19. SEVERE ACCIDENTS

19.0.1 Background

Title 10, Part 1, of the Code of Federal Regulations (10 CFR Part 1) defines the Federal regulations for the design, construction, licensing, and operation of commercial nuclear power plants. The U.S. Nuclear Regulatory Commission (NRC) evaluated the design of the AP1000 against these regulations, as documented in this report. Compliance with the Commission's regulations ensures adequate protection of the public health and safety during the operation of a nuclear power plant. In previous applications, the final safety analysis report (FSAR) demonstrated compliance with these regulations and established the design basis of the plant. The Commission has developed guidance and goals for resolving those safety issues related to reactor accidents more severe than the design-basis accidents (DBAs). These "severe accidents" are those in which substantial damage is done to the reactor core, regardless of whether serious offsite consequences occur.

Following the 1979 accident at the Three Mile Island (TMI) Nuclear Plant, Unit 2, it was recognized that severe accidents needed further attention. The NRC evaluated, generically, the capability of existing plants to tolerate a severe accident. The NRC 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, "Policy Statement on Severe Accidents Regarding Future Designs and Existing Plants," (50 FR 32138, August 8, 1985), 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 affecting these plants because of the risk posed by a severe accident. To address this issue for operating plants in the long term, the NRC issued SECY-88-147, "Integration Plan for Closure of Severe Accident Issues," in May 1988. This document identified the following necessary elements for closure of severe accidents:

- performance of an individual plant examination
- assessment of generic containment performance improvements (CPIs)
- 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 to accommodate events that are beyond the design basis of the plant. Designers should strive to meet these goals.

For advanced nuclear power plants, including both the evolutionary and passive designs, the NRC concluded that vendors should address severe accidents during the design stage. Designers can 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 is much more cost effective than modifying existing plants.

Regulatory Guidance

The NRC has issued requirements and guidance for addressing severe accidents in the following documents:

- NRC Policy Statement, "Severe Reactor Accidents Regarding Future Designs and Existing Plants" (Volume 50, page 32138, of the Federal Register (50 FR 32138) dated August 8, 1985)

- NRC Policy Statement, "Safety Goals for the Operations of Nuclear Power Plants" (51 FR 28044 dated August 4, 1986)

- NRC Policy Statement, "Nuclear Power Plant Standardization" (52 FR 34844 dated September 15, 1987)

- NRC Policy Statement, "The Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities" (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 (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements," issued January 12, 1990, and the corresponding staff requirements memorandum (SRM), issued June 26, 1990

- SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs," issued April 2, 1993, and the corresponding SRM, issued July 21, 1993

- SECY-96-128, "Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design," issued June 12, 1996, and the corresponding SRM, issued January 15, 1997

- SECY-97-044, "Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design," issued February 18, 1997, and the corresponding SRM, issued June 30, 1997

The first four documents provide guidance as to the appropriate course for addressing severe accidents and the use of probabilistic risk assessment (PRA). Title 10, Part 52, of the Code of Federal Regulations (10 CFR Part 52) contains general requirements for addressing severe accidents (10 CFR 52.47); and the SRMs relating to SECY-90-016, SECY-93-087,

SECY-96-128, and SECY-97-044 provide Commission-approved guidance for implementing features in new designs to prevent severe accidents and to mitigate their effects, should they occur.

Severe Accident Policy Statement

The Commission issued its policy statement entitled, "Severe Reactor Accidents Regarding Future Designs and Existing Plants," on August 8, 1985. This policy statement was prompted by the NRC's judgment that severe accidents, 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 is 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 describes the policy that the Commission uses to resolve safety issues related to reactor accidents more severe than DBAs. The statement focuses on the guidance and procedures the Commission intends 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, this policy statement affirms the Commission's belief that a new design for a nuclear power plant can be shown to adequately address severe accident concerns if it meets the following guidance:

- demonstration of compliance with the requirements of current Commission regulations, including the TMI requirements for new plants, as reflected in 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 (GSI), including a special focus on assuring the reliability of decay heat removal (DHR) systems and the reliability of both alternating current (ac) and direct current (dc) electrical supply systems

- completion of a PRA and consideration of the severe accident vulnerabilities exposed by the PRA, 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

At the time it issued the Severe Accident Policy Statement, the Commission believed that an adequate basis existed to establish appropriate guidance. 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 vendors engaged in designing new standard plants to achieve a higher standard of severe accident safety performance than they achieved in previous designs.

Severe Accidents

Safety Goals Policy Statement

The Commission issued its policy statement entitled, “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 risks are associated with the release of radioactive material from the reactor to the environment during normal operations, as well as from accidents. The Commission established the following two qualitative safety goals:

(1) 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.

(2) 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.

These two qualitative objectives are supported by the following two quantitative objectives that determine achievement of the above safety goals:

(1) 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.

(2) 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 the NRC safety policy expresses the Commission’s views on the level of risk 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 its policy statement entitled, “Nuclear Power Plant Standardization,” on September 15, 1987. This policy statement encourages the use of standard plant designs and contains information concerning the certification of plant designs that are essentially complete in terms of 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. With respect to severe accidents, the NRC expects applicants for a design certification to address the guidance for new plant designs provided in the Commission's Severe Accident Policy Statement.

Use of PRA Methods in Nuclear Regulatory Activities Policy Statement

The Commission issued its policy statement entitled, "Use of Nuclear Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities," on August 16, 1995. This statement outlines the policy that the NRC will follow for using PRA methods in nuclear regulatory matters. The Commission established this policy so that the many potential applications of PRA could be implemented in a consistent and predictable manner to promote regulatory stability and efficiency. The Commission adopted the following policy statement regarding the expanded NRC use of PRA:

- 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.

- 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.

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

- 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 (ESPs), standard design certifications, and combined licenses (COLs) 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, as well as to enhance the safety and reliability of nuclear power plants. With regard to severe accidents, 10 CFR Part 52 codifies some parts

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 do the following:

- demonstrate compliance with any technically relevant portion of the TMI requirements set forth in 10 CFR 50.34(f)

- propose technical resolutions of those USIs and medium- and high-priority GSIs which are identified in the version of NUREG-0933, "A Prioritization of Generic Safety Issues," 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 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 evolved from SECY-90-016. SECY-93-087 addresses the following preventive feature issues relating to the AP1000:

- anticipated transient without scram (ATWS)
- midloop operation
- station blackout (SBO)
- fire protection
- intersystem loss-of-coolant accident (ISLOCA)

SECY-93-087 addresses the following mitigative features relating to the AP1000:

- 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 (SGTRs)

The Commission approved some of the staff positions stated in 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 (ERVC)

The Commission provided additional guidance concerning prevention and mitigation of severe accidents and approved the staff's position concerning ERVC 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 responded 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 is 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 resolving the severe accident issues associated with the AP1000 design are the requirements of 10 CFR Part 52, as well as the guidance in 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:

- compliance with the TMI requirements in 10 CFR 50.34(f)
- resolution of USIs
- resolution of GSIs
- completion of a design-specific PRA

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

The Commission-approved guidance 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 this guidance in Section 19.2 of this report.

19.1 Probabilistic Risk Assessment

19.1.1 Introduction

As part of the AP1000 advanced design certification application, the applicant submitted a PRA in accordance with the requirements of 10 CFR 52.47 and the Commission's policy statement entitled, "Severe Reactor Accidents Regarding Future Designs and Existing Plants." The 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 the NRC review of the AP1000 design PRA include the following:

- identification of risk-informed safety insights based on systematic evaluations of risk associated with the design
- support of the process used to determine whether regulatory treatment of non-safety systems (RTNSS) was necessary
- determination, in a quantitative manner, as to whether the design represents a reduction in risk over existing plants
- assessment of the balance of preventive and mitigative features of the design
- assessment of the reasonableness of the risk estimates documented in the PRA
- support of the design certification requirements, such as inspection, tests, analyses, and acceptance criteria (ITAACs), design reliability assurance program (D-RAP), and technical specifications (TS), as well as 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-4/yr for core damage frequency (CDF) and less than 1E-6/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 Goals 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, the AP1000 PRA and the staff's review of this analysis have achieved these objectives.

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, TS, plant-specific emergency operating procedures, and design changes. These updates are the responsibility of the COL applicant. This is COL Action Item 19.1.1.1-1.

As plant experience data accumulates, the COL holder will update failure rates (taken from generic databases) and human errors assumed in the design PRA and incorporate them, as appropriate, into the quality assurance and maintenance rule programs. This is COL Action Item 19.1.1.1-2.

19.1.1.2 Evaluation of PRA Quality and Closure of Open Issues

In reviewing the AP1000 PRA, the staff relied 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 staff completed its review of the quality and completeness of the AP1000 PRA. These attributes are essential in using the PRA to gain insights about the robustness of the design and its tolerance of severe accidents, and in providing 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 reviewed the quality of the AP1000 PRA by evaluating the applicant's use of models, techniques, methodologies, assumptions, data, and calculational tools. In addition, the staff checked the AP1000 PRA for completeness by engaging in the following activities:

- comparing the AP1000 PRA 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 the AP1000 design or 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 included the issuance of requests for additional information (RAIs) to the applicant, followed by the evaluation of the applicant's responses to the RAIs. The staff used reported PRA results, as well as results of sensitivity,

uncertainty, and importance analyses, to focus its review. The use of PRA experience in the design certification process also achieves a sharper focus. The staff used applicable insights from previous PRA studies about key parameters and design features controlling risk in its review of the AP1000.

The staff 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. 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 a frequency high enough to impact results, but 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. The applicant considered T-H uncertainties and their impact on PRA models in the certification of the AP1000 design using the same approach used in the AP600 design certification. Section 19.1.10 of this report includes the staff's evaluation of the approach and associated analyses performed by the applicant to address the issue of T-H uncertainties and its impact on the PRA success criteria.

Although the AP1000 PRA review has been a continuous process, it involved two distinct stages. The first stage of the review ended with the issuance of a draft safety evaluation report (DSER). The DSER identified the following three classes of items which the staff believes needed additional attention by the applicant:

(1) open items (i.e., areas in which the staff disagrees with the submittal or requires additional supporting documentation)

(2) confirmatory items (i.e., areas in which resolution of previously open items has been reached but has not been incorporated into the PRA and/or the AP1000 Design Control Document (DCD))

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

The second stage of the review involved 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 involved close interaction between the staff and the applicant and required the applicant's response to additional RAIs. Section 19.1.10 of this report provides a summary of DSER open items and the associated resolutions.

The NRC staff concludes that the quality and completeness of the AP1000 PRA are adequate for its intended purposes, and that the PRA satisfies the requirements of 50.47 such as supporting the design certification processes. The applicant's approaches 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. All open items reported in the DSER were resolved satisfactorily.

Section 19.1.2 of this report briefly presents the special advanced design features that were incorporated into the AP1000 design for the purpose of preventing and mitigating accidents. Section 19.1.3 of this report provides safety insights about the AP1000 design drawn from the internal events risk analysis for operation at power. Section 19.1.4 of this report discusses safety insights about the AP1000 design drawn from the internal events risk analysis for low-power and shutdown operation. Section 19.1.5 of this report presents safety insights drawn from the external events risk analysis (e.g., seismic, internal fires and internal floods) for both at-power and shutdown operation. Section 19.1.6 of this report discusses representative examples of how the applicant used PRA in the design process. Section 19.1.7 of this report summarizes and evaluates the PRA input to the RTNSS process. Section 19.1.8 of this report documents the PRA input, derived from PRA insights and assumptions, to the design certification process. Finally, Section 19.1.9 of this report summarizes the staff's major conclusions and findings about the design consistent with the objectives of the PRA and its use in the design and certification processes.

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 the PRAs of operating reactors 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, thus reducing 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
- prevent severe accidents (core damage)

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

19.1.2.1 Special Advanced Design Features for Preventing Core Damage

The major features incorporated into the AP1000 design for the purpose of limiting plant transients and preventing severe accidents are discussed in the following sections.

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). 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 ac power for operation (to open) or for control, and no support systems are needed after actuation. This reduces significantly the risk contribution from loss of offsite power (LOOP) and SBO events, as compared to operating nuclear power plants. In addition, because of the passive systems, the AP1000 design eliminates several important contributions to risk for operating nuclear power plants. 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 the reliance on operator actions to mitigate accidents, as compared to operating reactor designs. To fairly compare the AP1000 design to operating and evolutionary reactor designs, using mostly active safety-related systems, the potential impact of T-H uncertainties on the performance of passive systems must be considered and appropriately included in the PRA models. The applicant's analyses concluded that the AP1000 design is robust with respect to T-H uncertainties. Section 19.1.10 of this report includes a discussion of the staff's review of this issue.

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 a challenge to the passive residual heat removal heat exchanger (PRHR HX) 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 which 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 (ESFs) which is diverse from the safety-related protection and safety monitoring system (PMS).

19.1.2.1.3 In-Containment Refueling Water Storage Tank

The important characteristics and functions of the IRWST include the following:

- possess a large capacity
- acts as a heat sink for the PRHR system

- provides water for low-pressure emergency core cooling (IRWST injection and RNS injection) after reactor coolant system (RCS) depressurization

- serves as the heat sink for the first three stages of the automatic depressurization system (ADS)

- 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 HX, it allows reliable core cooling at high RCS pressures when cooling through the steam generators (SGs) fails during anticipated transients and SGTR events (i.e., the IRWST 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 DHR systems provide defense-in-depth during all possible scenarios of an accident. The following represent alternate means of core cooling:

- main feedwater (MFW) and condensate

- startup feedwater

- automatically actuated (with manual actuation backup capability) PRHR

- automatic, with manual backup, feed-and-bleed capability using systems with adequate redundancy and defense against common-cause failures (CCFs) throughout the RCS depressurization range for both the feed function (two core makeup tanks (CMTs), two accumulators, the two RNS pumps, and the two IRWST 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)

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. The 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 fourth stage) and defense against CCFs (motor-operated valves (MOVs) in the first three stages and explosive valves in the fourth 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 IRWST gravity injection lines), as well as by non-safety-related defense-in-depth systems (the two chemical and volume control pumps and the two RNS 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 achieved either by gravity (through the safety-related IRWST injection lines) or pumping (through the non-safety-related RNS) 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 (RCPs). 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. The use of canned-motor RCPs in the AP1000 design eliminates the RCP seal LOCA (an important contributor to risk for operating nuclear power plants).

19.1.2.1.10 Improved Control Room Design and Digital Instrumentation and Control Systems

The AP1000 control room is an advanced design that is expected to provide more useful information to the operator than currently operating reactor designs. The AP1000 control room is still being designed (see Section 7.1.4 of this report). For this reason, the PRA took no credit 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 MFW, thus reducing the likelihood of a challenge to 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 ATWS event.

19.1.2.1.12 Physical Separation of Safety System Redundant Trains

The AP1000 design provides physical separation of safety systems or trains of systems that perform redundant safety-related functions. This increases the availability of systems because of their protection from failures associated with internal fires, internal floods, and similar CCFs. Except for support systems, such as Class 1E 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 design feature 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 125-V dc Class 1E vital I&C 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 I&C loads, which are associated with safety systems that may be required following the loss of ac power concurrent with a DBA, 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 AP1000 PRA and/or supporting deterministic analyses model the impact of these features on severe accident mitigation and containment performance. The staff provides its evaluation of these models and analyses in Sections 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, for core damage events in which early depressurization is not successful, late actuation of the ADS (i.e., 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 (i.e., direct containment heating (DCH), large hydrogen combustion events at vessel breach, ex-vessel steam explosions, and core-concrete interactions (CCIs)), thereby reducing the probability of early containment failure. The ADS also reduces the amount of fission products released to the containment atmosphere by

routing a portion of the discharge flow (from ADS Stages 1 through 3) through a sparger network in the IRWST. However, in many sequences, the RCS is vented to the containment airspace (via the fourth stage of the 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 SGTR events.

19.1.2.2.2 Large, Passively Cooled Steel Containment

The AP1000 design includes a large, passively cooled steel containment. The ratio of the containment building volume to reactor power for the 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 overpressure from noncondensable gas buildup. The containment pressure capacity is sufficiently large that the pressure loads associated with early challenges (e.g., hydrogen combustion and DCH) are at or below the applicant's Service Level C estimate (728.8 kPa (91 psig)) and pose an insignificant threat to containment integrity (i.e., a containment failure probability of less than 1 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 to prevent overpressure 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 because of its ability to condense steam and scrub fission products for release into the IRWST via Stages 1 through 3 of the ADS, as well as its ability to reduce the likelihood of reactor vessel failure and CCI by enabling reactor cavity flooding via gravity draining. The potential for hydrogen-rich mixtures to form in the vicinity of the IRWST (e.g., as a result of steam condensation as the hydrogen-steam blowdown passes through the IRWST) represents a unique containment challenge for the 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 a reactor vessel breach by molten core debris. By maintaining reactor vessel integrity, the potential for large releases caused by

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 which 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 AP1000 emergency response guideline (ERG) AFR.C-1 specifies the operator action to flood the cavity. It instructs the operator to flood the reactor cavity only 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 (as in the AP600) to the beginning of the procedure to achieve the higher water depths and earlier flooding times required to successfully cool the external reactor vessel of the AP1000. The following design features contribute to the effectiveness of ERVC in the 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

- refinements in the reactor vessel insulation system design (relative to the AP600) to increase the heat transfer capability (critical heat flux) from the reactor pressure vessel (RPV) to the surrounding water and to accommodate the higher decay heat level in the 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 can accommodate the loads associated with ex-vessel severe accident phenomena without early loss of containment integrity. These challenges include DCH, fuel-coolant interactions (FCIs), and CCI. The specific reactor cavity features that deal with each challenge are summarized below.

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

- the area around the reactor vessel flange
- the area where the coolant loops penetrate through the biological shield
- a ventilation shaft from the roof of the reactor coolant drain tank room leading to the SG 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 low that the corresponding probability of containment failure is negligible (less than 0.1 percent).

FCI: The deterministic evaluation of ex-vessel FCIs (see 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 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 RPV as a result of the impulse loading.

CCI: The AP1000 reactor cavity design incorporates features generally consistent with the Electric Power Research Institute's (EPRI) Utility Requirements Document (URD) guidance, including the following:

- a cavity floor area and sump curb that provide 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
- 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 Modular Accident Analysis Program (MAAP) codes indicate that in the event of unabated CCI, containment basemat penetration or containment overpressurization will not occur until after 2 days, regardless of concrete composition.

For a limestone basemat, which maximizes noncondensable gas generation and minimizes concrete ablation, basemat penetration would occur after about 3 days following the onset of core damage. Containment pressure will not reach the applicant's Service Level C estimate (728.8 kPa (91 psig)) until even later. Use of basaltic concrete, which maximizes concrete ablation and minimizes noncondensable 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 resulting from 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 to 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, “Investment Protection.” 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 the core exit temperature exceeds 648.9 °C (1200 °F). This action represents 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 nonessential diesel generators. In the event of an SBO, which represents less than 1 percent of the CDF, the system can be powered from the non-Class 1E batteries using dc-to-ac inverters. However, the PRA did not credit this feature. The AP1000 design also includes two non-safety-related passive autocatalytic recombiners (PARs) located within the containment. The PARs are provided for defense-in-depth protection against the buildup of hydrogen following a design-basis LOCA. Although the PARs are expected to function and reduce combustible gas concentrations during severe accidents, 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 Level 2 and Level 3 PRA do not credit the impact of the non-safety-grade containment spray system on containment response and fission product releases. Containment sprays could significantly reduce the estimated risk in the baseline PRA because 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 overpressurization of the 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, “Framework for AP1000 Severe Accident Management Guidance (SAMG),” issued January 15, 1998. The PRA does not credit the impact of the containment vent on containment response.

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

These insights include the following:

- dominant accident sequences contributing to CDF
- areas in which certain AP1000 design passive and defense-in-depth features were the most effective in reducing risk as compared to currently 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
- important insights and supporting sensitivity analyses from 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/yr. 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 are also shown for comparison. These estimates were taken from NUREG-1560, Volume 1, “Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance,” Part 1. The applicant estimated the total CDF of the AP1000 design, from internal events at power operation, 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, representing about an 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 events (less than 1 percent) are relatively small.

Section 19.1.3.1.1 of this report presents 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. Section 19.1.3.1.2 of this report describes the design features that contribute to the reduced CDFs, as compared to operating PWRs. Finally, Sections 19.1.3.1.3, 19.1.3.1.4, and 19.1.3.1.5 of this report discuss the insights drawn from the uncertainty analysis and the importance and sensitivity studies.

