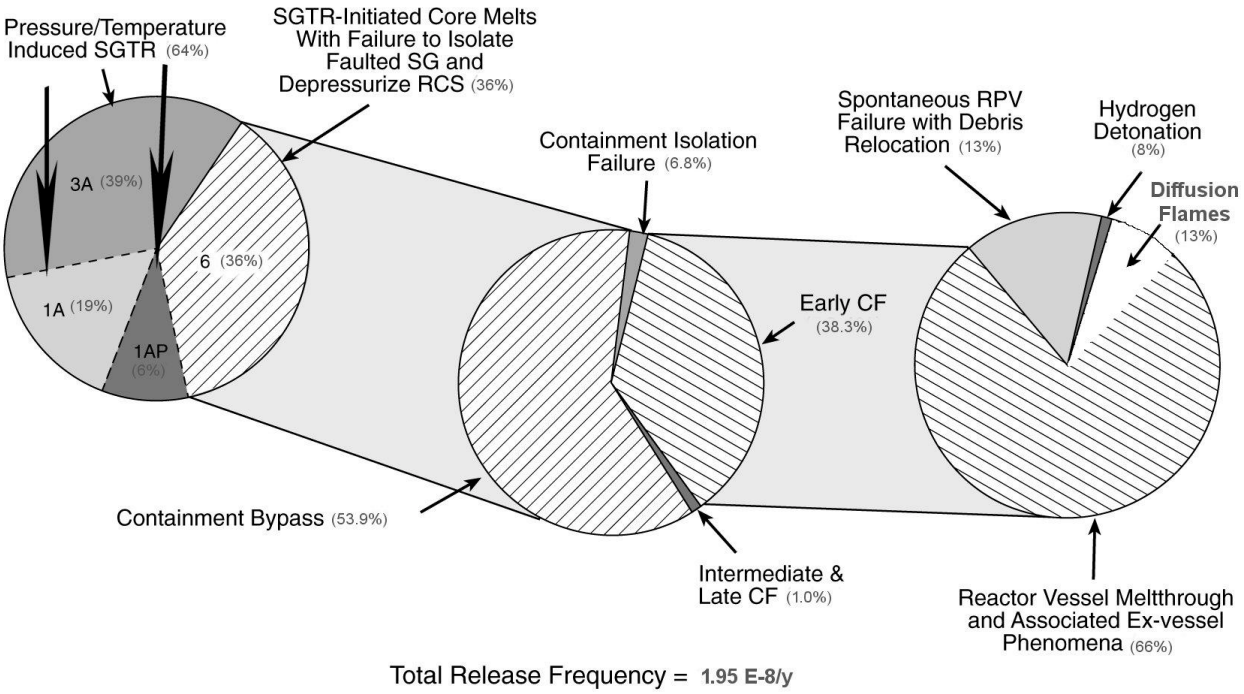


Figure 19.1-1

Breakdown of Containment Release Frequency
Based on the Level 2 PRA Results Reported by Westinghouse
(Baseline PRA, Internal Events)



Breakdown of AP1000 Containment Release Modes by Contributor, as Reported by Westinghouse

Figure 19.1-2

Breakdown of AP1000 Containment Release Modes by Contributor,
as Reported by Westinghouse