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/yr 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 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, the following risk-important failures appear in this sequence:

- plugging of the IRWST discharge line strainer in the intact line
- CCF of the two CVs in the intact IRWST discharge line
- 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 caused by 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, the following risk-important failures appear in this sequence:

- failure of any CV in the accumulator injection lines to open
- 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 this short timeframe. However, because of the failure of either CMT injection or 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 ESF input logic groups (causes CMT injection actuation failure which results in failure of automatic IRWST injection actuation with inadequate time for manual actuation)

- CCF of CMT-level sensors which prevents IRWST injection actuation

- CCF of CMT injection AOVs to open

- CCF of CMT injection CVs to open

- CCF of two 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 a 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 (0.952 cm to 5.08 cm (0.375 in. to 2 in.) 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). The following risk-important failures, in addition to the initiating event, appear in this sequence:

- 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)

- 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 (5.08 cm to 22.9 cm (2 in. to 9 in.) 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 those for Sequence #6.

Sequence #8, with a CDF of about 5E-9/yr and over 2 percent contribution, is initiated by a small LOCA event (0.952 cm to 5.08 cm (0.375 in. to 2 in.) 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 at which 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. The following risk-important failures, in addition to the initiating event, appear in this sequence:

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

Sequence #9, with a CDF of about 4.5E-9/yr and about 2 percent contribution, is initiated by a medium LOCA event (5.08 cm to 22.9 cm (2 in. to 9 in.) 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 at which injection by the RNS is possible), and by failure of the RNS to inject. High-pressure injection by the CMTs, 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 those 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 CVs, one in each of the two accumulator injection lines.

19.1.3.1.2 Risk-Important Design Features

Listed below are the 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 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, and instead 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 are 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 provide 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 (AFW) system, with at least one turbine-driven pump for SBO events, in addition to motor-driven pump(s)

  – a manual feed and bleed capability when onsite ac power is available

In contrast, 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 SFW system when onsite ac power is available

– the automatically actuated safety-related PRHR system

– an automatic, with manual backup feed-and-bleed capability using systems with adequate redundancy and defense against CCFs throughout the RCS depressurization range for both the feed function (two CMTs, two accumulators, the two RNS pumps, and the two IRWST 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 RCPs 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 (MFW and condensate, AFW, and manual feed-and-bleed). The AP1000 design provides better and more reliable defense-in-depth by relying on the following alternative means for core cooling:

  – MFW and condensate
  – SFW
  – automatically actuated (with manual actuation backup capability) PRHR
  – automatic, with manual backup, feed and bleed capability using systems with adequate redundancy and defense against CCFs throughout the RCS depressurization range for both the feed function (two CMTs, two accumulators, the two RNS pumps, and the two IRWST 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) significantly reduces 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.)

- The 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.

- The 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 (the chemical and volume control system (CVS) and the SFW system) and manual SG isolation

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

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

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

Severe Accidents

- Redundant means for reactor coolant inventory control:
  - automatic CVS injection at the upper end of the RCS pressure range
  - automatic CMT injection once an “S” signal is generated
  - 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 DHR 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 that 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 Loss-of-Coolant Accident 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 their chemical and volume control system (CVCS) pumps and HPSI pumps for high-pressure injection, while providing accumulators and low-pressure safety injection (LPSI) pumps for LPSI.

- 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 the automatic, with manual backup, feed-and-bleed capability of the AP1000 design).

- The ADS provides an alternate DHR 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 is significantly reduced and leak-before-break (LBB) objective was applied in the design of all piping larger than 7.62 cm (3 in.).

19.1.3.1.2.5 Anticipated Transient Without Scram 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 using the motor-generator (M-G) 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, and 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 also 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.

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

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 uncertainty analysis resulted in the following conclusions:

- 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 (e.g., 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 CCFs)
  - IRWST discharge line strainer plugging probability (both single and CCFs)
  - CCF probability of hardware in the PMS ESF input logic groups
  - CCF probabilities of several sensor groups, such as the 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)
  - failure probability of a M-G set circuit breaker (CB) to open by DAS (mechanical failure)

[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 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 CVs 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. Section 19.1.3.1.5 of this report discusses the insights from these studies, along with insights from other sensitivity studies.

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 identifying and ranking dominant contributors to risk to highlight 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 identifying dominant contributors to maintaining the built-in risk level to ensure that the risk does not increase and is as low as indicated by the PRA. To meet these objectives, the applicant used the following two risk importance measures to rank structures, systems, and components (SSCs) and human actions:

- Risk reduction worth 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). It also provides an indication of the existing margin for improvement.

- Risk achievement worth gives the factor by which the CDF increases when an SSC or human action is assumed to be absent or to be failed (event probability is assumed to be 1). It also provides an 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 because 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.

Severe Accidents

- Events that would decrease significantly the built-in reliability (i.e., those with the highest risk achievement worth) are hardware CCFs 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.

- CCF 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 the 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 CVs. 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 on demand because of a 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 strainers 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 CVs, and accumulator CVs. 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, and boric acid tank (BAT)), sensors in high-pressure environment, and pressurizer level sensors. If such components become unable to operate as designed on demand because of 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 on demand because of 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 (input/output), processing, and communications). Because such functions, and the associated software, are repeated across all major subsystems of the PMS and PLS, such software design errors could impact the reactor trip and ESF portions of the PMS, as well as all the PLS functions, failing 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 and 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 the 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
  – perform a controlled shutdown to control and mitigate an 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 HX

  – plugging or rupture of a flow-tuning orifice in an accumulator injection or CMT injection line

  – accumulator injection and CMT injection CVs

  – non-Class 1E dc distribution panel EDS3 EA 1 (supplies power to DAS which is important for ATWS sequences)

  - 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 CVs in the two IRWST discharge lines

  - CCF of the four explosive (squib) valves in the two IRWST discharge lines

  - failure of one CV 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 4.16-KV ac RCP trip breakers to open

  - 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 the DAS, given failure to do so through the PMS

  - manually actuate containment sump recirculation (when automatic actuation fails)

  - manually trip the reactor via the PMS or DAS within 1 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 these 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 the CDF is associated with transient and ATWS sequences.

- The DAS is very important in reducing the CDF associated with transient initiators (e.g., loss of MFW, 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 the 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, Chapter 50 of the AP1000 PRA, "Importance and Sensitivity Analysis," (for internal events at power operation) provides details on SSCs and human actions that the applicant found to be risk-significant. This information was integrated with similar information from external events and shutdown risk analyses, as well as information from the containment and offsite consequences analyses (Levels 2 and 3 of the PRA) to form the basis for the following two lists:

- A list of important SSCs which the applicant incorporated in the D-RAP program. The applicant included such a list of important SSCs in DCD Tier 2, Section 17.4. This was part of Open Item 19.1.10.1-2 (see Section 19.1.10.2 of this report). The COL applicant is responsible for incorporating these SSCs in the O-RAP. This is part of COL Action Item 17.5-2

- 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. The COL applicant should take this list into account in developing and implementing procedures, training, and other human-reliability-related programs. DCD Tier 2, Chapter 18, "Human Factors Engineering," discusses the use of such information in developing and implementing procedures, training, and other human-reliability-related programs for the plant. This is COL Action Item 19.1.3.1.4-1.

The applicant, in performing the Level 1 PRA for internal events at power operation, identified a number of risk-important tasks (with their PRA designators inside the parentheses) which must

be performed by the operator to prevent or mitigate severe accidents. The control room design should account for these tasks. Section 18.7 of this report addresses the process for inclusion of these tasks. The following is a list of these tasks:

- operator fails to manually actuate ADS (AND-MAN01)
- operator fails to manually trip reactor via PMS within 1 minute (ATW-MAN03)
- operator fails to manually trip reactor via DAS (ATW-MAN04C)
- operator fails to manually trip reactor via PMS within 5 minutes (ATW-MAN05)
- operator fails to diagnose an 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 because of IRWST-level signal failure (REN-MAN04)
- operator fails to perform controlled shutdown (OTH-SDMAN)

Sections 19.1.4.5 and 19.1.3.2 of this report, respectively, discuss additional risk-important operator tasks related to shutdown operation and to containment performance (Level 2 PRA).

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 human reliability analysis (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 19.1.3.1.4-2.

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. When necessary, the staff used the applicant's PRA results to perform additional sensitivity studies to gain more complete insights. 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 a 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

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

In addition, sensitivity studies were performed to investigate the impact of uncertainties on the PRA results assuming 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 within the RTNSS process. Insights related to the CDF are reported in this section, while similar insights related to the LRF 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

The 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 the uncertainties in extrapolating data from other designs and sizes to the AP1000 operating conditions, there is uncertainty in the mean value of the failure probability of a squib valve to operate. A sensitivity study, performed to assess the impact of this uncertainty on PRA results and insights, yielded the following results:

- By increasing the failure probability by a factor of 5 (i.e., the value recommended in EPRI's "Advanced Light Water Reactor Utility Requirements Document," Volume III, ALWR Passive Plant), the CDF would increase by less than a factor of 2.

- By increasing all CCF probabilities of squib valves by a factor of 10, the CDF would increase by about a factor of 3.

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. However, this sensitivity is not great 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 CBs the AP1000 PRA modeled 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 the 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, performed to assess the impact of this uncertainty on PRA results and insights, led to the following conclusions:

- By 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 relatively small sensitivity of the CDF to reasonable increases in the mean value of the failure probabilities of CBs to open on demand.

- By 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, the 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).

- By 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 the 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). Because 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 the DAS. This underscores the importance of the reactor trip function of the DAS in reducing the impact of uncertainties associated with CB failure probabilities on PRA conclusions and insights about the design (e.g., 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 into 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 that do not manifest themselves; 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. It is also 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 create 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 AP1000 design (such as redundancy, separation, operational testing, maintenance, and immediate detectability of failure provided by the online 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. Because 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:

(1) requirements for formalized design phases, for following design standards, and for performing formal design reviews

(2) requirement for an expected use-based software testing and verification program

(3) 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)

(4) 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 the 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:

- By increasing software failure probability by an order of magnitude, the CDF would increase by about 20 percent (from 2.4E-7/yr to about 3.0E-7/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.

- By 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-7/yr to almost 1E-4/yr). (Based on risk importance study results, the 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 non-safety-related SSCs for regulatory oversight according to the RTNSS process).

- By 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 the DAS, become unavailable and the plant continues operating at power, the plant CDF would increase by almost one order of magnitude (from 2.4E-7/yr to about 2E-6/yr). Because 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 relatively insensitive 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 the DAS. This underscores the importance of the ESF actuation function of the DAS in reducing the impact of uncertainties associated with software failure probabilities on PRA conclusions and insights about the design (e.g., 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

The results of sensitivity studies performed to determine the impact of a 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 the contributions of spurious ADS valve actuation, caused by faults in the 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, underscored the importance of incorporating features in the design of the ADS cabling to minimize the probability of hot shorts actuating an ADS squib valve. The applicant responded by incorporating additional features in the AP1000 design to 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 the adequacy of long-term containment cooling by airflow for some accidents. Late containment failure, and consequent loss of core cooling, cannot be ruled out for sequences involving the release of steam inside the containment and the unavailability of the water cooling mode of the PCS. The sensitivity study 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. A similar conclusion was reached for the focused PRA (i.e., when no credit is taken for non-safety-related defense-in-depth systems).

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:

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

(2) 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 shows that the impact of this issue on the estimated CDF is rather small (i.e., 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 indicates that this issue does not have a significant impact on PRA conclusions and insights about the design. Furthermore, the applicant addresses these concerns through the development of ERGs for long-term operator actions.

19.1.3.1.5.3 Sensitivity to Previously Raised Issues

The 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, EPRI has recommended increasing the standby failure rate of CVs in passive systems by a factor of five as compared to the CVs used in the pumped systems of in operating reactor designs (“Advanced Light Water Reactor Utility Requirements Document,” Volume III, ALWR Passive Plant). The applicant, however, did not use the higher failure rate recommended by EPRI in the AP1000 PRA. The applicant believes this decision is justified because the CVs used in the IRWST injection lines, which are the most risk-important CVs 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, making 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 demonstrate the degree to which 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 resulting from the lack of data to support the reliability of these CVs, as assumed by the applicant 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 CVs, assumed in the AP1000 PRA, are based on information provided in Revision 6 of the EPRI URD. The information on CCF of CVs, as revised in the last revision of the EPRI URD, leads to a decrease by about an order of magnitude in the value of the CCF probability recommended in previous URD revisions and used in previous PRAs for evolutionary designs and operating reactors. According to the applicant, this results from a better understanding of individual events involving failure of CVs at nuclear power plants and that "EPRI found no common-cause failures to open of CVs (other than failure modes unique to testable check valves)." An NRC-sponsored evaluation of licensee event report (LER) and Nuclear Plant Reliability Data System (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, found about 20 events involving CCF of CVs. Although it can be argued that only a portion of such events are applicable to the AP1000 design, the staff believes that significant uncertainty still exists 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, to assess 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) increases the CDF by about a factor of 5 (from 2.4E-7/yr to about 1E-6/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, increases the plant CDF almost two orders of magnitude (from 2.4E-7/yr to about 2E-5/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 the DAS become unavailable and the plant continues operating at power, increases the plant CDF about 10 times (from 2.4E-7/yr to about 3E-6/yr). If, in addition to the above changes, the explosive valve failure rate is also increased by a factor of 10 (as explained in the above mentioned study), the CDF would increase about 15 times (from 2.4E-7/yr to about 3.5E-6/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 the DAS and the RNS become unavailable and the plant continues operating at power, increases the plant CDF by almost one order of magnitude (from 2.4E-7/yr to almost 2E-6/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 5. This indicates that the availability of the RNS significantly reduces the impact of uncertainties associated with the failure probabilities of CVs and explosive (squib) valves on PRA conclusions and insights about the design (e.g., the selection of non-safety-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 the Westinghouse PRA models and results, indicates 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-Break LOCAs

The applicant performed a sensitivity study to address staff concerns regarding 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 the 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. The use of experience data resulted in a large-break LOCA frequency of about 5E-6/yr as opposed to about 5E-5/yr which was used in the AP600 PRA. The major findings of this study are summarized below.

- When the large-break LOCA frequency is increased by a factor of 10 (from 5E-6/yr to 5E-5/yr, as in the AP600 PRA), the plant CDF increases by almost a factor of 3 (from 2.4E-7/yr to about 6.4E-7/yr).

- When the large-break LOCA frequency is increased by a factor of 10 (from 5E-6/yr to 5E-5/yr, as in the AP600 PRA), and at the same time the conservatism in the success criteria for hot-leg breaks is removed, the plant CDF increases by about 80 percent (from 2.4E-7/yr to about 4.4E-7/yr). The conservatism in the success criteria arises from the assumption in the PRA that makeup from both accumulators is required following a large-break LOCA. However, thermal-hydraulic analyses have shown that makeup from one accumulator is adequate if the break is in the hot-leg.

- When the large-break LOCA frequency for the hot-leg pipes is increased by a factor of 10 (the large-break LOCA frequency for the cold-leg pipes is not changed), and at the same time the conservatism in the success criteria for hot-leg breaks is removed, the plant CDF decreases by about 3 percent (from 2.4E-7/yr to about 2.3E-7/yr). The rationale for keeping the large-break LOCA frequency for the cold-leg pipes unchanged

is that no special failure mechanisms have been identified for cold-leg pipes, such as primary water stress-corrosion cracking (PWSCC), and random pipe failures are universally considered to be of very low frequency. PWSCC events are associated with hotter RCS locations and with a specific type of material which is not used in the AP1000.

This sensitivity study indicates that the large-break LOCA frequency assumed in the AP1000 PRA does not affect PRA conclusions and insights about the design.

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 underscores the importance of those design features and operational requirements which aim to prevent CCFs, for example, divisional separation and 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 CBs, could have a significant impact on PRA conclusions and insights about the design (e.g., the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process). The availability control of the reactor trip function of the 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., the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process). The availability control of the ESF actuation function of the 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 CVs and explosive (squib) valves could have a significant impact on PRA conclusions and insights about the design (e.g., the selection of non-safety-related SSCs for regulatory oversight according to the RTNSS process). The 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 the 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)

The sections that follow present results and insights from the Level 2 portion of the PRA. These sections address 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. Table 19.1-2 of this report provides the definition of each accident class, 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 1.14 MPa (150 psig)) at the time of core uncovery. For high-pressure core melt sequences, the Level 2 event tree further evaluates the potential to depressurize the RCS in the time period between the onset of core damage and the challenge of the RCS pressure boundary. 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 the 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 (RCs). 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 RCs. Table 19.1-3 of this report presents the conditional containment failure frequency for each accident Class for the baseline PRA for internal events at power. The CCFP for accident classes 1A, 1AP, 3A, and 6 (40 to 92 percent) is considerably higher than for other classes because of the failure of late depressurization in these sequences, which leads directly to containment bypass. The CCFP for accident classes 3BL and 3BR is lower than for 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.

Figure 19.1-1 and Table 19.1-4 of this report present the frequencies of the various containment release categories and the fractional contributions by release category to the total LRF. Section 19.1.3.2.2 of this report further discusses the leading contributors to the various RCs.

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. The updated PRA does not treat basemat melt-through as a separate failure mode. Instead, all events that lead to reactor vessel melt-through are considered to result in early containment failure, as discussed below.

Figure 19.1-2 of this report identifies the important contributors to each of these RCs, which are 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-8/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 because 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 overpressure 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 Level 2 PRA analysis evaluates the potential for RCS depressurization. Depressurization is credited in sequences in which the following occurs:

- PRHR is successful and the ADS fails by operator error initially, but is successfully recovered before extensive core damage
- PRHR and the 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 because of low RCS pressure and high water level in the faulted SG.

Therefore, they 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 the 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. This is part of COL Action Item 19.2.5-1.

In previous PRAs, ISLOCA 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 the AP1000 (5E-11/yr). As such, the contribution of ISLOCA sequences to the CDF and risk is negligible.

The PRA characterizes the containment bypass release category by an SGTR case with coincident rupture of five SG tubes, a stuck-open secondary system relief valve, and failure of the ADS (Case 6E-1). 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 AP1000 PRA credits no additional decontamination for the SGTR 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-9/yr, 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 involving failure of reactor cavity flooding and subsequent reactor vessel failure. An additional 13 percent is attributed to spontaneous RPV failure events (3C) in which the vessel is not able to be reflooded to prevent debris relocation. The major causes of cavity flooding failure are listed below:

- operator failure to open the recirculation valves to flood the reactor cavity
- CCF of low-pressure recirculation squib valves to open
- CCF of strainers in IRWST tank
- CCF of actuation software and hardware

CFE is assumed to occur as a result of ex-vessel phenomena associated with debris relocation into the reactor cavity during 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 CFE. 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 ERVC features in the AP1000 design
- the large uncertainties associated with ex-vessel debris spreading and FCI

Deterministic calculations performed by the applicant and documented in DCD Tier 2, Appendix 19B, "Ex-Vessel Severe Accident Phenomena," indicate that containment integrity would be maintained despite localized structural failures predicted for an ex-vessel FCI (i.e., the interaction of molten fuel with residual breakflow expected to be present in the cavity with failure of reactor cavity flooding) and CCI. 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 end states. This assumption dominates the probability of CFE in the AP1000 PRA.

CFE as a result of hydrogen combustion accounts 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 the 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 include the following:

- CCF of igniters
- failure of the 12 V distribution panel
- operator failure to actuate the hydrogen control system
- CCF of hydrogen analyzer sensors

The actual frequency of CFE from hydrogen combustion is small because of the high reliability of the hydrogen igniter system, the small fraction of core damage sequences involving SBO sequences in the AP1000 design, and the addition of the IRWST louvered-vents.

The applicant evaluated the potential for CFE 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 CFE 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 CFE in the CET. (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 CFE, as discussed above.)

The AP1000 includes a non-safety-grade containment spray system, but its impact on containment response is not reflected in Levels 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. The staff also asked the applicant 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 the 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 CFE 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 Risk Oriented Accident Analysis Methodology (ROAAM), and judged to be physically unreasonable. This analysis and conclusion has been extended to the AP1000 (see Section 19.2.3.3.5.1 of this report). Even if the mean values found in NUREG-1150, Volume 1, "Severe Accident Risk: An Assessment of Five U.S. Nuclear Power Plants," were used to quantify the CCFP from this containment failure mode, the absolute value of containment failure frequency, as a result of an alpha mode failure, would be very small. Reactor vessel displacements associated with postulated ex-vessel steam explosions were also considered and determined not to affect the integrity of the containment and associated equipment. The AP1000 containment layout and the inclusion of a protective layer of concrete in the reactor cavity precludes the possibility of corium impingement on the containment shell, 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 2 valves with failure of IRWST injection, successful cavity flooding and in-vessel retention, and successful operation of the hydrogen igniters (Case 3D-4). A diffusion flame is assumed to occur at the IRWST vents near the containment shell and result in CFE.

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 timeframe. Sequences with containment overpressurization due to failure of both the PCS and containment venting also contribute, but this contribution is negligible. The total frequency of CFI in the baseline PRA is 1.9E-10/yr, or about 1 percent of the containment failure frequency.

Within the CET, global hydrogen deflagrations are modeled as a potential contributor to CFI for events in which the 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 preburn containment pressure) with the CCFP 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 CFE, as discussed above.)

The CFI release category is represented in the PRA by a direct vessel injection (DVI) line break in the passive core cooling system (PXS) compartment with failure of IRWST injection; successful cavity flooding, reactor vessel reflood, and in-vessel retention; and failure of the hydrogen igniters (Case CFI). 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 during the intermediate timeframe (after reflood) in the CMT room, 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)

The AP1000 PRA defines CFL as a failure occurring later than 24 hours after the onset of core damage. All contributors to CFL involve failure of the PCS and containment failure as a result of late overpressurization. The total frequency of CFL in the baseline PRA is about 3E-13/yr, or less than 0.1 percent of the containment failure frequency.

Unlike the AP600, in which air cooling of the containment alone is sufficient to maintain containment pressure less than Service Level C (728.8 kPa (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 the 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 because of the high reliability of PCS water delivery. The reliability of PCS water delivery in the AP1000 has been improved over the AP600 by the addition of a third, parallel water supply line for PCS, controlled by a diverse valve (an 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 PCS failure in the AP600 PRA was dominated by blockage of the PCS annulus drainlines. This failure mechanism is not modeled in the AP1000 PRA. The staff identified the omission of this failure mechanism as Open Item 19.1.3.2-2 in the DSER.

In response, the applicant noted that the treatment of PCS drain blockage as a containment failure mechanism in the AP600 was conservative, and this phenomenon was dropped as a

containment failure mechanism in the AP1000 because it would not realistically be expected to result in containment failure. Specifically, by definition of the drain failure case, PCS water flow over the containment shell is guaranteed. The cooling of the containment shell with water, even without airflow through the annulus, would remove sufficient heat from the shell to prevent containment failure. Although the water film temperature and containment pressure would be higher if there is no airflow, the containment pressure is not expected to exceed Service Level C. The staff concurs with this rationale and further notes that inclusion of this failure mode at the same failure probability used in the AP600 PRA would increase the containment failure frequency by about 2E-11/yr; the frequency of CFL would remain less than 0.1 percent of the total containment failure frequency. Therefore, Open Item 19.1.3.2-2 is resolved.

Although not a key failure mode, the availability of the PCS annulus drains will be confirmed every 2 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 overpressurization failure from noncondensable gas generation, or late hydrogen burn
- containment overtemperature failure (other than diffusion flames)

Sequences that proceed to RPV failure could lead to basemat melt-through or overpressurization from noncondensable 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 timeframes. Hydrogen combustion was therefore not modeled as contributing to CFL. Late containment overtemperature failure would be a viable threat only if the reactor cavity was dry and the containment heat removal was lost. Such events are of low frequency, given the high probability of a flooded reactor cavity and the high reliability and independent nature of the PCS in the AP1000 design. In addition, they are conservatively assumed to lead to CFE in the PRA. The overtemperature challenge would be further reduced by use of the non-safety containment sprays.

The PRA represents the CFL release category by a medium (5.1 cm (2 in.)) hot-leg break in the SG loop compartment with failure of IRWST injection, successful cavity flooding and in-vessel retention, and failure of PCS cooling water (Case CFL). Containment failure was assumed to occur from long-term containment over-pressure at 728.8 kPa (91 psig).

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 whose failure would result in a failure

of the containment isolation function, as well as 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 steamlines and feedwater lines
- SFW lines
- SG blowdown lines

Failure of SG isolation following an 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 1.3E-9/yr, or about 7 percent of the containment failure frequency. The probability of a preexisting opening in containment large enough to constitute an isolation failure (1.2E-04) is included in the Level 1 fault tree model for a LOCA, but was omitted in the containment isolation fault trees. This was Open Item 19.1.3.2-1 in the DSER.

In response, the applicant provided an assessment of the impact on results, if this failure mode were included in the model. This assessment, which is documented in Attachment 43D to the PRA, indicates that the CI release category frequency would increase by only about 7 percent (from 1.3E-9/yr to 1.4E-9/yr), and that the impact on the LRF would be insignificant. Therefore, Open Item 19.1.3.2-1 is resolved.

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 the hydrogen igniters (Case 3C-2). The CI is represented in the PRA by a failure to close the largest containment penetration, an 45.7 cm (18 in.) diameter purgeline, 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.

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

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 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, including the following:

- depressurization of the RCS to below 1.14 MPa (150 psig) 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 these criteria.

Sufficient depressurization (as the result of successful operation of Stages 1–3 of the ADS or large LOCA breakflow) 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-8/yr to 1.6E-7/yr, and the CCFP would increase from 8.1 to 66 percent. CCF of IRWST discharge line strainers is a dominant contributor to failure of reactor cavity flooding and CFE in the PRA. IRWST strainer plugging will be controlled by inclusion in the 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, thereby substantially enhancing 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 the cavity flooding system

function to mitigate the effect of additional hydrogen produced by reflood and retain the core debris in-vessel, in the majority of sequences.

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 LRF and CCFP. 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 overpressurization 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 because all events that lead to reactor vessel breach are assumed to result in CFE from other mechanisms. However, the staff expects the risk contribution from CCI to be small, because the consequences associated with basemat melt-through or late containment overpressure 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 overpressure 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, because 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 24 hours). The remainder (2 percent) are considered CFIs (prior 24 hours). The actual frequency of CFL is quite small because of the high reliability of PCS water delivery. The reliability of PCS water delivery in the AP1000 has been improved over the AP600 by the addition of a third, parallel water supply line for the PCS, controlled by a diverse valve (an 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. Inclusion of this failure mode would increase the frequency of CFL 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, the availability of the PCS annulus drains will be confirmed every 2 years in accordance with the TS.

A subset of the containment isolation valves (CIVs) are important in limiting offsite releases during core melt accidents, and are therefore actuated by the DAS in addition to the PMS.

These valves include the isolation valves in the containment purge supply and exhaust lines, and the normal containment sump line. The PRA assumes that the 45.7 cm (18 in.) containment purge supply and exhaust valves will be open 12 percent of the time during normal operation 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 LOOP 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 the 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 because containment overpressurization 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 the 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, overpressure failure of containment in events involving failure of the PCS or unmitigated CCI. However, the vent is not needed to meet the Commission's containment performance goals or quantitative health objectives. Venting is not credited in the PRA, and would not significantly impact the estimated containment failure frequency, because containment overpressurization is not a dominant failure mode in the PRA. Section 19.2.3.3.8 of this report further discusses the venting capabilities of the AP1000.

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. The PRA assumes that 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) always result in thermally induced SGTR. The PRA assumes that events with failure of cavity flooding (which could lead to CFE by ex-vessel FCI, CFL by basemat melt-through, or no containment failure) always result in CFE. In contrast, deterministic analyses indicate that DCH and ex-vessel FCI will not result in CFE, and that CCI will not lead to containment overpressure or basemat penetration until after 2 days. Accordingly, the containment failure frequency and dominant contributors could be substantially different than those reported in the PRA, if a more realistic, less conservative

treatment of these issues were performed. However, the risk would remain low, as discussed in the following paragraphs.

Eliminating credit for ERVC would increase the CCFP, but the LRF 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 applicant's 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 because all RPV breaches are assumed to lead to CFE 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-6/yr 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 the 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 ADS Stage 4. 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, as described below:

- 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.

- IRWST vents near the containment wall are equipped with louvers that are normally closed. These louvers are 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.

This latter feature was added to the AP1000 design to reduce the potential for diffusion flames at the containment shell and is safety-related. Operation of the IRWST louvered vents will preferentially direct the hydrogen releases to the IRWST pipe vents (located along the SG doghouse wall), where diffusion flames would not adversely impact the containment. Failure of the louvered vents to reclose is assumed to result in CFE because of the presence of diffusion flames, and accounts for about 5 percent of the containment failure frequency for the 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-8/yr to 2.3E-8/yr). If the system is assumed to be unavailable in all sequences, the containment failure frequency increases from 1.9E-8/yr to 6.3E-8/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 certain operator actions in the Level 2 analysis as important to LRF, based on sensitivity/importance analyses. The following risk-important actions will be taken into account in the 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 nonessential diesel generators or the non-Class 1E batteries. The COL applicant will develop detailed procedures for these latter actions 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 an SGTR accident. In approximately half of the Level 1 SGTR sequences, late RCS depressurization was successful. The PRA does not consider those SGTR sequences with successful late depressurization to result in containment bypass because of low RCS pressure and high water level in the faulted SG. Instead, these events are further evaluated in the CET, where they generally result in an IC and a benign source term. Eliminating credit for late depressurization during SGTR events increases the frequency of containment failure from 1.9E-8/yr to 2.9E-8/yr, and the CCFP from 8.1 to 12 percent. The assumptions 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 COL applicant's severe accident management guidance, as discussed in Section 19.2.5 of this report. This is part of COL Action Item 19.2.5-1.

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:

(1) Failure may result from the 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 LRF used by the applicant.

(2) Failure may result in releases leading to whole body doses of 0.25 Sv (25 rem) or greater at 0.80 km (0.5 mile) 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 mile) 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., they yield approximately the same containment failure frequency) because the conditional probability of exceeding 0.25 Sv (25 rem) at the boundary is close to unity for all release categories (except IC). Discussions below are based on the containment integrity definition of containment failure.

The containment failure frequency for internal events is 1.9E-8/yr in the baseline PRA and 4.3E-7/yr in the focused PRA. The corresponding CCFP is approximately 8.1 percent in the baseline PRA and 20 percent in the focused PRA. If credit is taken for availability controls on the automatic portion of the DAS and on the RNS (as discussed in Section 19.1.3.1.5 of this report), the staff estimates that the focused PRA CCFP would be about 10 to 15 percent. The PRA analysis includes the following major features:

- stand-alone assessments of ERVC and in-vessel steam explosions using 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 CFE or containment bypass. This is an artifact of the following two major simplifying assumptions in the Level 2 PRA:

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

(2) all accidents in which ERVC 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 severe accident phenomena.

Sensitivity studies reported in Chapter 43 of the AP1000 PRA, "Release Frequency Quantification," 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-7/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 because the bulk of the containment failures in the existing analyses are driven by the frequency of events leading to 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, as well as the focused PRA, is well below the general plant performance guideline of 1E-6/yr for a large release of radioactive material, as proposed in the NRC Safety Goal Policy Statement. The CCFP is less than the CCFP goal of 0.1 in the baseline PRA. 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 the CCFP goal is exceeded in several sensitivity cases, these increases are modest, and the corresponding containment failure frequencies remain well below 1E-6/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 LRF and CCFP.

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

In the updated AP1000 PRA, the endstates of the CETs were grouped into six 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 0.80 km (0.5 mile) from the reactor site, and the total person-rem exposure over a 80.4 km (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 are, therefore, acceptable.

The following sections present the results and insights from the Level 3 portion of the PRA. This includes the estimated probability of exceeding selected dose criteria, a breakdown of the total risk in terms of important release classes, and 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-8/yr for internal events. This value is about a factor of 50 lower than the Commission's LRF goal of 1E-6/yr and is, therefore, acceptable. The design also meets the public safety requirement goal established by EPRI in the ALWR URD (1E-6 probability of exceeding a dose of 0.25 Sv (25 rem) at a distance of 0.8 km (0.5 mile)). 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 0.05 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 (see 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 (1) a very low estimated CDF for AP1000, (2) a low CCFP, 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

Table 19.1-5 and Figure 19.1-3 of this report present the contribution to risk from each of the release categories. The following observations 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 mile)) is essentially flat and close to unity for all release

categories except 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. Intermediate and late containment failures also have a negligible contribution to risk because of the very low frequency of these events in the PRA.

- CFE contributes 38 percent of the containment failure frequency and accounts for 13 percent of the risk.

- Containment bypass events (BP) contribute 54 percent of the containment failure frequency and account for 81 percent of the risk. This large contribution to risk is the result of the relatively large consequences (about 4E6 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 5 percent of the total risk.

Selection of different representative sequences for the various release categories could alter the consequences by perhaps a factor of 3 and result in a reranking 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-8/yr, and is equivalent to the containment failure frequency (CDF less the frequency of events with IC). The release frequency is a factor of 50 lower than the Commission's LRF 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 LRF 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 (1) conservative assumptions regarding CFE from ex-vessel phenomena, and (2) optimistic assumptions that ERVC will always prevent RPV breach. The impact of these assumptions on risk results is described below.

In the baseline PRA, risk is dominated by events in which CFE 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 CFE is avoided, RPV breach may instead result in a delayed release (e.g., a containment failure in the intermediate time-frame). However, overall risk for internal events would not be substantially impacted because the population doses associated with early and intermediate containment failures are not substantially different.

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 because all RPV breaches are assumed to lead to CFE in the baseline PRA. Under the most limiting assumption that ERVC always fails and leads to CFE, the containment failure frequency would approach the core melt frequency, and risk would increase by about a factor of 4 (to about 0.2 person-rem/yr). Even then, however, the containment failure/LRF would remain below the Commission's LRF goal of 1E-6/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 PRA did not credit the impact of the containment spray system on fission product releases. Containment sprays would reduce the estimated risk in the baseline PRA because the sprays would be effective in reducing the source terms in the early containment failure and containment isolation failure release categories (i.e., CFE and CI). However, these release categories are insignificant contributors to risk because of their small frequencies.

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

- ISLOCAs 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 presented in Sections 19.1.4.1 through 19.1.4.5 of this report, while Section 19.1.5 of this report discusses 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, "Low Power and Shutdown Risk Assessment." The AP600 shutdown PRA, particularly the analyses contained in the Attachment 54B and Attachment 54C, provides the basis for the AP1000 shutdown PRA. Attachment 54B is a requantification of the shutdown PRA results using revised success criteria for injection and recirculation during reduced inventory conditions with loss of the RHR function. The revised success criteria state that (1) at least one of the four ADS Stage 4 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-7/yr (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 fourth stage ADS valves, and the containment sump recirculation trains, even though such outages are allowed by the AP1000 TS. The AP1000 internal shutdown CDF estimate can increase to 2E-6/yr if a COL applicant were to always choose minimal compliance with the AP1000 TS. Section 19.1.4.5 discusses these insights in more detail.

The reported CDF from internal events during shutdown operation (1.2E-7/yr) covers two plant operational states:

(1) safe shutdown/cold shutdown with the RCS filled and intact

(2) midloop/vessel flange operations with the RCS vented and drained

Midloop/vessel flange operations include draining to midloop, drained maintenance, and post-refueling maintenance.

Vacuum refill of the RCS from drained conditions (midloop) was mentioned in the PRA; however, no risk assessment was performed for this configuration. Vacuum refill of the RCS helps to reduce noncondensable gas pockets in the RCS, eliminating the need for dynamic venting of the RCS and the multiple RCP start and stop operations that it requires.

The applicant stated that the shutdown risk associated with vacuum refill operations is included in the calculation of shutdown risk during vented drained conditions. The applicant also stated that vacuum refill operations do not pose additional risk in the AP600 for the following reasons:

- The decay heat during vacuum refill will be about 50 percent of that during drained conditions before refueling, which is already considered in the shutdown PRA.

- Although ADS Stages 1, 2, and 3 will be closed, the TS requires 9 out of the 10 ADS paths to be open. As a result, at least three out of four ADS Stage 4 valves will be

operable, instead of the two out of four that are operable during RCS-drained conditions with an open RCS.

- During vacuum refill operations, both RNS pumps and support system are required to be available by the short-term availability controls. As discussed in the bases for the short-term availability controls (DCD Tier 2, Table 16.3-2), the RCS is considered open if there is no visible level in the pressurizer.

- The AP1000 Emergency Response Guidelines (ERG-SDG-2, Step 6) provide direction for the operators in the event of a loss of RNS during shutdown conditions, and the ERG response is applicable during vacuum refill operations in Mode 5. For a loss of RNS during vacuum refill operations, the operators are immediately directed to open the ADS Stage 1, 2, and 3 valves.

- The RNS provides the low-temperature, overpressure protection for the plant during Mode 5 conditions (including vacuum refill operations), in accordance with TS 3.4.14. The applicant responded that the operators will be trained on brittle fracture prevention and the RCS pressure-temperature limits. The applicant added that the operators will thoroughly understand their priority to maintain the RCS overpressure protection flowpath to the RNS during low-pressure, low-temperature shutdown conditions. The applicant addressed the importance of the operators not isolating the RNS unless the hot-legs are empty as a PRA insight (DCD Tier 2, Table 19.59-18, insight 82).

- In the event that a leak develops through the RNS system, the RNS pumps would be stopped, and the lines would be isolated. In this situation, the ERGs require the ADS Stage 1, 2, and 3 valves to be opened.

The staff accepts the applicant's argument for not explicitly evaluating vacuum refill operations.

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 90 percent of the 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. Because the safety-related systems (except for the accumulators below 6.97 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 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. Section 19.1.4.3 of this report describes the AP1000 design features that reduce the AP1000 shutdown risk as compared to those of

operating PWRs. Sections 19.1.4.4 and 19.1.4.5 of this report discuss insights drawn from the importance and sensitivity studies.

19.1.4.2 Dominant Accident Sequences Leading to Core Damage

As discussed above, over 90 percent of the 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 the ADS), and the RCS is drained to reach midloop conditions so that nozzle dams can be installed in the hot- and cold-legs to perform SG maintenance. When the RCS boundary is open, emergency core cooling using the PRHR is not viable; therefore, gravity injection from the IRWST and fourth stage ADS actuation must be initiated. Given that the fourth stage ADS must open during reduced inventory conditions following an extended loss of the RNS, containment sump recirculation would be initiated within 72 hours following accident initiation.

As shown in Table 54-4 in the AP1000 PRA, approximately 68 percent of the core damage sequences are initiated by a loss of component cooling water (CCW) or SWS during vented, drained conditions. Fourteen percent of the core damage sequences are initiated by a LOOP during vented, drained conditions. Core damage sequences initiated by overdraining of the RCS and by loss of the RNS during vented, drained conditions contribute another 12 percent to the shutdown CDF.

The top six AP1000 dominant cutsets for the AP1000 internal event shutdown PRA, which contribute approximately 64 percent of the risk, are described below. The rest of the dominant cutsets contribute less than 3 percent of the shutdown CDF.

Sequence #1, with a CDF of 2.2E-8/yr and a 17 percent contribution, is initiated by a loss of CCS/SWS with the RCS vented and drained. CCF of all fourth stage ADS squib valves results in failure of gravity injection, leading to core damage.

Sequence #2, with a CDF of 1.9E-8/yr and a 15 percent contribution, is initiated by a loss of CCS/SWS with the RCS vented and drained. Actuation of the fourth stage ADS squibs is successful. CCF 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.

Sequence #3, with a CDF of 1.9E-8/yr and a 15 percent contribution, is initiated by a loss of CCS/SWS with the RCS vented and drained. Actuation of the fourth stage ADS squib valves is successful. Postulated CCF of two out of two low-pressure squib valve failures was assumed to lead to core damage. CCF of the low-pressure squib valves (118A/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.

Sequence #4, with a CDF of 8.6E-8/yr and a 7 percent contribution, is initiated by a loss of CCS/SWS with the RCS vented and drained. Postulated CCF of the IRWST recirculation sump strainers due to plugging fails recirculation and results in core damage.

Sequence #5, with a CDF of 8.6E-8/yr and a 7 percent contribution, is initiated by a loss of CCS/SWS with the RCS vented and drained. Postulated CCF of the IRWST strainers due to plugging fails gravity injection and results in core damage.