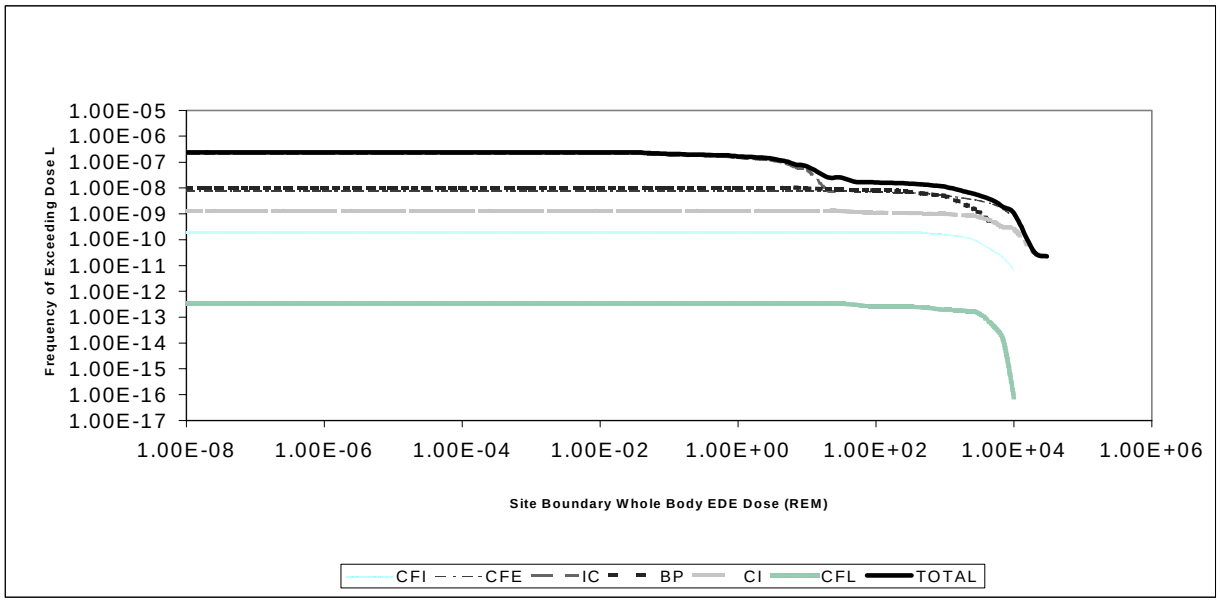


Figure 19.1-3
Overall Dose Risk
Site Boundary Whole Body EDE, 24 Hour Dose

Section 19A Seismic Margin Analysis

Background

In DCD Tier 2 Chapter 19, with supporting details in Chapter 55 of the AP1000 PRA, Revision 0, the applicant discusses the seismic margin analysis (SMA). In this section, the staff evaluated the adequacy of the AP1000 seismic margin analysis to estimate the high confidence in low probability of a failure (HCLPF) capacity of the AP1000 plant in terms of a minimum peak ground acceleration value of 0.5 g, as explained below.

In the SRM dated July 21, 1993, the Commission approved the following staff recommendation specified in Section II.N, "Site-Specific Probabilistic Risk Assessments and Analysis of External Events" of SECY-93-087 with modification:

> PRA insights will be used to support a margins-type assessment of seismic events. A PRA-based seismic margins analysis will consider sequence-level High Confidence, Low Probability of Failures (HCLPFs) and fragilities for all sequences leading to core damage or containment failures up to approximately one and two-thirds the ground motion acceleration of the Design Basis SSE [safe shutdown earthquake].

For the AP1000 standard design, application of the above criteria results in a requirement of a HCLPF value of 0.5 g.

19A.1 Seismic Margin HCLPF Methodology

The applicant based the AP1000 SMA on established criteria, design specifications, existing qualifications test reports, established designs, and public domain generic data. A review level earthquake (RLE) equal to 0.5 g was established for the SMA, and used to demonstrate a margin over the SSE of 0.3 g. This RLE is consistent with SRM SECY-93-087.

The site parameters that constitute the seismic design basis for AP1000 are discussed in DCD Tier 2 Table 2.1. The seismic ground motion spectrum for 0.5 g RLE is based on the AP1000 design response spectra anchored to 0.5 g peak ground acceleration value, and the seismic design criteria and methodology used in the design of structures, systems and components are described in DCD Tier 2 Chapter 3. The applicant used highly simplified hierarchical failure levels to arrive at the plant level HCLPF value. The basic approach is PRA centered and consistent with, Budnitz, R. J., et al., “An Approach to the Quantification of Seismic Margins in Nuclear Power Plants,” NUREG/CR-4334, UCID-20444, August, 1985. The staff finds the applicant has tended to use a lower capacity where a more detailed evaluation can yield a higher capacity. This approach of using a simplified method to obtain a lower capacity, incorporates a conservative bias, and is, therefore, acceptable.

19A.2 Calculation of HCLPF Values

There are two parts to the calculation of plant HCLPF value; one part consists of an analysis of systems required for safe shutdown of the plant, and the other part consists of evaluating the seismic capacity of components and structures that comprise those safe shutdown systems.

The applicant did not rely on any non-safety related systems to achieve safe shutdown following a seismically induced plant damage condition. The applicant used a sustainable safe plant state to achieve its success criterion for treating seismically induced plant challenges.

For the determination of HCLPF values of equipment and structures, the applicant used one of the following means:

- Probabilistic fragility analysis
- Conservative deterministic failure method
- Test results
- Deterministic approach
- Generic fragility data.

Probabilistic Fragility Analysis (FA)

In many seismic PRAs, the fragility of a component is represented by a lognormal model using three parameters as follows: (1) A_m for median ground acceleration capacity, (2) logarithmic standard deviation (LSD) $ß_r$ for randomness in the capacity, and (3) LSD $ß_u$ for uncertainty in the median value. The values of $ß_r$, and $ß_u$, are estimated using design analysis information, test data, earthquake experience data, and engineering judgment. In estimating the median ground acceleration capacity and the associated variability, an intermediate variable defined as margin factor, F, is used. The margin factor is related to the median ground acceleration capacity by the equation of $A_m = FA_d$, where A_d is the ground acceleration of the reference design earthquake (i.e., the SSE peak ground acceleration [PGA] for the plant) to which the structure or component is designed. The composite LSD for the associated variability ($ß_c$) is defined by $(ß_r^2+ß_u^2)^{½}$.

A key step in the seismic fragility estimate involves the evaluation of the margin factor associated with the design for each important potential failure mode. The design margins inherent in the component capacity and the dynamic response to the specific acceleration are two basic considerations. Each of the capacity and response margins involves several variables, and each variable has a median margin factor and variability associated with it. The overall margin factor F is the product of the margin factor for each variable F_i. The overall composite LSD is the square root of sum of squares (SRSS) of the composite LSDs in the individual margin factors.

The HCLPF capacity is calculated using this fragility model as:

$$\text{HCLPF capacity} = A_m \exp(-1.65\,[ß_r + ß_u]) = A_m \exp(-2.326\,ß_c)$$

The mean peak ground acceleration capacity, $A_{m,}$ is related to the stress and and strength design margin factors by the following expression:

$$A_m=(\Pi_i[X_i])Ao$$

where, A_m = Median capacity with respect to the peak ground acceleration value
X_i = ith design margin factor
Π_i = product notation
Ao = nominal design capacity with respect to peak ground acceleration capacity

The applicant included the following basic factors for the seismic margin calculation:

- Deterministic strength factor
- Variable strength factors
- Material
- Damping
- Inelastic energy absorption/ductility
- Analysis or modeling error
- Soil-structure interaction

Deterministic Strength Factor

The deterministic design process involves the use of: (1) actual stress that is less than the allowable value specified in the design code, and (2) the margin used in the code allowable values by the code or standard developing body. The applicant has not explained how this factor was used in its probabilistic fragility analysis. This is Open Item 19A.2-1.

Variable Strength Factors

Variability exists between the design capacity and the test capacity. This phenomenon is inherent in the manner in which an actual structure redistributes loads based on redundancy, excess capacity provided by design, end constraints and other factors. The applicant has not explained how this factor was used in its probabilistic fragility analysis. This is Open Item 19A.2-2.

Material

The allowable stress values provided in codes and standards are based on minimum specified yield strength in tension or compressive strength in crushing. Consequently, actual material properties that are derived from the yield strength or crushing strength have variability. The applicant has not explained how this factor was used in its probabilistic fragility analysis. This is Open Item 19A.2-3.