Sequence #6, with a CDF of 3.0E-8/yr and a 3 percent contribution, is initiated by a LOOP with the RCS vented and drained. The operators fail to recover offsite ac power in 1 hour, and there is a common-cause software failure of all PMS and PLS logic cards.

19.1.4.3 Risk-Important Design Features

Listed below are key AP1000 design features that significantly reduce the shutdown CDF as compared to the CDF for 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 currently operating PWRs, the AP1000 PRHR provides an additional path of core cooling which is diverse from the RNS, as well as ac independent and safety-related (passive). The PRHR does not depend on traditional support systems, such as CCW, to operate. In addition, the PRHR is capable of functioning at low pressures and temperatures, as long as the RCS is intact and the pressurizer level is above 20 percent. However, manual actuation is required before RCS pressure increases to cause the RHR valve to open.

In current PWRs, operator action is required to restore all interruptions of RHR. In the AP1000 design, should manual actuation of the PRHR fail, an alternate core cooling path is automatically established using the CMTs for injection, the 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 an RCS drain-path occur that is unisolable, RCS injection and core cooling are automatically provided using the CMTs, the ADS, gravity injection from the IRWST, and containment recirculation (for long-term cooling).

19.1.4.3.3 Loss of Station Power (LOSP)/SBO during Safe Shutdown/Cold Shutdown with the RCS Intact

The AP1000 design provides much better protection against LOSP/SBO events as compared to the current PWRs because the operator is not required to perform many recovery actions. Following a LOOP, 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, the PRHR provides core cooling automatically, because the PRHR AOVs are expected to fail open. Should manual

actuation of the PRHR fail, an alternate core cooling path is automatically established using the CMTs, the 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 Midloop Conditions

Previous PWR shutdown PRAs have reported that overdraining of the RCS during midloop 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 SGs 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 SGs (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, as well as the RNS net positive suction head (NPSH) requirements, allow the RNS pumps to be started and operated with saturated conditions in the RCS. In addition, there is no need to throttle RNS flow when the RCS is in midloop conditions.

If adequate NPSH is lost, recovery of the RNS is expected to be quicker as compared to operating PWR designs. The RNS pump suction line is sloped continuously upward from the pump to the RCS 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 because of excessive air entrainment. This self-venting suction line allows the RNS pumps to restart immediately once an adequate level in the hot-leg is reestablished.

To assist the operator, the AP1000 design contains hot-leg level instrumentation with indication in the main control room (MCR). 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 SG as possible. The AP600 design also provides a cold-calibrated, wide-range pressurizer level that can measure the RCS level down to the bottom of the hot-legs. This pressurizer level indication can be used as an alternative way of monitoring the 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 upon a low hot-leg level (one-out-of-two basis). On low hot-leg level, two safety-related AOVs close automatically to isolate letdown. On a low, low hot-leg level, the PMS provides automatic actuation of IRWST injection (two-out-of-two basis), as well as automatic actuation of fourth stage ADS valves to prevent surge line flooding (two-out-of-two basis). Long-term cooling is provided by containment recirculation.

19.1.4.3.5 LOSP/SBO during RCS Open Conditions

The AP1000 design provides much better protection against LOSP/SBO events as compared to current PWRs because the operator is not required to perform many recovery actions. Following a LOOP, 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 fourth stage ADS actuation (to prevent surge line flooding) is automatically provided upon a low hot-leg level. Gravity injection and fourth stage ADS actuation require only a Class 1E dc power train to operate. Containment sump recirculation provides long-term cooling.

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 the RNS as compared to current plants because the operator is not required to mitigate the event. Following a loss of the RNS, gravity injection from the IRWST and concurrent fourth stage ADS actuation (to prevent surge line flooding) is automatically provided upon an indication of a low hot-leg level from the PMS system. On a low IRWST level, automatic containment recirculation provides long-term core cooling.

19.1.4.3.7 Boron Dilution Events

The Surry Shutdown PRA (NUREG-6144, Appendix I, “Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry Unit 1”) evaluated a potential boron dilution event during reactor startup following a LOSP event, with subsequent startup of the RCPs. This scenario was estimated in Appendix I to NUREG-6144 as having a CDF of 9E-6/yr. The scenario assumes an occurrence of a LOOP during an 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 Class 1E dc and uninterruptible power supply (UPS) system battery chargers receive low-input voltage, the PMS provides a boron dilution signal that automatically realigns CVS pump suction to the BAT. 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 and failure of operator control of the 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 realigns CVS pump suction to the BAT. 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 concluded 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 of this report, the staff plans to use the results of the applicant's AP1000 importance analyses to identify (1) SSCs and/or human actions for which the reported reliability contributes most to achieving the low reported shutdown CDF (risk achievement worth), and (2) SSCs and/or human actions which would contribute most to a reduction in the shutdown CDF if the reliabilities were improved (risk reduction worth). Because the reported AP1000 internal shutdown CDF is very low and clearly meets the Commission's safety goals, as well as the EPRI ALWR CDF requirements (less than 10E-5/yr), the staff will focus on the results of the applicant's risk achievement analyses. The staff will use 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.

Risk importance analyses were performed at the component/human action level only. In summary, the components, whose reported reliability is most critical to achieving the low shutdown CDF, are required to support gravity injection during reduced inventory operation. The major insights from the risk achievement analysis (from Table 54-18 of the AP1000 Shutdown PRA) are summarized below in order of risk importance.

(1) Similar to the full-power internal events results, common-cause software failure among the PMS and PLS logic cards has very high risk significance (basic event CCX-SFTW). If a software fault of this kind existed and manifested itself every time an accident occurred during shutdown, the CDF would increase more than four orders of magnitude.

(2) Actuation of fourth stage ADS valves is required to maintain a vent path to mitigate all shutdown events when gravity injection and containment recirculation are required following an extended loss of the RNS during safe/cold shutdown with the RCS intact, as well as during cold shutdown with the RCS open. Therefore, CCF of the Stage 4 ADS squib valves to open has very high risk significance (basic event ADX-EV-SA). Should the fourth stage ADS squib valves fail to open when demanded, the shutdown CDF would increase more than three orders of magnitude.

(3) Containment sump recirculation is required to mitigate every loss of shutdown cooling event during cold shutdown with the RCS open (except LOSP events in which the diesels and automatic restart of the RNS are available). Containment sump recirculation is also required to mitigate every loss of shutdown cooling event during safe/cold shutdown with the RCS intact and the PRHR unavailable (except LOSP events in which the diesels and automatic restart of RNS are available). Therefore, the two basic events that result in the failure of containment sump recirculation have very high risk significance. These two events include the CCF of two-out-of-two low-pressure

recirculation squib valves (basic event, IWX-EV4-SA) and common-cause plugging of both containment strainers (basic event, REX-FL-GP). Assuming that either event were to always occur following a shutdown initiator, the CDF would increase more than three orders of magnitude.

(4) Gravity injection is required to mitigate every loss of shutdown cooling event during cold shutdown with the RCS open (except LOSP events in which the diesels and automatic restart of RNS are available). Gravity injection is also required to mitigate every loss of shutdown cooling event during safe/cold shutdown with the RCS intact where the PRHR is not available (except LOSP events in which the diesels and automatic restart of the RNS are available). Therefore, events that result in the failure of gravity injection have very high risk significance. Specifically, CCFs of six out of six of the high-pressure gravity injection squib valves (basic event, IWX-EV-SA) and plugging of both IRWST strainers (basic event, IWX-FL-GP) have very high risk significance. Plugging of both strainers fails both gravity injection through the IRWST injection lines and the RNS pump suction lines. Assuming that either event always occurs following a shutdown initiator, the CDF would increase more than three orders of magnitude.

(5) CCF of I&C components that fail automatic gravity injection and/or ADS actuation have very high risk significance, including CCF of the instrument orifices, CCF of the pressure transmitters, and CCF of the power interface output boards in the PMS system (basic events CCX-ORY-SPX, CCX-XMTRX, and CCX-EP-SAM). Should any one of the components fail when demanded, the shutdown CDF would increase more than three orders of magnitude.

(6) Inadvertent overdraining of the RCS while reducing inventory to reach midloop conditions has very high risk significance (initiating event IEV-RCSOD). This event results in loss of shutdown cooling (RNS) and requires manual RCS injection and manual fourth stage ADS actuation. For this initiator, the applicant did not credit recovery of the RNS using the non-safety-related CVS to restore the RCS level and operator action to vent the RNS pumps.

Three scenarios were postulated that would result in overdraining of the RCS. The first scenario starts with failure of either hot-leg-level instrument channel. The operator fails to recognize hot-leg instrument failure and thereby fails to stop the RCS overdraining. The second scenario assumes that the hot-leg-level instruments are working correctly; however, the safety-related CVS letdown valves fail to close. The third scenario assumes that the hot-leg-level instruments are working correctly. However, the signal to close the safety-related CVS letdown valves automatically fails, and the operator fails to respond to the low hot-leg alarm and close the CVS letdown valves.

(7) Occurrence of any one of these scenarios leads to RCS overdraining and requires manual actuation of gravity injection and fourth stage ADS. If the RCS was always overdrained when reaching midloop conditions, the CDF would increase by more than three orders of magnitude.

(8) Loss of shutdown cooling with the RCS drained (resulting from RNS failure or its support system failures) has high risk significance (initiating events IEV-CCWD and IEV-RNSD). These initiating events require fourth stage ADS actuation and gravity injection to maintain core cooling. Long-term cooling requires containment sump recirculation. Should either of these events occur each time the plant operates with reduced inventory, the shutdown CDF would increase close to three orders of magnitude.

(9) Inadvertent opening of RNS Valve V024 by an operator during RCS drained conditions causes reactor coolant to drain into the IRWST. This initiating event requires gravity injection from the IRWST and fourth stage ADS actuation. Long-term core cooling requires containment sump recirculation. Should this event occur each time the RCS is drained, the shutdown CDF would increase close to three orders of magnitude.

(10) Inadvertent opening of RNS Valve V024 by an operator during safe/cold shutdown with the RCS intact causes reactor coolant to drain into the IRWST. This initiating event requires gravity injection from the IRWST, full RCS depressurization, and containment recirculation for long-term cooling. Should this event occur each time the plant is at shutdown, the shutdown CDF would increase close to three orders of magnitude.

(11) Failure of the PMS boron dilution signal to generate upon high flux has high risk significance. Boron dilution events during safe shutdown were quantified separately from the PRA. Upon review of the associated event tree, failure of this signal to generate following every dilution event during safe shutdown results in a criticality frequency approximately four orders of magnitude higher than the shutdown CDF. Other boron dilution scenarios were not explicitly quantified. Therefore, the staff believes that all instrumentation associated with the boron dilution signal are important to keeping the core damage risk associated with boron dilution events low.

While performing the Level 1 PRA for internal shutdown events, the applicant identified the risk-important tasks outlined below, using the risk importance analyses results and threshold values. The applicant also examined shutdown initiating events to identify risk-important tasks for which 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. DCD Tier 2, Section 18.5, “Task Analysis Implementing Plan,” describes the process for ensuring that these tasks are addressed.

- 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 the 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 reclosing 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). This operator action is quantified as RCS-MANOD1S.

- 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 midloop conditions. This operator action is quantified as RCS-MANOD2S.

19.1.4.5 Insights from the Sensitivity Studies

The applicant performed sensitivity studies to gain insights about the impact of uncertainties on the reported 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.

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, as well as additional sensitivity studies, are described below.

19.1.4.5.1 Shutdown CDF Assuming Minimal Compliance with AP1000 TS

In the baseline and focused shutdown PRA, 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 midloop 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, CIV 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 the AP1000 TS during cold shutdown operation. With respect to RCS venting, the applicant credits, in the PRA, all four 4th stage ADS valves to be available. However, the AP600 TS only requires two out of the four ADS Stage 4 valves to be operable. With respect to containment sump recirculation, the AP1000 TS only requires one out of the two containment sump recirculation trains to be available.

The bases for the AP1000 TS include 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 the 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 2E-6 per year (a factor of 5 higher than the full-power CDF).

19.1.4.5.2 Impact of Operator Error

Based on the 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 event initiators quantitatively analyzed in the AP1000 shutdown PRA. Therefore, the dependency on operator action is significantly reduced in the AP1000. The applicant performed a sensitivity study setting all human error probabilities associated with event mitigation to 0.5. Additionally, the applicant also set the two operator actions (RCS-MANOD1S and RCS-MANOD2S) used to calculate the frequency of overdraining the RCS (IEV-RCSOD) to 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.

For this sensitivity case, the shutdown CDF becomes 5.5E-5/yr assuming all operator actions associated with event mitigation and overdraining are set as 0.5. 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 unavailable. 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.

Except for the LOSP trees, no other changes to the event trees were required because all event mitigation functions are safety-related. In the LOSP event tree, credit was removed for the non-safety-related diesel generators and grid recovery. In the system fault trees, the SBO fault trees were used for the Class 1E and the UPS systems so that only safety-related power supplies were credited.

Motor-operated valve RNS-V23 can be used for gravity injection by an operator action, if the normal IRWST injection fails. RNS valve V-23 is a safety-related, CIV and can be actuated using the PMS. The function of RNS V-23 is to open to provide gravity injection which is not a safety-related function, but use of this valve was credited in this sensitivity study.

The focused PRA shutdown CDF was estimated to be 1.2E-6, approximately a factor of ten increase over the AP1000 baseline internal shutdown CDF. The increase results from the postulated loss of the diesel generators to mitigate a LOOP during RCS filled conditions and RCS drained and vented conditions.

19.1.5 Safety Insights from the External Events Risk Analysis

The AP1000 PRA analyzed three external events, including seismic, internal fires, and internal floods. In many PRAs performed to date, these external events have had combined CDFs that are of the same magnitude as those for internal events. It is not unusual for the combined CDFs for these events to be in the 1E-4/yr 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. In addition, these 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, internal 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 reveal any 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) data 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 the PRA results are significantly impacted. 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 19.1.1.1-1.

19.1.5.1 PRA-Based Seismic Margin Analysis (SMA)

The AP1000 is designed to withstand a 0.3g safe-shutdown earthquake (SSE). Because the analyses used in designing the capability of SSCs to withstand the SSE have significant margin in them, it is expected that a plant built to withstand the SSE will actually 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-2) that failure of the SSC will occur. An 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 acceleration of the SSE (i.e., 0.5g). The PRA-based SMA 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. Because such systems are not seismic Category I, it is conservatively assumed that they become unavailable as a consequence of the seismic initiating event. Because 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 LOOP (HCLPF of ceramic insulators is 0.09g), all accident sequences are treated in the SMA as SBO sequences. The analysis investigated and accounted for the potential for adverse interactions between assumed seismically damaged non-safety-related SSCs and safety-related systems. 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 were used when insufficient information was available to determine the HCLPF value by means of one of the above-mentioned approaches. The min/max approach[2] was used for the sequence- and plant-level HCLPF calculations. The

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

staff's review of these calculations indicated that they were performed in accordance with the rules of the min/max approach and were, therefore, found to be acceptable. DCD Tier 2, Appendix 19A, offers additional background information about the seismic margins methodology and its implementation to the AP1000.

19.1.5.1.1 Dominant Accident Sequences for Seismic Events

The staff used the results of the applicant's risk-informed SMA 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. Because, 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 nonseismic failures were examined to find out if any cutsets would lower the plant HCLPF below 0.5g. This examination has shown that no such cutsets exist for AP1000. 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 SMA. These sequences have the lowest HCLPFs (cutsets with seismic only failures considered) or the lowest combination of HCLPF with random failure/human error (cutsets with both seismic and nonseismic failures considered).

Seismic sequence #1, with HCLPF value 0.5g, is a seismically induced break of the RCS pressure boundary which results in loss of coolant beyond the capacity of the emergency core cooling system (ECCS) to provide makeup and leads directly to core damage. Major contributors are fuel failure (HCLPF value 0.5g), SG 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 0.5g, is a seismically induced structural collapse of parts of the nuclear island. Major contributors are collapse of (1) the shield building wall or roof (0.51g), (2) the passive containment cooling water tank (0.51g), (3) an interior (concrete) structure of containment (0.5g), and (4) IRWST structure (0.5g).

Seismic sequence #3, with HCLPF value 0.54g, is a seismically induced ATWS event and failure of the ADS. The most important cutsets associated with this sequence involve failure of the reactor internals or core assembly which causes failure of the control rods to insert (HCLPF value of 0.5g), combined with failure of the Class 1E 120-V ac control power (HCLPF value of 0.55g), which causes failure of the ADS. The most important contributors to the seismically

induced failure of the Class 1E 120-V ac power are (1) failure of the 125-V dc distribution panels (0.55g), (2) failure of the 120-V ac distribution panels (0.55g), (3) failure of the 125-V 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 CMTs. The most important cutset associated with this sequence involves failure of the reactor internals or core assembly which causes failure of the control rods to insert (0.5g), 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 nonseismic failures) in which the HCLPF of the seismic portion is less than the plant HCLPF value (i.e., less than 0.5g). This indicates that no random failures or human errors are 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 (i.e., 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-2).

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 assumed that the containment fails when the reactor vessel fails because of 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. Because 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 an 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, using importance analyses, of which plant features are most important to risk. 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. 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, drawn from the examination of the SMA results (accident sequences and associated cutsets), about the capability of the AP1000 design to withstand earthquakes 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, the details of which are to be developed by the COL applicant. This is COL Action Item 19A.2-1.

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

- A number of accident sequences 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 an 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 an HCLPF value close to the plant HCLPF. The following sequences contain this kind of cutsets:

  - ATWS sequences which involve failure of the reactor internals or core assembly which causes failure of the control rods to insert (HCLPF value 0.5g), in combination with one other failure for which the HCLPF is considerably higher than the plant HCLPF value of 0.5g, such as IRWST injection CVs (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 125-V 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 nonseismic failures) in which 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 to below 0.5g when certain nonseismic (random) failures occur are LOOP 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-7 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 to 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 revealed that human errors are not significant contributors to nonseismic failure probabilities.

Severe Accidents

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

- There are no safety-related SSCs with HCLPF values less than 0.5g.

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

- Because of 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 (0.5g) 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 MCR 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 PXS valves are concentrated, is an important factor in the ability of the AP1000 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, the details of which are to be developed by the COL applicant. This is COL Action Item 19A.2-2 (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 SMA 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 because hazard curves have a large uncertainty which reduces their value in helping to make judgments 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, because the margins method does not quantify risk (e.g., in terms of CDF), importance analyses were not performed. The applicant 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 presented below.

- A decrease in the "generic" HCLPF values assumed in the SMA for several SSCs, such as the 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 because these values affect a large number of components. One or more sequences always exist for which the 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 (the COL applicant will confirm this during a seismic walkdown of the as-built plant). This process is part of COL Action Item 19A.2-2.

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

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

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

- Because 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, 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, and 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., as described in NUREG/CR-2300, 1983, and NUREG/CR-4840, 1989).

In general, the fire PRA is a screening-level analysis and employs a number of conservative assumptions. For two fire areas,[3] the containment and the main control room (MCR), the PRA uses somewhat less conservative assumptions. 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 be only slightly conservative for plant areas housing sensitive electronic 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, the analysis assumes 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. The analysis treats fire-induced hot shorts in relevant safety- and DAS-related cables and cabinets as leading to medium LOCA (MLOCA) or large LOCA (LLOCA) scenarios when the reactor is at power. The analysis also considers fire-induced MLOCA scenarios when the reactor is shut down (but not in midloop). It does not give credit for the potential use of fiber optics cabling and digitally encoded signals in portions of the control system.

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

- 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 a 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 analysis does not modify the human error probabilities used in the recovery analysis 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 firefighting activities and plant response) will not place any significant additional burden on the MCR operators.

- The hot/cold shutdown (HCSD) and midloop (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 digital I&C design of the AP1000, fires within these areas are not expected to inhibit the automatic actuation of safe-shutdown equipment. Within the containment, continuous structural or fire barriers without penetrations and labyrinth passageways generally separate redundant divisions (in a few cases, large open spaces without intervening combustibles separate the divisions). 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 failures (not caused by fire) 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, both at power operation and during shutdown, by using applicable event and fault tree models from the internal events PRA. The applicant assessed the fire-induced CDF at about 5.6E-8/yr for fires occurring during power operation and about 8E-8/yr for fires occurring during shutdown. The applicant considers these 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 insights that the internal fires analysis provides about the design. Based on this information, the staff concludes 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 the reliability assurance program (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. This is COL Action Item 19.1.5.2.1-1.

19.1.5.2.1.1 Operation at Power

The top 10 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-8/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 to fail are the Class 1E power and control Divisions A and C, one CMT, one PRHR isolation valve, and one CCS flowpath to the containment. The dominant fire scenarios associated with a fire in Fire Area 1100 AF 11300B are the following:

- 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 an MLOCA. The remaining safety systems do not mitigate the fire-induced MLOCA, which leads to core damage. This scenario contributes about 8.5E-9/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 an medium LOCA. The remaining safety systems do not mitigate the fire-induced MLOCA, which leads to core damage. This scenario contributes about 3.1E-9/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 remaining safety systems do not mitigate the fire-induced transient, which leads to core damage. This scenario contributes about 8.3E-10/yr to the fire CDF.

- Fire suppression fails, but the fire does not propagate. However, “hot shorts” occur that cause the spurious opening of a Stage 1, 2, and 3 line leading to an MLOCA. The remaining safety systems do not mitigate the fire-induced MLOCA, which leads 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-9/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 to fail 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 an MLOCA. The remaining safety

systems do not mitigate the fire-induced MLOCA, which leads to core damage. This scenario contributes about 9.0E-9/yr to the fire CDF.

Fire Area #3, with a CDF of about 6.7E-9/yr and about 12 percent contribution, includes the auxiliary building corridors at Elevation 100’ and 117’-6" (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 receives power or actuation signals through cables passing through the area. Important equipment assumed to fail are I&C cables for Divisions B and D (since no cables dedicated to any ADS valves pass through this area, the ADS valve operation is not affected), 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 the following:

- a fire-induced transient not mitigated by the remaining safety systems, which leads to core damage (contributes about 4.4E-9/yr to the fire CDF)

- 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 and leads to core damage (contributes about 2.2E-9/yr to the fire CDF)

Fire Area #4, with a CDF of about 5.1E-9/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 the compressed and instrument air system (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 remaining safety systems do not mitigate the fire-induced loss of MFW transient, which leads to core damage. This scenario contributes about 5.1E-9/yr to the fire CDF.

Fire Area #5, with a CDF of about 4.3E-9/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 a fire-induced transient the remaining safety systems do not mitigate, and which leads to core damage. This scenario contributes about 4.3E-9/yr to the fire CDF.

Fire Area #6, with a CDF of about 4.0E-9/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 a fire-induced transient, which is not mitigated by the remaining safety systems and leads to core damage. This scenario contributes about 3.9E-9/yr to the fire CDF.

Fire Area #7, with a CDF of about 2.3E-9/yr and about 4 percent contribution, is the auxiliary building non-Class 1E electrical compartment at Elevation 100' (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 a fire-induced transient which is unmitigated by the remaining safety systems and leads to core damage. This scenario contributes about 2.1E-9/yr to the fire CDF.

Fire Area #8, with a CDF of about 2.1E-9/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 following are the dominant fire scenarios associated with a fire in Fire Area 1200 AF 03:

- a fire-induced spurious actuation of one ADS Stage 4 valve (an LLOCA) which is not mitigated and leads to core damage (contributes about 1.0E-9/yr to the fire CDF)

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

Fire Area #9, with a CDF of about 2.0E-9/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 and leads to core damage.

Fire Area #10, with a CDF of about 1.8E-9/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 following are the dominant fire scenarios associated with a fire in Fire Area 1200 AF 03:

- a fire-induced spurious actuation of one ADS Stage 4 valve (an LLOCA) which is not mitigated and leads to core damage (contributes about 1.2E-9/yr to the fire CDF)

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

The AP1000 PRA predicts that fire-induced spurious actuation of ADS valves leading to a LOCA event (about 54 percent contribution) dominates the at-power fire risk. Spurious opening of one ADS Stage 1, 2, and 3 line (an MLOCA) contributes about 44 percent while spurious opening of a Stage 4 squib valve (an LLOCA) contributes about 10 percent. Most of the remaining CDF (46 percent) is attributed to 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. Because the analyses for the various areas of the plant employ different levels of conservatism (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 to identify potential vulnerabilities and to offer insights into 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, some of these failures involve single component failures. Thus, the AP1000 fire PRA predicts that there may be scenarios (although of low probability) in which 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) if non-safety-related defense-in-depth systems, such as DAS and RNS, had 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 can bring the plant within one failure of core damage.

19.1.5.2.1.2 Low Power and Shutdown Operation

The AP1000 Shutdown PRA reported the fire-induced CDF during shutdown to be on the order of 8E-8/yr, approximately 66 percent of the shutdown internal events risk. The AP1000 Shutdown fire risk is dominated by fires occurring while the plant is in vented, drained conditions. This contributes 95 percent of the AP1000 shutdown fire risk.

To develop the fire analysis, analysts evaluated the dominant sequences from the AP600 shutdown fire PRA and the AP1000 fire PRA. It is important to note that the analysts used the focused PRA to develop the conditional core damage probabilities given a shutdown fire in a specific fire area, and therefore, non-safety-related systems were not credited to mitigate the fire.

In Table 57-24 of the AP1000 PRA, the applicant reported two shutdown fire sequences occurring during vented, drained conditions that contribute approximately 94 percent of the AP1000 shutdown fire risk. The first sequence initiates from a fire that results in a loss of the RNS or its support system CCW or SWS (Scenario, SC-14-2). Subsequent random failure to remove decay heat from IRWST injection or containment recirculation leads to core damage. This sequence represents approximately 58 percent of the AP1000 shutdown fire CDF.

The second sequence initiates from a fire inside containment that results in spurious actuation of RNS V024 during vented, drained conditions (Scenario, SC-18-1). Spurious actuation of RNS V024 leads to a loss of RCS inventory. The fire zone grouping considered in SC-18-1 includes fires in the PXS valve accumulator room, Fire Zone 1100 AF 11206. Fires in the PXS valve accumulator room result in loss in one of two divisions of IRWST injection valves and one of two divisions of containment sump recirculation valves. Subsequent random failure of the other division of IRWST injection or the other division of containment sump recirculation leads to core damage. This sequence represents approximately 36 percent of the AP1000 shutdown fire CDF.

It is important to note that none of the identified internal fire events during shutdown operation leads to core damage unless additional random failures occur.

19.1.5.2.2 Risk-Important Design Features and Operator Actions for Internal Fires

The following is a list of important design features contributing 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 four safety-related electrical divisions (Divisions A through D) are in separate fire areas (i.e., barriers of at least 2-hour fire rating or equivalent separate them). In particular, 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 these 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).

- Separation of automatic actuation systems from MCR and RSW. The MCR and the RSW are the only two plant areas where there is a significant likelihood of a single fire affecting all four divisions. For fires in these areas, the plant is designed to have an independent, automatic means to reach safe shutdown. (In fact, the design does not require operator actions from the MCR and RSW; the design treats these actions as backups to the automatic response.)

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

- 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 the containment maintenance floor (Fire Area 1100 AF 11300B). Compared to operating reactors, the AP1000 design is significantly less dependent on human actions to mitigate internal fires. The COL applicant will develop procedures for implementing these fire-specific operator actions. This is part of COL Action Item 9.5.1-4.

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 relatively small for the I&C rooms (as compared to other areas of the plant which contain more rugged components).

Comparing fire risk at shutdown versus at full power, the staff considered the impact of transient combustible materials and fire barrier integrity (two key AP1000 PRA-based insights included in Table 59-18). Regarding transient combustibles, the applicant stated that they are to be controlled administratively. With respect to fire barrier integrity, the AP1000 Shutdown PRA assumes that fire barriers are intact. Acknowledging that fire barriers may be breached to perform maintenance at shutdown, the applicant stated that the COL applicant will establish procedures to address a fire watch for fire areas breached during maintenance. This is part of COL Action Item 9.5.1-3.

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

The applicant performed no uncertainty and importance analyses for internal fires. Because of the conservatism in the approach taken in the AP1000 internal fire PRA, the applicant judged that uncertainty and importance analyses would result in biased insights. Since the applicant took no credit 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 (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 the fire PRA (ADS Stage 4 line opening by DAS) credited with meeting the success criteria for depressurization during spurious opening of ADS paths leading to a LOCA event. TS 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 into the impact of uncertainties on fire risk. The following are important insights from these studies:

- Increasing the “hot short probability” assumed in the fire risk analysis by a factor of 2 would increase the plant fire CDF for power operation about 3 times (from 5.6E-8/yr to

about 1.6E-7/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. 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 prevent spurious actuation of ADS valves.

- Increasing the failure probability of the two fire-specific human actions (discussed in Section 19.1.5.2.2 of this report) to 1 (i.e., taking no credit for such operator actions) would increase the plant fire CDF for power operation almost 5 times (from 5.6E-8/yr to about 2.6E-7/yr). This bounding analysis result shows that the fire CDF is somewhat sensitive to reasonable increases in the probabilities of fire-specific operator action failure, but the sensitivity is not large enough by itself to affect 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-8/yr to about 2.2E-7/yr). This result indicates some sensitivity of the fire CDF to reasonable increases in the manual DAS actuation failure probability. However, this sensitivity is not large enough by itself to affect PRA conclusions about the design.

19.1.5.3 Internal Flooding Risk Analysis

Because of 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 such as 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 commensurate with the level of detail available and made conservative assumptions, where detailed information was not available, to bound the flooding analysis. The staff finds that this analysis is adequate to identify potential vulnerabilities and to lend insight into the design which can be used to support design certification requirements, such as ITAACs.

The performance of the internal flooding PRA had four stages. During the first stage, the applicant collected information required to perform the flooding analysis, 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, the applicant performed an initial screening of the areas identified during the first stage, using conservative assumptions (e.g., total immersion and failure of equipment in affected areas) and considering 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, the applicant screened the areas identified in the second stage (e.g., by determining maximum expected flood height and evaluating the potential for spray of safe-shutdown equipment and the potential for propagation into other areas) to identify plant areas where flooding could affect safe-shutdown equipment modeled in the internal events PRA. During the fourth stage, the applicant quantified the risk from flooding in

the areas which were not screened out during the second and third stages 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 identified 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-9/yr.

The risk analysis for internal flooding during shutdown operation was performed in a manner similar to the analysis performed for at-power operation. The screening of potential flooding areas performed as part of the at-power analysis was reviewed for applicability to shutdown operation based on the 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 3.2E-09 per year. However, during the staff's review of the responses to RAI 720.38 (dated 3/28/03 and 4/12/2003), the staff noted some math errors that could have increased the shutdown CDF from internal floods by about 20 percent. Flooding scenario numbers 5 and 6, a rupture of the 20.3 cm (8 in.) fire main extension that fails RNS, with or without the RCS drained, appeared to have been mis-calculated. This was Confirmatory Item 19.1.10.2-1 in the DSER. The applicant revised Chapter 56 of the AP1000 PRA, "Internal Flooding Analysis," correcting the calculations, showing the CDF to be 3.2E-09 per year. Therefore, Confirmatory Item 19.1.10.2-1 is resolved.

The applicant considered 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 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 applicant's internal flood risk analysis 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. This is COL Action Item 19.1.5.3-1.

19.1.5.3.1 Dominant Accident Sequences for Internal Floods

The applicant quantified the CDF associated with internal floods, 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. The analysis assumes that the flooding and spraying damage 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/SWS" accident-initiating event with several non-safety-related support and balance of plant equipment unavailable. Several combinations of random failures can lead 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

- 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 the same consequences in terms of both equipment failures and propagation to other areas. Flow from a rupture in the turbine cooling water system (TCS) initiates Scenario #2, while flow from a rupture in the heater drain system initiates Scenario #3.

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 the flood 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. The analysis assumes that the flooding and spraying damage 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. Several combinations of random failures can lead to core damage in this flooding scenario. The dominant ones are the same as those in 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, the flood propagates via floor grating to the Elevation 100'-0" areas. The analysis assumes that the flooding and spraying damage 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/SWS" or a "loss of main feedwater to both steam generators"

accident-initiating event with several non-safety-related and balance of plant equipment unavailable. Several combinations of random failures can lead to core damage in this flooding scenario. The dominant ones are the same as those mentioned 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 midloop operation (RCS drained condition). The analysis assumes that this break and the subsequent flooding and spraying damage all equipment contained in the turbine building. This causes a loss of DHR accident-initiating event because of 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 midloop operation (RCS drained condition). The analysis assumes that the flooding and spraying damage the RNS contained in the auxiliary building RCA area and cause a loss of DHR 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 quantities of water are outside the nuclear island (containment and auxiliary building) and the annex building.
- No safety-related equipment is 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.

Severe Accidents

- 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 15.2 cm (6 in.). 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 watertight 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—the sloped floor directs flow to drains and to the yard area through the door of the annex building.

- Floor drains direct flow from any postulated ruptures above grade level (Elevation 100'-0") in the annex building 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 the 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 nonradiologically controlled areas of the nuclear island where all safety-related equipment, except for some CIVs, is located.

- To prevent flooding in an RCA in the auxiliary building from propagating to non-RCAs (where all safety-related equipment except for some CIVs 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 is 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.

- Two compartments inside containment (PXS-A and PXS-B) contain safe-shutdown equipment other than CIVs 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. Redundant backflow preventers protect drainlines from the PXS-A and PXS-B compartments to the reactor vessel cavity and SG compartment from backflow.

- 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, CIV 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 flowpath as straight as possible. Drain headers are at least 10.2 cm (4 in.) in diameter and include features, such as CVs 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 of 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 and 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, the internal flooding PRA regarding human errors offers no additional significant insights.

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

The applicant did not perform uncertainty, importance, or sensitivity analyses for internal floods. Because of the conservatism in the approach taken in 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.

- Compared to operating reactors, the AP1000 design is significantly less dependent on human actions to mitigate internal floods.

- If the applicant takes no credit 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-8/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 affect the criteria (reported in Section 19.1.7) used to select non-safety-related systems for "regulatory treatment" according to the RTNSS process.

- If the applicant takes no credit for 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 a 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

The applicant 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. It first used this information 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 the applicant had introduced these features, it used PRA 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 applicant used the AP600 PRA insights 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:

- The normal position of the two MOVs in the sump recirculation lines (which are in series with squib valves) was changed 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 the AP600, the ATWS contribution to 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 the 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 CCF probability of the recirculation lines which is a dominant contributor to risk.

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

The applicant also made operational changes 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 applicant modified the procedure for this severe accident response so that the operator performs the action associated with IRWST draining earlier to allow more time for operator success and also to fill the cavity as soon as possible.

Severe Accidents

Finally, the applicant used PRA 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 Process

The NRC and the ALWR Steering Committee reached consensus on a process for resolving the RTNSS issue (SECY-94-084) which was identified during the certification of the AP600 design. The same process was used for resolving the RTNSS issue in the AP1000 design certification. This process included the use of both probabilistic and deterministic criteria to achieve the objectives of (1) determining whether regulatory oversight for certain non-safety-related systems was needed, (2) identifying risk-important SSCs for regulatory oversight (if it were determined that regulatory oversight was needed), and (3) deciding on an appropriate level of regulatory oversight for the various identified SSCs commensurate with their importance to risk. 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-4/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-6/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 considering the risk importance of SSCs contributing to the frequencies of initiating events. Specifically, the RTNSS process requires that the following two items be addressed:

- uncertainties, such as in the assumed reliability values for passive system components
- the possibility that non-safety-related SSCs contributing to initiating event frequencies 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 to assess the plant's CDF and LRF values (except for the RPV thermal insulation system which is subject to regulatory oversight). This assessment resulted in a CDF value smaller than 1E-4/yr, which meets the first probabilistic criterion. However, the assessed LRF value exceeded 1E-6/yr, which does not meet the second probabilistic criterion. This result required, according to the RTNSS process, the identification of SSCs for an appropriate level of regulatory oversight commensurate with their risk importance. Based on

the review of dominant cutsets and insights from the risk importance analysis, it was determined that both probabilistic criteria are met when credit is taken for manual DAS controls in the focused PRA. The focused PRA credits the following DAS manual controls:

- reactor trip
- PRHR HX and IRWST gutter valves
- CMT isolation valves
- ADS Stages 1, 2, 3, and 4
- IRWST injection isolation valves
- containment recirculation isolation valves
- PCS water drain valves
- CIVs

Since the DAS manual controls are credited in the focused PRA to meet the probabilistic criterion for LRF, the applicant decided to include these manual controls in the AP1000 technical specifications (see Chapter 16 of this report).

In addition, the applicant provided probabilistic arguments showing that SSCs contributing to initiating event frequencies need no additional regulatory oversight, 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 the 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, SWS 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, SWS, 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, insights from the sensitivity studies documented in Section 19.1.3.1.5 of this report 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 the PRA uses more bounding data 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, regulatory oversight of certain SSCs is needed as 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 CBs
- ESF actuation components, such as software
- passive system CVs and explosive (squib) valves

A series of sensitivity studies were performed 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 into the risk importance of the various defense-in-depth systems considered in selecting non-safety-related systems for regulatory treatment according to the RTNSS process (Section 19.1.3.1.5 of this report discusses detailed results and insights related to CDF, while Sections 19.1.3.2 and 19.2.4 of this report discusses insights related to LRF and CCFP). The following summarizes the most important insights from such sensitivity studies, as they relate to the RTNSS process:

- Availability control of the automatic RT function of DAS provides an efficient means for minimizing the impact of uncertainties in reactor trip components, such as CBs, 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 automatic 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 CVs 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.

- The CCFP is approximately 0.1 in the baseline PRA and is not dramatically changed in the focused PRA (CCFP is about 0.2 in the focused PRA, which credits manual DAS controls but not other non-safety-related system).

These insights indicated that availability controls on the automatic portion of DAS (for both the reactor trip and ESF actuation functions) and for RNS compensate for the uncertainties in passive system reliability discussed in Section 19.1.3.1.5 of this report. The COL holder will control the availability of these systems, as documented in Section 16.3 of this report, so that on average, they will be available at least 90 percent of the time. This commitment will satisfy both probabilistic criteria (i.e., CDF less than 1E-4/yr and LRF less than 1E-6/yr) even when the identified uncertainties in passive system reliability are considered. In addition, with this commitment, the applicant reduces the CCFP to about 0.13. The staff concludes that an appropriate balance between prevention and mitigation is maintained.

In meeting the second probabilistic criterion (i.e., LRF less than 1E-6/yr) and the CCFP goal, the assessment credited ERVC as a strategy for retaining molten core debris in-vessel. This results in the majority of core melt accidents (about 90 percent) being arrested in-vessel, thereby avoiding RPV failure and associated containment challenges from ex-vessel phenomena. Successful RCS depressurization and reactor cavity flooding are prerequisites for

ERVC, and credit for these aspects of ERVC in the focused PRA is appropriate since both functions are fulfilled by safety-related systems. However, successful ERVC also requires the non-safety-related RPV thermal insulation system. The thermal insulation system limits thermal losses during normal operations but provides an engineered pathway for supplying cooling water to the vessel and venting steam from the reactor cavity during severe accidents. Attributes of the system include specific RPV/insulation clearances and water/steam flow areas based on scaled tests, water inlets and steam vents which change position during flood-up of the reactor cavity, and insulation panel and support members designed to withstand the hydrodynamic loads associated with ERVC.

In view of the reliance on ERVC to meet the Commission's LRF and containment performance goals, the applicant has committed to regulatory oversight of the RPV thermal insulation system according to the RTNSS process. Specifically, the reliability assurance program includes the system as a risk-significant SSC, the DCD contains the design description and functional requirements for the RPV insulation, and the ITAAC includes important criteria associated with the insulation design. This oversight provides reasonable assurance that the as-built insulation system conforms with design specifications contained in Chapter 39 of the PRA, "In-Vessel Retention of Molten Core Debris," and that periodic surveillance checks the operability of the system.

19.1.8 PRA Input to the Design Certification Process

PRA has been used in the design certification process to achieve the following objectives:

- develop an indepth understanding of design robustness and tolerance of severe accidents initiated by either internal or external events

- 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 more refined procedures

- identify important safety insights related to design features and assumptions made in the PRA to support certification requirements, such as ITAACs, D-RAP requirements, TS, as well as COL and interface requirements

The applicant achieved the first two objectives 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 of this report). The applicant achieved the third objective by using PRA insights and assumptions to develop the following list of design certification requirements. The DCD incorporates these requirements, as appropriate, to ensure that any future plant that references the AP1000 design will be built and operated in a manner consistent with the important assumptions made in the AP1000 design certification PRA.