Damping

The design seismic load is determined from response spectrum curves associated with the design damping value. Design damping values are established conservatively because the seismic Category I structures, systems and components are expected to remain functional at the design level in order to achieve safe shutdown. Damping values at the capacity level earthquake, near failure, are higher. Of the components that the applicant used the probabilistic fragility analysis, conservative damping values in the range of 4 percent to 5 percent of critical damping were used. The staff finds the damping values used by the applicant to be lower than the values associated with failure level motion; consequently, the values selected by the applicant are conservative. Therefore, the values are acceptable.

Inelastic Energy Absorption/Ductility

The inelastic energy absorption depends on the behavior of the structure or component. If the structure is ductile, it can undergo considerable post-yield deformation without rupture or failure. The postyield deformation of a structure allows it to absorb the earthquake energy, and as a secondary effect, the stiffness of the structure is reduced. This leads to a lower demand in earthquake loading. The applicant used a global ductility margin factor of 2.25 for the inner containment structure and the IRWST module which is a concrete filled shear wall type structure made of steel plates. The corresponding composite logarithmic standard deviation is 0.25. These values are reasonable and consistent with test results. The staff finds the use of the value of the ductility margin factor reasonable and acceptable.

Analysis or Modeling Error

Modeling error stems from a number of sources that include stiffness parameters, modeling of masses due to live load, connectivity between structural members, support conditions, and others. The applicant did not explain how this factor was used in its probabilistic fragility analysis of various structures and equipment. For the modal frequency variation, the applicant used a composite logarithmic standard deviation, $ß_c$, of 0.3. The use of a $ß_c$ value of 0.3 means that modal frequency values can vary by a factor of 1.8. The applicant needs to justify the use of such a high variability factor for the natural frequency calculations when using detailed finite element models. This is Open Item 19A.2-4.

With respect to the containment buckling failure mode, the applicant used a composite logarithmic standard deviation of 0.64 for the critical buckling load. The use of 0.64 as a logarithmic standard deviation is consistent with NUREG/CR-3127, "Probabilistic Seismic Resistance of Steel Containment," dated January 1984 (page 9). Therefore, it is acceptable.

Soil-Structure Interaction

How the structure behaves with the foundation material in which the structure is embedded when subjected to seismic excitation, is analytically determined by the soil-structure interaction (SSI) analysis. For design purposes, the soil parameters are varied by a factor of 2 higher and lower, then the results are enveloped. Consequently, the SSI effect can introduce a

considerable variation in the calculated margin. However, the AP1000 design is to be located on hard rock sites, since the seismic design assumes a fixed base condition; consequently, no SSI analysis is involved in its design. Therefore, the discussion about the SSI related variability in Chapter 55 of the PRA report for AP1000 is inappropriate, since the use of the variability factor $(\beta_c)_{SSI}$ is not justified. This issue is Open Item 19A.2-5.

Conservative Deterministic Failure Margin Method (CDFM)

The applicant used the CDFM method to calculate the HCLPF value of the shield building using strength, inelastic energy absorption and damping as areas where the shield building capacity is increased over the design capacity to determine the cumulative effect of those factors. The applicant has increased the shear capacity of a concrete section by increasing the shear modulus to account for the shear strength of reinforcement bars where the shear load exceeds the shear strength of concrete alone. The ACI 349 Code, the applicable concrete design code, allows the addition of reinforcement strength, but not by increasing the shear modulus of the concrete section. The shield building tension ring has a HCLPF value of 0.51 g (Table 55-1, Sheet 1 of 4). Therefore, a validation of the capacity of the shield building shear walls is important. With respect to inelastic energy absorption and damping factors, it is not clear as to whether or not the applicant has double counted damping values through the use of hysteretic damping for inelastic energy absorption and a damping value of 10 percent. The applicant needs to justify the details of the CDFM approach for calculating HCLPF values for important structures and equipment. It should be noted that the containment internal structure and the nuclear island basemat are predicted to lift up under the SSE loading. As noted in Section 3.7 of this report, the effect of uplift due to design basis seismic excitation is an open area. Consequently, at 0.5 g review level earthquake, the capacity of the tension ring could potentially be lower. Therefore, the validation of HCLPF values calculated by the CDFM approach is Open Item 19A.2-6.

Test Results

AP1000 has many design features that contribute significantly to enhance safe plant configuration during and following an earthquake challenge (e.g., control rods are automatically inserted in the core on loss of AC power, the passive residual heat removal and core makeup tank system valves automatically fail open on loss of instrument air whenever these losses are caused by seismically induced loss of off-site power). In the AP1000 design, the applicant uses solid-state switching devices and robust electro-mechanical relays to avoid plant safety system degradation due to relay chatter. Consequently, relay chatter phenomenon does not control any equipment HCLPF value. This aspect of the AP1000 design is seismically robust and acceptable.

The applicant determined the HCLPF values on the basis of the estimated lower bound of qualification test results. When natural frequencies were not known, it was assumed that the equipment natural frequency coincides with the response spectra peak. When equipment frequencies are known and used for comparing the required response spectra (RRS) to the test response spectra (TRS), this information is to be included in the design specification. The applicant has not identified any equipment for which such design specification will be included.

Although the applicant appears to have used a conservative approach to obtain the equipment HCLPF value from test results, it not clear how the use of known natural frequency values for equipment within the standard design scope will be implemented. Since there are many electrical components with HCLPF values at 0.54 g and one at 0.53 g, electrical components may become critical in determining the plant HCLPF value. This is Open Item 19A.2-7.

Deterministic Approach

The applicant used the deterministic approach to estimate the HCLPF values of primary system component supports. The components included in this approach are: polar crane, baffle plate supports, heat exchanger for the passive residual heat removal system, core makeup tank and valves. The applicant used lower bound values, and it appears that there was no need for invoking factors of conservatism to arrive at the HCLPF values. It is noted that the core makeup tank has a HCLPF value of 0.54 g; therefore, any increase in seismic response of the containment internal structure due to lift off of the internal structure or the nuclear island structure would necessitate a review of this HCLPF value. This is Open Item 19A.2-8.

Generic Fragility Data

When HCLPF values could not be determined by using one of the methods described above, Westinghouse used generic fragility data. The cases where this approach was used are the following:

- Reactor internals and core assembly that includes fuel
- Control rod drive mechanism (CRDM) and hydraulic drive units
- Reactor coolant pump
- Accumulator tank
- Piping
- Cable trays
- Valves
- Main control room operation and switch stations
- Ceramic insulators
- Battery racks

The generic fragility data came from the Utility Requirements Document which was reviewed by the NRC. Therefore, the use of generic fragility data developed by a joint industry group in the Utility Requirements Document is acceptable. However, the applicant has not indicated what amplification factor, if any, was used to adjust the generic fragility data for the AP1000 configuration. The PCS water flow transmitter, located at Elevation 261' with a HCLPF value of 0.53 g, is likely to have an amplified seismic response. The applicant needs to justify the HCLPF values in the range of 0.53 g and 0.73 g that were obtained from the generic data as shown in the AP1000 PRA Table 55-1, Sheet 3 of 4. This is Open Item 19A.2-9.

Evaluation of Seismic Capacities of Components and Plant

As shown in the fragility values list (AP1000 PRA Table 55-1), all the HCLPF values are higher than 0.5g, except for the ceramic insulators. Ceramic insulators are not safety related, so their failure during an earthquake can disrupt the off-site AC power; however, the AP1000 plant design is such that it can safely accommodate the loss of off-site power. The staff finds that upon resolution of the open items discussed above, the seismic HCLPF value of 0.5 g will be validated.