19.1.8.1 General and Plant-Wide Requirements

- The applicant identified risk-important SSCs and included them in the D-RAP (DCD Tier 2, Section 17.4).

Severe Accidents

- 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. The COL applicant will develop the details of the process. This is part of COL Action Item 19A.2-2.

- The COL applicant referencing the AP1000 certified design will review differences between the as-built SSC HCLPFs and those assumed in the AP1000 seismic margin evaluation. The applicant should evaluate deviations from the HCLPF values or assumptions in the seismic margins evaluation to determine if vulnerabilities have been introduced. This is part of COL Action Item 19A.2-1.

- 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. Section 17.5 of this report discusses these COL Action Items.

- 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 programs related to human reliability. This is part of COL Action Item 19.1.3.1.4-1.

- 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 reevaluate the qualitative screening of external events. The updated PRA will include any site-specific susceptibilities found and the applicable external events. This is COL Action Item 19.1.8.1-1.

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

- A combination of multiple isolation valves, valve interlocking, and increases in the piping pressure limits and pressure relief capability protects the AP1000 against an ISLOCA.

- The AP1000 safety-related I&C system will use solid state switching devices and electromechanical 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 flowpath 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 non-safety-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. This is COL Action Item 9.5.1-1(c).

  – COL applicant programs will implement requirements for fire barriers and their maintenance. 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). This is COL Action Item 9.5.1-1(f).

  – When a fire door or a fire barrier penetration must be open to allow specific maintenance (e.g., during plant shutdown), the COL applicant will take appropriate compensatory measures to minimize risk. Appropriate outage management, administrative controls, procedures, and operator knowledge of plant configuration minimize risk during shutdown. In particular, minimizing risk will call for configuration control of fire barriers to ensure the integrity of fire barriers between areas containing equipment performing redundant safe-shutdown functions. This is COL Action Item 19.1.8.1-2.

- The design provides fire detection and suppression capability. The design also provides flooding control features and sump level indication. The COL applicant is expected to take compensatory measures to maintain adequate detection and suppression capability during maintenance activities. This is part of COL Action Item 19.1.8.1-3.

- In addition to the dedicated ventilation system for the MCR, there are separate ventilation systems for each of the two pairs of safety-related equipment divisions supporting redundant functions (i.e., Divisions A and C and B and 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 implement the maintenance guidelines as described in WCAP-14837, Revision 3, "AP600 Shutdown Evaluation Report," issued March 1998. This is COL Action Item 19.1.8.1-4.

- The COL applicant will control transient combustibles. This is particularly important during shutdown operation with ongoing maintenance activities. This is COL Action Item 19.1.8.1-5.

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 an 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 the PMS cabinets, in which the automatic functions are housed, are located in fire areas separate from the MCR.

- The RSW provides sufficient I&C 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 if 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 that originate in areas outside the control room 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 CIVs 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 that the plant can achieve safe-shutdown conditions. Such features include separation (structural or space), suppression, lack of combustibles, and operator actions.

- Two compartments inside containment (PXS-A and PXS-B) contain safe-shutdown equipment that is 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. Redundant backflow preventers protect drain lines from the PXS-A and PXS-B compartments to the reactor vessel cavity and SG compartment.

- 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 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 preventing small animals from entering the drains) of two 100-percent drain openings, located in the sidewall 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 blockage 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 19.1.8.3-1.

- 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 part of COL Action Item 6.2.1.8.1-1.

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 and C and B and D). This prevents smoke, hot gases, and fire suppressants originating in Divisions A or C from propagating to Divisions B and D.

- Fire walls with a 3-hour rating and 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. 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 MCR 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 0.61 m (2 ft) and 0.91 m (3 ft) walls and floor slabs prevents flooding in an RCA in the auxiliary building from propagating to non-RCAs. In addition, electrical penetrations between RCAs and non-RCAs in the auxiliary building are located above the maximum flood level.

- The location of the two 72-hour-rated Class 1E Division B and C batteries is 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 watertight 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 connections to sources of a large quantity of water are in the turbine building. They are the SWS, which interfaces with the CCS, and the CWS, which interfaces with the turbine building closed cooling system (TCS) and the condenser. The following features minimize flood propagation to other 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.

– 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 direct 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 nonradiologically controlled areas of the nuclear island, where all safety-related equipment except for some CIVs is located.
- 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 SGs 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 the RCS level during midloop 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 SG as possible.
- Wide-range pressurizer level indication (cold calibrated) measures the 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 RCS 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 because of excessive air entrainment. This self-venting suction line allows the RNS pumps to immediately restart once reestablishment 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. The operators should receive training 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 19.1.8.7-1.

19.1.8.8 Passive Core Cooling Systems

The PXS is composed of the accumulator subsystem, the CMT subsystem, the IRWST subsystem, and the PRHR subsystem. In addition, the ADS, which is part of the RCS, 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:

- Each of the two accumulators has an injection line to the reactor vessel/DVI nozzle. Each injection line has two CVs in series.

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

- Diversity between the accumulator CVs and the CMT CVs minimize the potential for CCFs.

19.1.8.10 Core Makeup Tanks

The CMTs provide safety-related means of HPSI of borated water to the RCS.

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

- Each of the two CMTs has 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 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 CVs in series.

- Actuation of the CMT AOVs from the 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 TS require the CMTs to be available from power conditions down through cold shutdown (Modes 1 through 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. The following are important aspects of the IRWST subsystem as represented in the PRA:

- The IRWST subsystem has the following flowpaths:

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

  – Two (redundant) recirculation lines run 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, and the other path contains a squib valve and a CV.

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

- Screens for each IRWST injection line and recirculation line prevent 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 through the development of a cleanliness program. This is part of COL Action Item 6.2.1.8.1-1.

- Explosive (squib) valves provide the pressure boundary and protect the CVs 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 CVs are diverse from the other recirculation squib valves in order to minimize the potential for CCF 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 CVs 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.

- TS require IRWST injection and recirculation to be available from power conditions to refueling without the cavity flooded (from Modes 1 through Mode 6).

- ERG AFR-C.1 governs the operator action to flood the reactor cavity. This guideline instructs the operator to flood the reactor cavity when the core-exit thermocouples reach 648.9 °C (1200 °F).

- A low IRWST level signal automatically actuates the PXS recirculation valves. If automatic actuation fails, the valves can be actuated manually from the control room.

19.1.8.12 Passive Residual Heat Removal System

The PRHR provides a safety-related means of performing the following functions:

- removes core decay heat during accidents

- allows adequate plant performance during transient (non-LOCA and non-ATWS) accidents without ADS

- allows automatic termination of RCS leak during an SGTR accident without ADS

- 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 (the safety-related PMS and the non-safety-related DAS) automatically actuate the PRHR AOVs. Operators can also manually actuate the PRHR from the control room using either PMS or DAS.

- Diversity between the PRHR AOVs and the AOVs in the CMTs minimize the probability of CCF 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 pool cooling 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 1892 liters per day (500 gallons per day) 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 drainline shut, and the gutter overflow returns directly to the IRWST. The following design features provide proper realignment 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 redirect the flow will, by design, fail closed.

  - The PMS and DAS automatically actuate the drain isolation.

- TS 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. Each stage comprises two separate groups of valves and lines. 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.

- By design, the valve arrangement and positioning for each stage reduce 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 position 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 DHR is lost.

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

- TS require ADS to be available during power operation and shutdown conditions until the cavity is flooded (i.e., from Modes 1 through 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 AP1000 design includes features that prevent fire-induced spurious actuation of a squib valve. These features include the use of a squib 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, in the case of PMS, the use of arm and fire signals from separate PMS cabinets), and provisions for operator action to remove power from the fire zone.

- The COL applicant will provide an analysis demonstrating that manual actions to allow fire water to reach the automatic fire system in the containment maintenance floor can be accomplished within 30 minutes following detection of the fire. Also, the COL applicant will develop procedures for implementing these manual actions which minimize the probability that spurious ADS actuation will result from a fire. This is part of COL Action Item 9.5.1-4.

- The ADS mitigates high-pressure core damage events which can challenge containment integrity because of the following severe accident phenomena:

  – high-pressure melt ejection
  – DCH
  – induced SGTR
  – induced RCS piping rupture and rapid hydrogen release to containment

19.1.8.14 Instrumentation and Control Systems

The PRA credits three I&C systems with 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 ESF

- monitoring of 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
- 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)

- 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 two redundant channels.

- The PMS has redundant divisions of safety-related postaccident 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 following contribute to the reliability of the PMS:

  – The reactor trip functions are divided into two subsystems.

  – Two microprocessor-based subsystems that are functionally identical in both hardware and software process the ESF functions.

- 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 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 the following:

  – 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 that 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 for which installation is intended (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")

- COL applicants referencing the AP1000 certified design will resolve generic open items and plant-specific action items resulting from NRC review of the I&C (PMS) platform. This is COL Action Item 7.1.7-1.

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

- The PRA assumes diversity that eliminates the potential for CCFs between PMS and DAS. The DAS automatic actuation signals are generated in a diverse manner than the PMS signals. The use of different architecture, different hardware implementations, and different software contributes to the diversity between the DAS and PMS.

- 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. The PRA assumes that this eliminates the potential for CCFs between automatic and manual DAS functions.

- Implementation of the DAS reactor trip function is through a trip of the control rods via the 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 DAS manual controls are included in the TS. The availability of the DAS automatic controls, 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 the PLS as represented in the PRA:

- The PLS has redundancy to minimize plant transients.

- The 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 is 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 comprising 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 provides 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 preferred power supply provides the main ac power 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 non-safety-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 CB and bus load CBs 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 consist 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 DBA. 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 2 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 the protection provided by the passive safety-related systems.

The RNS also provides a safety-related means of performing (1) containment isolation for the RNS lines that penetrate the containment, (2) isolation of the RCS at the RNS suction and discharge lines, and (3) pathway for long-term, postaccident 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 HXs.

- 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 CV 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 RNS system:

  – The portion of the RNS outside containment is capable of withstanding the operating pressure of the RCS.

  – At least three valves isolate each RNS line.

  – Interlocking of the pump suction isolation valves, which connect the RNS pumps to the RCS hot-leg, with RCS pressure prevents opening of the valves until the RCS pressure is less than 3.20 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 protects 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 the RCS.

  – 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 no open manual valves in the drainlines.

- 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 D-RAP includes the IRWST suction isolation valve (V023).

- 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 19.1.8.16-1.

- 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 19.1.8.16-2. The control room design will take into account this error. This is COL Action Item 19.1.8.16-3.

- The RNS is an important defense-in-depth system for accidents initiated while the plant is at power or at midloop during shutdown. The RNS and its support systems (CCW, SWS, and diesel generators) are important to RTNSS, 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 SWS. 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 HX.

- 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 HXs 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 CVS provides a safety-related means to terminate inadvertent RCS boron dilution and to preserve containment integrity by isolation of the CVS lines penetrating the containment. In addition, the CVS provides a non-safety-related means to provide makeup water to the RCS during normal plant operation, provide boration following a failure of reactor trip, and 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 AOVs provide isolation of normal CVS letdown during shutdown operation on low hot-leg level.
- The safety-related PMS boron dilution signal automatically realigns CVS pump suction to the BAT. 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 19.1.8.16-4.

19.1.8.20 Startup Feedwater System

The 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 HX for non-LOCA or SGTR accidents which minimizes the PRHR challenge rate. The D-RAP includes the SFW pumps.

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 design minimizes the probability of plugging by including (1) two 100-percent drains in the sidewall 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 2 years to identify and to eliminate debris that can potentially plug the drains.

19.1.8.22 Containment Isolation System

The DAS, in addition to PMS, controls CIVs 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. The D-RAP includes the CIVs controlled by the DAS as risk-significant SSCs. Short-term availability controls for the 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 system offers the following design features:

- 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 an MOV in each recirculation line, each powered from the Class 1E dc power supply, and actuated from the control room
- a reactor vessel thermal insulation system designed specifically to enhance RPV cooling, as described in Section 19.2.3.3.1.3 of this report

Included as risk-significant SSCs within the 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 for the related piping and valves.

Specific guidelines govern 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.

The ITAAC will confirm key aspects of the reactor cavity flooding system.

19.1.8.24 RPV Thermal Insulation System

The AP1000 design includes a reflective reactor vessel insulation system that provides an engineered flowpath 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. The following are key attributes of the insulation system:

- RPV/insulation panel clearances, water entrance and steam exit flow areas, and loss coefficients derived from the ULPU Configuration V tests with prototypical RPV insulation
- the entrance and exit of the insulation boundary incorporates water inlets and steam vents that open because of buoyant forces during cavity flood-up

- insulation panels and support members designed to withstand the pressure differential loading associated with the ERVC boiling phenomena, as determined from the ULPU Configuration V tests

There are no applications of coatings to the outside surface of the reactor vessel that will inhibit the wetability of the surface.

A metal grating covers the opening between the vertical access tunnel and the reactor coolant drain tank (RCDT) room. This 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 waterflow 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. This is part of COL Action Item 19.2.3.3.1.3.2-1.

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 ITAAC will confirm key aspects of the as-built system.

19.1.8.25 Reactor Cavity Design for Direct Containment Heating

The reactor cavity and RPV arrangement provide no direct flowpath 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 the following features:

- a minimum floor area of 48 m^2 (516.7 ft^2)for spreading of the molten core debris
- a minimum thickness of concrete above the embedded containment liner of 0.85 m (2.8 ft)

- no buried piping in the concrete beneath the reactor cavity and no enclosed sump drainlines in either the reactor cavity floor or reactor cavity sump concrete and thus, no direct pathway from the reactor cavity to outside the containment in the event of CCIs

- a 61 cm (24 in.) 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 avoiding a 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 system has the following features:

- 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 nonessential diesel generators, or non-Class 1E batteries via dc-to-ac inverters

- manually actuated from the control room when core exit temperature exceeds 648.9 °C (1200 °F), 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 LOCA. Although the PARs are expected to function to reduce combustible gas concentrations during severe accidents as well, the PRA does not credit them.

19.1.8.29 Protection of Containment from Diffusion Flames

The following features of containment layout prevent the formation of diffusion flames that can challenge the integrity of the containment shell:

- 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.

- 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 ITAAC will confirm the above provisions. The scope of D-RAP will also include the IRWST vents.

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 affect 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 CDF; 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 (see COL Action Item 19.2.5-1).

19.1.9 Conclusions and Findings

The NRC has evaluated the AP1000 design PRA quality and its use in the design and certification processes. The NRC concludes that the quality and completeness of the AP1000 PRA are adequate for its intended purposes, such as supporting the design and certification processes and satisfy the requirements of 10 CFR 52.47. 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 concludes that the use of PRA in the AP1000 design process helped improve the unique passive features of the design by providing a better understanding of plant response, including potential system interactions, during postulated beyond-DBAs. Such features contributed to the reduced CDF and CCFP

estimates of the AP1000 design when compared to those of operating PWRs. The 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). On the basis of this review, the NRC believes 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

The staff reviewed the quality of the PRA submittal by evaluating the models, techniques, methodologies, assumptions, data, and calculational tools that were used by the applicant. In addition, the staff reviewed the AP1000 PRA for completeness by comparing it with PRAs performed for current generation and APWR 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 on addressing issues related to these features, such as the issue of T-H uncertainties and the reliability of digital I&C software. The following discussion summarizes the resolution of the DSER open items.

19.1.10.1 Digital Instrumentation and Control (Open Item 19.1.10.1-1)

Chapter 26 of the AP1000 PRA proposes a design option for the PMS in addition to the one modeled in the PRA. The applicant proposed the option to use the Common Qualified Platform (Common Q) because of the rapid changes 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 place of the PRA PMS model, does not have any impact on the design certification process. The staff asked the applicant 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. This was Open Item 19.1.10.1-1 in the DSER.

The applicant addressed this issue by comparing the Common Q design features of the PMS to the design features of the PMS modeled in the PRA. This comparison indicates that the differences between the two options either do not affect PMS reliability or the Common Q feature will result in a higher PMS reliability. Therefore, Open Item 19.1.10.1-1 is resolved.

19.1.10.2 PRA Input to Design Certification Process (Open Item 19.1.10.1-2)

An important objective of the AP1000 design certification PRA was 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. The DCD incorporates these requirements 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. This was

designated Open Item 19.1.10.1-2 in the DSER pending completion of the staff's review of the PRA insights and assumptions.

The staff review found the proposed list of design certification requirements to be complete, consistent with important PRA assumptions, and reflective of the final resolution of the DSER open items. Therefore, Open Item 19.1.10.1-2 is resolved.

19.1.10.3 PRA Input to RTNSS Process (Open Item 19.1.10.1-3)

An important objective of the AP1000 PRA was to provide risk-informed input to design certification regarding the need for regulatory oversight of certain non-safety-related systems (RTNSS). The staff asked the applicant to use the results of the AP1000 PRA to provide input to the RTNSS process. At the pre-DSER stage of the design certification process, the applicant had identified RTNSS systems, but the staff needed additional information to determine the proper use of PRA results and insights in the RTNSS process. This was Open Item 19.1.10.1-3 in the DSER.

The staff asked the applicant to provide all steps in the process of using PRA results to identify RTNSS systems, as well as the type and level of regulatory oversight for such systems. These steps were necessary to 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. The applicant provided this information, and the staff found it acceptable. Therefore, Open Item 19.1.10.1-3 is resolved.

19.1.10.4 Impact of Uncertainties on PRA Results and Conclusions (Open Item 19.1.10.1-4)

The staff review identified two areas of uncertainty which individually, or collectively with other areas of uncertainty (e.g., uncertainty associated with failure probabilities of squib valves), could affect the PRA results and conclusions regarding the need for certification requirements, such as ITAACs, RTNSS, and COL action items. The first such area of uncertainty relates to the initiating event frequencies assumed in the PRA for large LOCAs and SGTR accidents. Sensitivity studies performed by the applicant have shown that this area of uncertainty, by itself, does not affect PRA conclusions and insights about the design (Section 19.1.3.1.5.3.3 of this report discusses the results of the sensitivity study for the assumed frequency of large-break LOCAs).

The second area of uncertainty relates to the success criteria assumed in the AP1000 PRA for passive containment cooling. Specifically, no core damage path is modeled in the PRA event trees for accidents involving steam release inside the containment when the containment is cooled by airflow alone (i.e., when the PCS water fails). The applicant recognized that accident sequences with successful emergency core cooling could lead to containment failure and, thus, core damage when the PCS water is unavailable. However, the applicant argued that containment failure is likely only for a small fraction of such sequences, and any core damage that might occur would not lead to a large release (core damage would be initiated in the long term because of loss of water from the primary system by steaming or draining from the failed containment). The staff requested more analysis to justify this argument.

The applicant analyzed the containment capability with air cooling alone (documented in Chapter 40 of the PRA) and concluded that the nominal long-term CCFP is small (about 2 percent). Thus, only a small fraction could contribute to large release. Furthermore, the applicant provided information showing that the progression of the accident to a large release is unlikely. Although failure of the containment precedes core damage in the accident sequence, core damage is not expected to begin for almost 2 days after containment failure. The staff concludes that sequences involving containment cooling by airflow alone do not contribute significantly to core damage or early release frequency, and therefore, there is no need for additional treatment of these sequences in the PRA or the RTNSS process.

The impact of these two areas of uncertainty on the results of PRA, including the PRA results in the RTNSS process was Open Item 19.1.10.1-4 in the DSER. The applicant has addressed the two areas of uncertainty acceptably. Therefore, Open Item 19.1.10.1-4 is resolved.

19.1.10.5 Success Criteria and Thermal-Hydraulic Uncertainty (Open Item 19.1.10.1-5)

The applicant identified event tree paths that do not result in core damage. 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. Section 6.2 of the PRA describes the success criteria as those conditions necessary to ensure that the following critical safety functions are maintained:

- DHR (core cooling)
- RCS inventory control
- RCS pressure control
- reactivity control
- containment heat removal and containment isolation

The discussions in this section summarize the T-H basis for success paths to ensure that the first four critical safety functions are maintained. Section 19.2.4 of this report discusses the basis for ensuring success paths for maintaining the containment heat removal and containment isolation function.

For the AP1000, the applicant listed in Table 6-1 of the AP1000 PRA the minimum sets of equipment necessary to mitigate various plant failure events at power. These are the minimum sets of equipment that ensure meeting critical safety functions. The applicant referenced its justifications for success for each case, and based many of these justifications on analyses using the computer codes employed to verify the design basis in the DCD. The NRC staff has reviewed these design-basis codes, as discussed in Section 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. The applicant based other justifications on analyses using the MAAP4 computer code, which the staff has not reviewed but which has been benchmarked against NOTRUMP results for the AP600 as discussed in WCAP-14869 “MAAP4/NOTRUMP Benchmarking to Support the Use of MAAP4 for the AP600 PRA Success Criteria Analyses,” issued April 1997. Subsequent paragraphs within this section further discuss the staff’s evaluations of the use of MAAP4 for the AP1000 PRA.

The occurrence of an ATWS event will be unlikely at AP1000 reactors since the plants will be equipped with a DAS in addition to the reactor protection system. For the PRA, the applicant performed T-H analyses of ATWS events assuming that both reactor trip actuation systems failed. The applicant analyzed a loss of feedwater event which was determined to be the limiting ATWS precursor for the AP600. The applicant utilized the LOFTRAN computer code, which the NRC staff has approved 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 -22.5 pcm/°C (-12.5 pcm/°F). For the first cycle, the analysis determined that the core moderator coefficient was in excess of -18.0 pcm/°F (-10.0 pcm/°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 the AP1000 using LOFTRAN, and the results are acceptable to use in the PRA since the applicant has used approved methodology.

DCD Tier 2, Chapter 15 describes LBLOCA T-H analyses as part of the design basis for the AP1000. The applicant performed these analyses using the WCOBRA/TRAC computer code. For the PRA, the applicant performed additional LBLOCA analysis of a double-ended cold-leg break and inadvertent opening of all four ADS Stage 4 valves. Unlike the design-basis analyses, the LBLOCA analysis assumed containment isolation to have failed. All four ADS Stage 4 valves were assumed to operate for the PRA, whereas only three ADS Stage 4 valves were assumed to operate for the Chapter 15 design-basis analyses. These analyses are acceptable for use in determining success criteria for systems and operator actions employed in the PRA.

The applicant analyzed long-term cooling following a LOCA, as discussed in DCD Tier 2, Chapter 15. These analyses also used 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. The 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 where 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 design-basis analyses these inputs are generated by the NOTRUMP and WGOTHIC computer codes. Section 21.6 of this report describes the staff review of these computer codes. For the two additional long-term cooling analyses performed for the PRA, the applicant obtained the initial conditions and other inputs to WCOBRA/TRAC 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 applicants use NRC-reviewed computer codes 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 was Item (a) of Open Item 19.1.10.1-5 in the DSER.

The applicant responded to the staff's concern by reanalyzing post-LOCA long-term cooling with containment isolation and failure of one of the four ADS Stage 4 valves. The applicant also reanalyzed the case with failure of the containment to isolate and operation of all ADS Stage 4 valves. In these analyses, the applicant utilized the WGOTHIC code and conservative hand calculations to produce input to WCOBRA/TRAC. The staff has concluded these calculations to be conservative and to properly bound the uncertainty in the T-H calculations. Therefore, Item (a) of Open Item 19.1.10.1-5 is resolved.

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 the applicant in Table 6-1 of the PRA. The applicant has supplied the additional requested information. These were Items (b), (c), (d), and (e) of Open Item 19.1.10.1-5 in the DSER.

The resolution of Items (b) through (e) are discussed below:

- The staff requested justification that an LBLOCA can be mitigated if one of the two CMTs fails (Item (b)). The applicant referred to DCD Tier 2, Section 15.6.5.4A.5, "Large-Break LOCA Analysis Results," where a sensitivity study presents the results of an LBLOCA analysis without CMT operation. This analysis demonstrates acceptable results without CMT operation. The analysis used the WCOBRA/TRAC code (see Section 21.6 of this report for the staff review of WCOBRA/TRAC). Accordingly, this issue is resolved. Therefore, Item (b) of Open Item 19.1.10.1-5 is resolved.

- The staff requested justification that adequate water can be maintained within the containment to provide for long-term core cooling if containment isolation fails (Item (c)). The applicant presented an evaluation which considered the large volume into which the break would discharge and the torturous path that liquid ejected from the break or from the ADS Stage 4 valves would have to travel before leaving the containment through a failed open vent line. The staff agrees with the applicant's conclusion that no significant liquid carryover from the containment would occur from a failed open vent line. Therefore, Item (c) of Open Item 19.1.10.1-5 is resolved.

- The staff requested justification that one of the two startup feedwater pumps can deliver adequate water to the two SGs following an ATWS event (Item (d)). The applicant performed this analysis which assumed main feedwater flow to the SGs to be lost and failure of the reactor to scram. The analysis assumed that one startup feedwater pump was assumed to feed both SGs and one CMT was assumed to be available to circulate borated water to the core. Core negative reactivity was assumed to be that which will occur at the beginning of the first fuel cycle, which is a conservative assumption. The applicant performed the analysis using LOFTRAN, which the NRC has approved for analysis of loss of feedwater transients, as discussed in Section 21.6 of this report. The analysis predicted that reactor conditions would remain within acceptable limits. Therefore, Item (d) of Open Item 19.1.10.1-5 is resolved.

- The applicant had made 12 references to AP600 PRA sections as the basis for determining success. The NRC staff requested justification for utilizing AP600 evaluations for the AP1000 (part of Item (e)). The applicant repeated the evaluations for

the AP1000. The applicant's revised calculations demonstrated that for the 12 cases success will be maintained for AP1000. The NRC staff agrees with the applicant's conclusions. Table 6-1 of the AP1000 PRA now references the results from these evaluations. This issue is therefore resolved.

- As discussed in the response to RAI 720.025, the applicant assumed that 30 minutes of core cooling is available following an SBLOCA, SG tube rupture, or transient with no CMT or accumulator injection. It based this estimate of 30 minutes on MAAP4 calculations for the AP600 and MAAP4 calculations for the AP1000 but with fewer failures. The NRC staff requested that the applicant perform appropriate calculations for the AP1000 using a computer code which the NRC staff has reviewed (remainder of Item (e)). The applicant performed the requested analysis of an SBLOCA, which assumed a 30-minute delay in actuating a single CMT. The analysis assumed no accumulator injection. The applicant performed the analysis using the NOTRUMP code which the staff has reviewed for SBLOCA analysis (see Section 21.6 of this report). These results show that the single CMT manually actuated after 30 minutes will adequately cool the core. Therefore, Item (e) of Open Item 19.1.10.1-5 is resolved.

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 a frequency high enough to impact results, while not predicted to lead to core damage by a best-estimate T-H analysis, may actually lead to core damage when the PRA models consider T-H uncertainties. T-H uncertainties and their impact on PRA models are being considered in the certification of the AP1000 design using the same approach taken in the AP600 design certification.

The applicant utilized the MAAP4 code for analysis of many of the small and medium LOCA events sequences evaluated in the PRA. The applicant used MAAP4 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 AP600 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 WCAP-14869. 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 the 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 staff has reviewed. The MAAP4

code uses a number of nonphysical models for the T-H conditions within the reactor system. Input provided by the code analyst to obtain the desired result controls these models. Therefore, MAAP4 does not provide a rigorous solution of reactor system conditions during transient and accidents. Thus, the applicant needs to confirm the results using more rigorous methods. The applicant performed the additional analyses as described in the following paragraphs.

During the AP600 PRA evaluation, the staff asked the applicant to evaluate the T-H uncertainty in the calculational results used in the PRA including those from the MAAP4 code. Rather than performing detailed uncertainty evaluations, the applicant chose to perform a set of bounding calculations using NOTRUMP and WCOBRA/TRAC. Use of an elevated core decay heat equivalent to 1.2 times the 1971 ANS standard made the calculations conservative. WCAP-14800, "AP600 PRA Thermal/Hydraulic Uncertainty Evaluation for Passive System Reliability," issued June 1997, describes these bounding analyses for the AP600. The applicant took this same approach for the AP1000. Appendix A to the AP1000 PRA describes the bounding calculations for the AP1000.

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, were originally not properly justified using a computer code reviewed by the staff. Those included the following sequences:

- Sequences that assume failure of one of the four ADS Stage 4 valves and also assume failure of containment isolation during long-term cooling. The applicant performed a long-term cooling analysis using methodology which the staff has reviewed. This analysis showed that the core will remain cooled. This was Item (f) of Open Item 19.1.10.1-5 in the DSER. The analysis was not designed to bound T-H uncertainties since it utilized best estimate decay heat and nominal passive system flow resistances. The applicant determined that it is not necessary to perform a T-H uncertainty analysis for this combination of failures since this combination is not risk significant as it has a CDF of 2E-10 or less. The NRC staff evaluated the risk significance of these event sequences and agrees with the applicant's assessment. Therefore, Item (f) of Open Item 19.1.10.1-5 is resolved.

- LBLOCA sequences that assume failure of one of two CMTs. As discussed earlier in this section, the staff identified this as Item (b) of Open Item 19.1.10.1-5 which is now resolved.

In addition to the OK sequences, other events were judged to have an uncertain outcome (UC end states) because the assumed failures 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 bounding analyses using NOTRUMP and WCOBRA/TRAC. The applicant provided in Table A.5.1.2 of Appendix A to the PRA, a listing of the UC end states and

reference to the bounding analyses demonstrating success. Not all of the sequences producing UC end states are shown to be bounded. Those sequences that 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 staff performed audit calculations for the applicant's NOTRUMP and MAAP4 analyses. The staff utilized the RELAP5 computer code, which is an advanced T-H simulation tool developed by the staff. The RELAP5 core model is somewhat more detailed than the model in NOTRUMP or MAAP4 in that a hot rod was modeled having a higher heat flux than the average core. The staff assumed the same set of failures as the applicant. The staff ran three cases. 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—7.62 cm (3 in.) hot-leg break; both CMTs fail to inject; one of two accumulators inject; complete failure of ADS Stages 1, 2, 3; manual actuation of ADS Stage 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 Stages 1, 2, 3; one of four ADS Stage 4 valves fails closed; the PRHR HX is blocked; containment isolation fails; decay heat at 1.2 times the 1971 ANS standard.

Case 3 involves the following—8.89 cm (3.5 in.) hot-leg break; one accumulator fails to inject; one of four ADS Stage 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 successes for the PRA. Furthermore, the results demonstrate the robust design of the AP1000 for SBLOCA mitigation, since even with many multiple failures, excessive core heating does not occur.

In the MAAP4—RELAP5 comparison (Case 3), both codes predicted that the core remained covered. 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 breakflow compared to RELAP5. The sudden changes in breakflow 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 utilized a systematic approach to categorizing success paths for the PRA for the purpose of minimizing the number of analyses needed to justify success. In many

cases, the applicant used the MAAP4 code to identify the limiting sequences. To justify that the limiting sequences provide for adequate core cooling, the applicant performed bounding analyses using conservative computer codes that the staff has reviewed for DBAs. In the course of the review, the staff identified some limiting sequences that were not bounded. Other sequences were not analyzed for the AP1000, but the applicant inferred success from analyses performed for the AP600. As discussed in the preceding paragraphs of this section, the previously identified open issues involving PRA success criteria and T-H uncertainty have all been resolved. Therefore, Open Item 19.1.10.1-5 is resolved.

19.1.10.6 Fire-Specific Operator Actions (Open Item 19.1.10.1-6)

The fire PRA identified two fire-specific operator actions. The first such operator action is the switching off of the electrical power for each division in case of fire to avoid spurious action of valves. The second such operator action is the manual actuation of a valve to allow fire water to reach the automatic fire suppression system in the containment maintenance floor (Fire Area 1100 AF 11300B). The staff requested the applicant to include in the DCD a COL action item to ensure proper implementation of these fire-specific operator actions. This was Open Item 19.1.10.1-6 in the DSER.

The applicant responded by including in the DCD the COL action item proposed by the staff. This is part of COL Action Item 9.5.1-4. Therefore, Open Item 19.1.10.1-6 is resolved.

19.1.10.7 Shutdown Risk Due to Vacuum Refill Operations (Open Item 19.1.10.2-1)

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 was concerned that additional risk due to vacuum refill operations was not explicitly included in the calculation of shutdown risk and that potential risk contributor to vacuum refill conditions may not be considered. This was Open Item 19.1.10.2-1 in the DSER.

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 applicant stated that vacuum refill operations do not pose an additional risk in the AP1000 for the following reasons:

- The decay heat during vacuum refill will be about 50 percent of that during drained conditions before refueling, which is already considered in the shutdown PRA.

- Although ADS Stages 1, 2, and 3 will be closed, the TS require 9 of the 10 ADS paths to be open. As a result, at least three of the four ADS Stage 4 valves will be operable instead of the two out of four during RCS drained conditions with an open RCS.

- During vacuum refill operations, both RNS pumps and support systems are required to be available by the Short-Term Availability Controls. As discussed in the AP1000 TS Bases of the Short-Term Availability Controls, the RCS is considered open if there is no visible level in the pressurizer.

- The AP1000 ERGs (ERG-SDG-2, Step 6) provide direction for the operators for a loss of RNS during shutdown conditions, and the ERG response is applicable during vacuum refill operations in Mode 5. For a loss of RNS during vacuum refill operations, the operators are immediately directed to open the ADS Stage 1, 2, and 3 valves.

- RNS provides the low-temperature overpressure protection for the plant during Mode 5 conditions (including vacuum refill operations), in accordance with TS 3.4.14. The applicant stated that the operators will receive training in brittle fracture prevention and the RCS pressure-temperature limits. The applicant added that the operators will thoroughly understand the priority to maintain the RCS overpressure protection flowpath to the RNS during low-pressure, low-temperature shutdown conditions. The applicant addressed the importance of the operators not isolating the RNS unless the hot-legs are empty as a PRA insight (DCD Table 19.59-18, insight 82).

- In the event that a leak develops through the RNS system, the RNS pumps would be stopped, and the lines would be isolated. In this situation, the ERGs require the ADS Stage 1, 2, and 3 valves to be opened.

Based on this information, particularly that vacuum refill operations are adequately covered by TS, short-term availability controls, and the AP1000 ERGs, the staff finds the applicant's justification for not explicitly evaluating vacuum refill operations acceptable. Therefore, Open Item 19.1.10.2-1 is resolved.

19.1.10.8 Dominant Shutdown Accident Sequences (Open Item 19.1.10.2-2)

The applicant did not report the dominant shutdown accident sequences in the AP1000 shutdown PRA. The staff requested the applicant report the dominant shutdown accident sequences in the AP1000 shutdown PRA. This was Open Item 19.1.10.2-2 in the DSER.

The applicant responded that its process of using cutset files from the AP600 PRA as a starting point does not allow the automatic generation of dominant accident sequences, only cutsets. The applicant did provide the top initiating event categories in the shutdown PRA that contribute 95 percent to plant CDF in Table 54-4 of the AP1000 PRA. Therefore, Open Item 19.1.10.2-2 is resolved.

19.1.10.9 Shutdown Risk Importance Analysis (Open Item 19.1.10.2-3)

The applicant's response to RAI 720.038 did not include any importance analyses (such as risk achievement worth). This was Open Item 19.1.10.2-3 in the DSER.

The applicant provided importance analyses (including risk achievement and risk worth) to the staff in Tables 54-18, 54-19, 54-20, and 54-21 of the AP1000 PRA. Therefore, Open Item 19.1.10.2-3 is resolved.

19.1.10.10 Shutdown PRA Sensitivity Studies (Open Item 19.1.10.2-4)

The staff requested that the applicant provide results of the shutdown PRA sensitivity studies (including cutsets). This was Open Item 19.1.10.2-4 in the DSER.

The applicant provided the cutsets to the four shutdown CDF sensitivity cases reported in the AP1000 PRA. Therefore, Open Item 19.1.10.2-4 is resolved.

19.1.10.11 Documentation of Shutdown Focused PRA Results (Open Item 19.1.10.2-5)

The focused PRA shutdown CDF was estimated to be 1.23E-6. Over 85 percent of the risk resulted from a LOOP during drained conditions and during nondrained 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 CCF to open of the four out of four IRWST injection MOVs. The later versions of the AP600 design and the AP1000 design changed the four MOVs to squib valves. In the AP1000 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, CCF of six out of six IRWST HP squib valves. This basic event has a failure probability of 2.6E-5. As a followup to RAI 720.38, the staff needed to understand why basic event IWX-MV-GO1 appears in the focused PRA cutsets for the AP1000 design. The staff also needed a list of basic events and their description for the AP1000 shutdown model. This was Open Item 19.1.10.1.2-5 in the DSER.

The applicant responded that it used the IWX-MV-GO1 to represent the failure mode of “CCF of 6 out of 6 IRWST HP SQUIB VALVES TO OPEN.” In the cutset files, the basic event identifier was left as is, the probability was changed to 2.6E-5 to reflect IWX-MV-GO1, and the calculations were made. Thus, the numerical results and the cutset logic were reported as intended. However, the applicant corrected the summary tables in Tables 54-10, 54-13, and 54-15 of the AP1000 PRA to show IWX-EV-SA versus IWX-MV-GO1. Also, to prevent confusion, the applicant gave the basic event descriptions in the attached cutset Tables 54-10, 54-13, and 54-15. Based on this response, the staff concludes that Open Item 19.1.10.2-5 is resolved.

19.1.10.12 Shutdown Fire Risk Evaluation (Open Item 19.1.10.2-6)

The applicant submitted the AP1000 shutdown fire risk evaluation on March 28, 2003. The AP1000 fire risk analysis has a different grouping of fire areas and different combustible loadings than the AP600 shutdown fire risk evaluation. This was Open Item 19.1.10.2-6 in the DSER.

The applicant submitted a revised shutdown fire risk evaluation on June 24, 2003, in the AP1000 PRA. This PRA contained sufficient information for the staff to derive risk insights. Therefore, Open Item 19.1.10.2-6 is resolved.

19.1.10.13 Representative Sequences for Assigning Source Terms (Open Item 19.1.10.3-1)

Chapter 45 of the PRA, "Fission-Product Source Terms," identifies and briefly describes the accident sequences used to represent the various release categories. Chapter 34 of the PRA, "Severe Accident Phenomenon Treatment," provides additional sequence information. The staff noted that the applicant did not explain the basis for selecting the representative sequence for each release category. Such information was considered necessary in order to confirm that the sequence selected to represent each release category is reasonably representative of the collection of sequences assigned to that category, in terms of the magnitude, timing, energy, and elevation of release. Based on the limited information 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 timeframe for late containment failure. This was Open Item 19.1.10.3-1 in the DSER.

In response, the applicant reconsidered the sequences used to represent each release category and provided revised sequences and source terms for each of the affected release categories and the rationale for selecting these sequences. The revised representative sequences are now consistent with the expected release characteristics for the associated release categories. Section 19.1.3.2.2 of this report reflects the updated sequence information. Therefore, Open Item 19.1.10.3-1 is resolved.

19.1.10.14 Major Contributors to System Failures (Open Item 19.1.10.3-2)

The staff noted that the applicant did not provide the major causes of reactor cavity flooding failure and hydrogen igniter failure in the AP1000. Such information is useful for identifying major contributors to system failure and confirming that reasonable measures have been taken to reduce risk. This was Open Item 19.1.10.3-2 in the DSER.

In response, the applicant provided additional information regarding the dominant contributors to failure of these systems/functions. Section 19.1.3.2.2.2 of this report reflects these contributors. Therefore, Open Item 19.1.10.3-2 is resolved.

19.2 Severe Accident Performance

19.2.1 Introduction

The purpose of Section 19.2 of this report is to evaluate the applicant's proposed approach to resolving severe accident issues for the AP1000 design and to determine whether the applicant is consistent with the guidance in SECY-93-087, SECY-96-128, SECY-97-044 and the corresponding SRMs dated July 21, 1993, and January 15 and June 30, 1997, respectively.

To adequately protect the public health and safety, current NRC regulations require conservatism in design, construction, testing, operation, and maintenance of nuclear power

plants. The NRC has mandated a defense-in-depth approach in order to prevent accidents and, if accidents should occur, to mitigate their consequences. Regulations emphasize siting in less populated areas. 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 system designs 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. DCD Tier 2, Chapters 6 and 15, document the analysis of LBLOCA and other accidents done in accordance with the NRC's standard review plan (SRP).

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 ATWS (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 the design's 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 a 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 adversely affecting the environment. However, the possibility, albeit remote, does exist for a LOCA or seemingly ordinary plant transient coupled with numerous plant failures to progress to a severe accident. The use of PRA reveals information about the potential for substantial offsite releases.