Verification of Equipment Fragility Data

In order to ensure that a plant, built in accordance with the AP1000 standard design, has a minimum seismic HCLPF value of 0.5 g, the applicant has a COL applicant interface requirement to compare the as-built HCLPF to the seismic margin evaluation. The staff agrees that this interface requirement is appropriate and acceptable. This is COL Action Item 19A.2-1.

Turbine Building Seismic Interaction

The applicant examined the seismic interaction between the turbine building and the nuclear island as part of the SMA, and determined the following:

- The structural integrity of the adjacent auxiliary building will not be lost with the failure of the turbine building.

- It is not likely that the size and energy of debris from the turbine building will be large enough to result in penetration through the auxiliary building roof structure.

Nevertheless, the applicant evaluated the consequences of damage to the safety-related equipment in the auxiliary building. Assuming the failure of equipment in the upper elevations of the auxiliary building as a result of an adverse seismic interaction with the non-safety related turbine building, the plant HCLPF value, and the insights derived from the SMA would not be affected. The applicant indicates that the steamline break events that could damage equipment in upper elevations are not dominant contributors to the core damage frequency. Therefore, any loss of equipment in the upper elevations should not affect the passive safety systems used to put the plant in a safe-shutdown condition. The staff finds that Westinghouse has adequately considered the interaction effect between the non-safety related turbine building and the safety-related auxiliary building. Any minor damage to the safety related auxiliary building should not degrade the seismic performance of the plant or reduce its seismic HCLPF value. This consideration of the interaction effect is acceptable.

19A.3 Seismic Margin Model

Major SMA Model Assumptions

The applicant has used a PRA based seismic margin analysis method similar to the AP600 plant. In conducting its SMA, the applicant made the following assumptions:

- Seismic events occur at full power

- The review level earthquake (RLE) is 0.5 g
- The loss of offsite power occurs at the RLE. No credit is taken for non-safety related diesel generators for on-site AC power
- No credit is taken for non-safety related systems
- Initiating seismic event categories are derived from the AP600 model and the min-max method was used to calculate the plant HCLPF value

The staff notes that the seismic response of the AP1000 structures and some primary system components could be higher than those in AP600, because the height of the containment and the overall mass of AP1000 plant have increased. As indicated in the previous section of this report, it will be necessary to resolve the open items prior to the acceptance of the validity of plant seismic event trees derived from the AP600 model. This is Open Item 19A.3-1.

Seismic Initiating Events

The applicant arranged the seismic event categories in the following hierarchical groups:

- EQ-STRUC - Gross structural failure.
- EQ-RVFA - Failure of the reactor vessel occurs.
- EQ-LLOCA - Failure of reactor coolant system.
- EQ-SLOCA - Steam generator tube rupture and large secondary line break.
- EQ-ATWS - Anticipated transient without scram caused by an earthquake.
- EQ-LOSP - Loss of off-site power caused by an earthquake.

Assuming that the HCLPF values of structures and components, as shown in Table 55-1 of the AP1000 PRA, are validated following the resolution of open items discussed in the previous section, the staff considers the use of the simplified seismic event tree approach to be reasonable for the purpose of assessing the seismic vulnerability of components and systems.

Initiating Event Category HCLPFs

For all seismic event categories, except for the EQ-LOSP category, the HCLPF values of various seismic initiating event groups exceed 0.5 g. Each category of HCLPF group is discussed further below:

- EQ-STRUC Group: The lowest HCLPF value of the Nuclear Island (NI) structure that can influence the plant HCLPF value is .05 g, based on the values shown in Table 55-1 of the AP1000 PRA. The HCLPF values shown in Table 55-1 need to be validated through the resolution of Open Item 19A2-8 discussed in the previous section. The applicant has assumed that there is no detrimental effect from any seismic interaction between the NI and the adjacent turbine, annex, diesel generator and radwaste building structures. The applicant has stated, “this assumption needs to be verified by a plant walkdown when an AP1000 plant is built.” However, there is no entry on the COL interface requirement about the plant walkdown in Table 1.8-2 of the DCD. There is an entry in Table 1.8-2 19.59.10-1, “As-Built SSC HCLPF Comparison to Seismic Margin Evaluation.” The applicant needs to justify why a specific item on plant walkdown

verification of seismic interaction between the NI and adjacent structures is not included in the COL interface requirement. This is Open Item 19A.3-2.

- EQ-RVFA: The HCLPF of this group is dominated by the core (fuel) failure. The staff finds this approach and fuel HCLPF values reasonable. The staff notes that this approach was similar to the AP600. There are several areas in the seismic analysis methods where the applicant will have to resolve open issues related to seismic uplift, and stiffness reduction of concrete shear walls. Consequently, the seismic response of the EQ-RVFA group could increase leading to a reduced HCLPF value for the EQ-RVFA group.

- EQ-LLOCA: The applicant has included break sizes larger than 22.9 cm (9 in.), assumed simultaneous failure of all similar redundant pipes, and also included the failure of the passive RHR heat exchanger in this group. The staff finds the approach used for this group reasonable.

- EQ-SLOCA: The applicant included a number of elements of seismic fragility in this group. These elements include, simultaneous failure of all small diameter instrument lines, steam generator tube rupture, and large steam line breaks. Steam generator tube rupture event considers up to 5 simultaneous tube ruptures. The EQ-SLOCA grouping appears reasonable. However it is not clear if the applicant considered degradation of steam generator tubes under the full service life of steam generators for developing the seismic fragility. The applicant should explain how service related degradation of steam generator tubes was considered in the development of the HCLPF value of this group. This is Open Item 19A.3-3.

- EQ-LOSP: The applicant has conservatively assumed 0.09 g as the HCLPF value for the EQ-LOSP category bounded by the capacity of ceramic insulators. The AP1000 design does not rely on diesel generators to prevent core damage. Instead, it relies on the passive systems to maintain a stable plant configuration without core damage. The staff agrees that the EQ-LOSP does not control the plant HCLPF value.

19A.4 Calculation of Plant HCLPF

The applicant calculated the HCLPF values for the basic events from the seismic analysis model, and presented the values in Table 55-2. There are identical and closely spaced HCLPF values, 4 at 0.5 g and 6 at 0.51 g. There are several open items associated with this safety evaluation that must be resolved, before the HCLPF values for the basic events can be accepted as reasonable. The applicant used established criteria, design specifications, existing qualification test reports, established design characteristics and configurations, and public domain generic data to obtain the HCLPF values of the equipment and structures. The staff finds that the approach and methodology used by the applicant for the analysis of plant HCLPF value is reasonable, and has a conservative bias.

19A.5 Conclusion

SECY-93-087 provides that each plant designer perform a PRA-based margins analysis to identify the vulnerabilities of the design to seismic events larger than the design basis SSE. In the SRM dated July 21, 1993, the Commission approved the HCLPF values at least one and two-thirds of the ground motion acceleration of the design basis SSE for the important SSCs required for safe shutdown. For the AP1000 standard design, this ground motion should be at least at a level that causes peak ground acceleration value of 0.5 g.

In order to satisfy this requirement, the applicant performed a PRA-based SMA to assess the seismic robustness of the AP1000 design, and to provide an acceptable estimate of the maximum earthquake ground motion which the AP1000 plant is expected to be able to survive without core damage.

On the basis of its review of the methodology discussed in Chapter 55 of the AP1000 PRA, the staff concludes that upon the closure of the open items discussed above, the AP1000 SMA is founded on an acceptable methodology and that the HCLPF values for the important SSCs are equal to or greater than the minimum required peak ground acceleration of 0.5 g. Thus, the AP1000 standard design meets the criteria indicated in SECY-93-087, the corresponding SRM regarding the SMA methodology, and is, therefore acceptable.