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 the three categories of small, medium, and large, depending 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, SG water level, and containment parameters within the design-bases spectrum. Of most importance is the assurance of 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 PRAs, 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 ATWS, 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 reactor protection system (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 RCPs, 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, operators must manually scram the reactor 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. The staff promulgated regulations to address ATWS 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 DCD Tier 2, Section 7.7.1.11, "Diverse Actuation System," the AP1000 has a DAS. Sections 7.7.2 and 15.2.9 of this report contain the staff's evaluation of the DAS to meet the requirements of 10 CFR 50.62. On the basis of the staff's evaluation of whether the DAS meets the requirements of 10 CFR 50.62, the staff concludes that the AP1000 design conforms to the ATWS guidance specified in SECY-93-087.

19.2.2.1.2 Mid-Loop Operation

During refueling or maintenance activities, the RCS is sometimes reduced to a “midloop” level. During this period, the potential exists for loss of DHR 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 DHR capability during all phases of shutdown activities, including refueling and maintenance. The applicant summarized the specific AP1000 design features that address mid-loop operations in DCD Tier 2, Section 5.4.7.2.1, “Design Features Addressing Shutdown and Mid-Loop Operations.” DCD Tier 2, Table 16.3-2, “Investment Protection Short-Term Availability Controls,” provides availability controls for the RNS during mid-loop operation. 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 DCD Tier 2, Table 16.3-2, the staff concludes that the AP1000 design conforms to the mid-loop operation guidance specified in SECY-93-087. Chapter 22 of this report evaluates short-term availability controls.

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., an SBO is 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 its belief 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 provided for the electrical power systems appear in DCD Tier 2, Table 16.3-2. 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 DCD Tier 2, Table 16.3-2, the staff concludes that the AP1000 design conforms to the SBO guidance specified in SECY-93-087 and is, therefore, acceptable. Chapter 22 of this report evaluates short-term availability controls.

19.2.2.1.4 Fire Protection

The Commission concluded that fire protection issues 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 on 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. DCD Tier 2, Section 9.5.1, "Fire Protection System," describes the AP1000's fire protection system. DCD Tier 2, Appendix 9A, "Fire Protection Analysis," contains the fire protection analysis. Section 9.5.1 of this report discusses the staff's acceptance of the AP1000 fire protection systems relative to the guidance in SECY-93-087.

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 guidance 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 on 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 HXs, 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 not designed to withstand full RCS pressure should have the following attributes:

- the capability for leak testing of the pressure isolation valves
- valve position indication available in the control room when isolation valve operators are de-energized
- 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 guidance 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 guidance 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. The shield building supports a 2,858-m^3 (755,000-gallon) water storage tank 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 waterflow. 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 physical and chemical processes that may occur during the progression of a severe accident, and how these phenomena affect containment performance, follows in this section. Because of the complex processes involved, the postulated core melt progression scenarios will potentially vary. 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 summarizes 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 DHR 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 CCI, FCI, and DCH.

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 the degraded core within the reactor vessel stabilizes and cools, or 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 the following:

- 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)
- 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 to the point at which damage to the fuel and fuel cladding may occur. Transfer of decay heat occurs through the radiative, conductive, and convective heat transfer to the steam, other core materials, and nonfuel 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 the 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 1757 °C (3194 °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 steamflow 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 steamflow 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—1877 °C (3410 °F) (beta-Zr), 1977 °C (3590 °F) (alpha-Zr(O)), and 2677 °C (4850 °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 1897 °C (3446 °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 occurred after the onset of Zr/UO_2 liquefaction and relocation.

Hydrogen production and accumulation during a severe accident may challenge the containment in numerous ways, including deflagration, detonation, and pressurization, as hydrogen gas is noncondensable. 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 noncoherent 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
- 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
- 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 DCH 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 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, preexisting in the containment or produced during DCH, could ignite adding to the loads on the containment. This phenomena is known as high-pressure melt ejection with DCH.

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 the following:

- pressurization as a result of the production of steam and noncondensable gases to the point of containment rupture
- the transport of high-temperature gases and aerosols into the containment leading to high-temperature failure of the containment seals and penetrations
- containment liner melt-through
- reactor support structures melt-through leading to the relocation of the reactor vessel and tearing of containment penetrations
- the production of combustible gases such as hydrogen and carbon monoxide

Many factors affect CCI, 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

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 so 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 DBAs. This section provides the results of the staff's review of the ERVC strategy for the AP1000.

The AP1000 design includes several features that enhance ERVC relative to operating plants, specifically

- safety-grade systems to provide RCS depressurization and reactor cavity flooding
- a "clean" lower head that is unobstructed by in-core instrument lines or other penetrations
- an 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. Similar to the method in 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 three 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 following sections describe the results of the review.

19.2.3.3.1.1 Likelihood of Achieving Requisite Conditions for ERVC in AP1000

Successful ERVC requires both RCS depressurization and reactor cavity flooding. Important considerations include the manner in which the PRA success criteria define these conditions, the potential for the RCS to be depressurized automatically or by manual backup of the 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 1.14 MPa (150 psig) before RCS pressure boundary challenge, and (2) flooding of the reactor cavity to a level above the reactor vessel nozzle gallery (Elevation 98') before 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. The following sections discuss each of these criteria.

19.2.3.3.1.1.1 RCS Depressurization

RCS depressurization can occur as a result of the initiating event (e.g., an LLOCA) or operation of the safety-grade ADS. In case automatic actuation of the ADS does not occur, the emergency response guidelines address manual actuation, which is 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 (less than1.14 MPa (150 psig)) at the time of core uncovery. For high-pressure core melt sequences, the Level 2 event trees further evaluate the potential to depressurize the RCS in the time period between the onset of core damage and challenge of the RCS pressure boundary. After analysis gives credit for late depressurization, an even larger fraction of the core melt sequences (about 95 percent) is 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., 1.14 MPa (150 psig) or less) is greater than the RCS pressure assumed in the baseline analysis in the UCSB study for the AP600 (the UCSB study assumed a fully depressurized RCS). However, Appendix G to the UCSB report provides a supplemental structural analysis 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 2.86 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 the AP1000 is greater than in the AP600 because of the higher decay heat level and core mass in the AP1000. The higher decay

heat level results in greater heat flux through the RPV lower head relative to the 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 the thinned RPV wall must carry. In Section 39.4 of the PRA, "Reactor Vessel Failure Criteria," the applicant assessed 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 this margin is significant, 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 can erode this margin. For example, an internal pressure differential of 6.89 kPa (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 differential of 241 kPa (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 because of the lack of steam generation and the available discharge area through the open ADS valves, and that the maximum RCS differential pressurization during reflood would be limited to about 152 kPa (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. The staff considers these assumptions 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, COL Action Item 19.2.5-1 regarding the severe accident management program will minimize the likelihood of such interactions in the AP1000. 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 the AP1000, the applicant 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 the 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 the emergency response guideline. The operator instructions to flood the cavity have been moved from the end of ERG AFR.C-1 (in the AP600) to the entry of the procedure (in the AP1000) to achieve the water depths and flooding times required for successful ERVC in the 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 one of two lines to flood the cavity within a 20-minute time window. This probability is reasonable for the 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 the applicant 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/yr to 2.6E-8/yr).

The applicant confirmed the effectiveness of reactor cavity flooding 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) typically, approximately 70 minutes or more 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 applicant's success criterion for cavity flooding. In view of this confirmation, the staff concludes that the applicant's 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, the plant achieves adequate reactor cavity flooding 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 fault tree used to quantify the failure probability of cavity flooding considers the availability of the power sources, availability of the valves, ability of the operator to diagnose the situation, and success of the operator. Since the system fault trees are linked to the CET (CET), the analysis treats the availability of power sources consistently for all sequences in the CET.

In summary, the staff concludes that the success criteria for RCS depressurization and reactor cavity flooding are appropriate and that the safety-related systems for RPV depressurization and reactor cavity flooding provide high confidence that the applicant can achieve requisite conditions for ERVC (i.e., a depressurized RCS and timely flooding of the reactor cavity) in most core melt sequences. In those events where either condition is not met, the AP1000 PRA conservatively assumes that the sequence leads to containment failure. 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 the 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. Transient forced convection and jet impingement effects dominated one configuration, and natural convection in the final steady-state dominated the other. 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 (FIBS) in the UCSB report, are fully developed natural circulation of a homogeneous oxidic molten pool in the lower head of the RPV with an overlying metallic layer, debris pool masses corresponding to relocation of essentially all of the core and most of the steel structures, a depressurized RCS, and heat transfer coefficients on the outside of the reactor vessel corresponding to a fully flooded reactor cavity.

Severe Accidents

The technical treatment in the UCSB study for the AP600 includes the following:

- 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 nonheated layers on top (the mini-ACOPO and MELAD experiments, respectively)

- 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

- 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 that 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 T-H loads associated with ERVC. The UCSB analysis of ERVC did not address the RPV pressure loads associated with late reflood of the reactor vessel.

A total of 17 internationally recognized experts in the fields of severe accidents, heat transfer, and structural mechanics peer-reviewed the UCSB report. The review identified and addressed numerous technical issues related to ERVC. The peer review comment resolution process addressed the impact of these issues on the study conclusions by performing sensitivity studies and additional evaluations to address the impact of these issues on the margins to failure. The results of the additional assessments indicated that even when analysts consider these issues, 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 the AP600, the Office of Nuclear Regulatory Research (RES) and the Idaho National Engineering and Environmental Laboratory (INEEL) undertook parallel review efforts. The review included an indepth review of the UCSB study and the model used to assess ERVC effectiveness an indepth review of the peer review comments and their resolution to identify areas where technical concerns were not addressed, and 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 also identified the following areas of concern:

- The potential exists 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 exists 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 potential exists for 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 the integral solution explicitly addressed peer reviewer concerns and additional parameter uncertainties. 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 the AP600 that reactor vessel integrity is likely to be maintained if the requisite conditions for ERVC are met. However, in view of the potential for certain hypothetical debris configurations to produce heat fluxes exceeding CHF, the staff could not rule out RPV failure for all possible core melt scenarios.

The staff assessed the applicability of these conclusions to the AP1000. The AP1000 decay heat level is higher than that for the 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 the AP1000. To offset the potential reduction in the margin to CHF, the applicant has increased the CHF value by 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 of this report, and increasing the reactor cavity flood level associated with successful cavity flooding (as discussed in Section 19.2.3.3.1.1 of this report) to ensure that sufficient water/steam flows past the RPV are achieved, consistent with the conditions

simulated in ULPU Configuration IV and V testing. The results of ULPU Configuration IV testing show that these changes can achieve up to a 30 percent increase in CHF.

The applicant's calculations 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 prototypical 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 the AP1000, Energy Research, Inc. (ERI) performed confirmatory analyses using a mathematical model for lower head thermal behavior under severe accident conditions (NUREG/CR-6849, "Analysis of In-Vessel Retention and Ex-Vessel Fuel Coolant Interaction for AP1000," August 2004). 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 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
- 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 the AP1000. The first configuration is similar to Configuration A in the INEEL study for the 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 model treated the quantities of core debris relocated into the lower plenum 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. Sensitivity analyses examining the impact of heat transfer correlations, material properties, and the mass of debris in the lower plenum found this probability to vary from 0.04 to 0.3.

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.

The applicant does not consider a thin metallic layer in Configuration I to be applicable to the AP1000 because its analyses indicate that the lower plenum debris pool will contact the lower support plate and create a thick metal layer, and 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, the applicant provided an analysis which produced results similar to those from 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, programs sponsored by the Organization for Economic Cooperation and Development (OECD), in particular, the RASPLAV and MASCA programs, have performed additional experiments relevant to in-vessel retention of molten core debris. 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 the 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 prototypical 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 depend 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 subject to considerable uncertainties.

For purposes of design certification, the staff has accepted the applicant’s 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 CCI 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 are 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-6/yr for a large release of radioactive material (as proposed in the Safety Goal Policy Statement) because of the low estimated CDF. The staff therefore concludes that the design of the AP1000 for ERVC is acceptable. The applicant's 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

19.2.3.3.1.3.1 Reactor Cavity Flooding System

The reactor cavity flooding system comprises 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 MOV and one explosive (squib) valve are 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 for the related piping and valves. The first step of ERG AFR.C-1 specifies the operator action to flood the reactor cavity. Operators would begin this step 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 emergency operating procedures (EOP). They 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.

19.2.3.3.1.3.2 Reactor Pressure Vessel Thermal Insulation System

In addition to RCS depressurization and reactor cavity flooding, several other conditions are necessary 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 prototypical 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 flowpath by debris, and (3) RPV exterior coatings do not preclude the wetting phenomena identified as the cooling mechanism in the ULPU testing. The following sections discuss each of these areas.

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. DCD Tier 2, Section 5.3.5, "Reactor Vessel Insulation," and Chapter 39 of the PRA describe the general features of the insulation system. 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 cylindrical section. It then passes through one of four steam flowpaths/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 (an approximately 9.3 m^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 buoyant covers over the outlets of the four embedded water/steam flowpaths 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

- 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; it 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 prototypical insulation), the applicant estimates that the upper limit flow rate past the RPV would be approximately 57 kiloliters per minute (kL/min) (15,000 gpm). The damper between the reactor cavity compartment and the 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 flood-up 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 reliability assurance program includes the RPV insulation system and the damper between the reactor cavity and the RCDT room as risk-significant SSCs, and the ITAAC incorporates important criteria associated with their design.

The AP1000 RPV insulation system is purchased equipment and not within the applicant's scope. The COL applicant will be responsible for completing the design of the reactor vessel insulation system. This is COL Action Item 19.2.3.3.1.3.2-1. 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. Section 39.10 of the PRA, "Reactor Vessel Insulation Design Concept," provides general design requirements for the AP1000 insulation. Information needed to complete the final design, such as the hydrostatic and dynamic load information, will come from the ULPU Configuration V test data as described below. For the AP600, the applicant 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 flowpath between the RPV and insulation, thereby enhancing convection. The tests, which evaluated CHF for a curved baffle located at various positions/spacings from the vessel, showed that a significant enhancement in CHF is possible relative to the Configuration III experiments for the AP600 (see "Quantification of Limits to Coolability in ULPU-2000 Configuration IV," CRSS-02.05.3, May 2002). These tests provide a basis for further optimizing the insulation design.

The applicant refined the AP1000 insulation design based on insights from the Configuration IV tests, and a prototypical 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 an improvement in coolability performance compared to Configuration IV and also include information on transient pressure loads which the COL applicant will need to establish the pressure loads for the structural analysis of the final insulation design. The staff noted that the applicant had 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. The staff needs this information to evaluate the margins to lower head failure for the AP1000 and the viability of the applicant's proposal that the COL applicant complete the RPV insulation design. This was Open Item 19.2.3.3-1 in the DSER.

In response, the applicant provided the ULPU Configuration V test report, which contains additional information regarding the RPV insulation design and the test results for the revised insulation design. These results include data on the pressure generated in the region between the reactor vessel and the reactor vessel insulation, and fast Fourier transform analysis of the pressure data. The data and analysis show that the pressure variations in the channel between the vessel and the insulation are on the order of ±0.5 m (±1.64 ft) of water, and the dominant frequency of the pressure variations is less than 2 Hz. In contrast, the natural frequency of the insulation system is expected to be well above 2 Hz. The COL applicant will use the pressure data from the ULPU configuration testing to determine the design loads for the insulation panels and their support structure. Section 39.10.2 of the AP1000 PRA specifies the functional requirements for the RPV insulation design. This is part of COL Action Item 19.2.3.3.1.3.2-1. Therefore, Open Item 19.2.3.3-1 is resolved.

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, the applicant evaluated of the potential for such debris to block the ERVC flowpath. On the basis of the estimate of 57 kL/min (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. A metal grating covering the opening between the vertical access tunnel and the RCDT room 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, the RPV insulation design will include a functional requirement to assure that the minimum flow area is met through each water inlet, as well as around the recirculating flow loop. The staff considers the functional requirements of the insulation design and the related system ITAAC to adequately address the potential for debris blockage of the ERVC flowpath, and therefore finds the resolution of debris blockage acceptable.

The ULPU testing included tests using prototypical RPV steel with paint applied according to the applicant paint application specifications. This paint is intended to protect the vessel's 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 wetability of the vessel external surface and increase the critical heat flux. Therefore, it is important that the applicant paint application specifications for the RPV exterior be met.

The COL applicant will be responsible for completing the design of the reactor vessel insulation system. This is COL Action Item 19.2.3.3.1.3.2-1.

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
- provide containment-wide hydrogen control (such as igniters or inerting) for severe accidents

In its SRM, dated July 21, 1993, the Commission approved the staff's position. The issue of containment combustible gas control is 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

noncondensable 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 guidance:

- 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
- 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 guidance 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

- 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

Section 19.2.3.3.1 of this report discusses the cavity flooding system. The following discusses the reactor cavity floor area and response of the concrete basemat.

The reactor cavity comprises 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 m (5 ft) wide tunnel and a 0.9 m (3 ft) wide ventilation duct connect the two volumes. A door that serves as an HVAC barrier during normal operation protects the tunnel connecting the two regions of the cavity. 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, located along the back side of the wall dividing the two compartments, is surrounded by a 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. A stainless steel plate that supports the reactor cavity drain pumps covers the sump. A number of sleeved 1.27 cm (0.5 in.) 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 25.4 cm (10 in.), which is less than the debris depth in the 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 preexisting water in the cavity, and long-term heat removal by the overlying water pool) but will not necessarily ensure it. Accordingly, the staff has relied on the 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-8/yr. 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 the applicant 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 the 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. As part of the equipment survivability analysis, Appendix D to the PRA, "Equipment Survivability Assessment," provides a MAAP4 analysis of CCI assuming a uniform debris bed with the AP1000 reactor cavity. The applicant performed these calculations 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 noncondensable 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 the applicant's Service Level C estimate (728.8 kPa (91 psig)) until even later. For a basemat composed of basaltic concrete (which maximizes concrete ablation and minimizes noncondensable gas generation), the predicted time of basemat melt-through is reduced to about 2 days, with containment overpressure failure expected some time later.

The applicant performed additional, detailed calculations which tracked the metallic and oxidic components of the in-vessel core debris separately during the release, spreading, and CCI phases, thereby allowing evaluation of concrete ablation in different regions of the reactor cavity. Appendix B to the PRA documents these calculations. The applicant assumed an initial in-vessel core debris pool configuration consistent with the final bounding state in the DOE assessment of ERVC (DOE/ID-10460) (i.e., essentially the entire inventory of core materials and steel structures, with the metal layer overlying the oxide pool). The applicant 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 evaluated were (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, the applicant used the THIRMAL code to assess the breakup 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 the 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 nonuniform 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 the AP600, in terms of the characterization of debris composition in the two regions of the cavity, were considered applicable to the 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 the 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 are 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 noncondensable 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 the applicant's Service Level C estimate (728.8 kPa (91 psig)) until even later. For a basemat composed of basaltic concrete (which maximizes concrete ablation and minimizes noncondensable gas generation), the predicted time of basemat melt-through is reduced to about 3 days, with containment overpressure 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 applicant's 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 the 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 the AP600. The core debris mass and height are greater for the 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 the AP600. The maximum height will be greater for the 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 the 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 reasonable and consistent with its expectations for the postulated failure scenarios. In judging the adequacy of the sump protection, the staff has also considered the following:

- There is a 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.

- It is likely 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 the AP1000 (NUREG/CR-6849). 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 point. The ablation rates predicted by MELCOR are considerably lower than those 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 applicant's calculations, the MELCOR calculations support the applicant's finding that basemat penetration would not occur for several days.

The staff concludes that in the event that core debris is not retained in the 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 guidance 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 the applicant 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

A 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 ADS and reactor cavity design features.

In SECY-93-087, the staff recommended that the Commission approve the general guidance 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.

The ADS is one of the major features of the AP1000 design. The ADS is an automatically actuated, safety-grade system consisting of four different valve stages that open sequentially to reduce RCS pressure sufficiently so that the PXS can provide long-term cooling. In the event that automatic actuation fails, operator action from the MCR initiates the ADS using the DAS. The ADS valves are designed to remain open for the duration of any ADS event, thereby preventing repressurization of the RCS. DCD Tier 2, Section 6.3, "Passive Core Cooling System," and Sections 5.1.3.7 and 6.3 of this report discuss the performance of the ADS for DBAs. Chapters 11, "Passive Cooling System-Automatic Depressurization System," and 36 of the PRA describe the modeling of the ADS.

The Level 1 PRA includes consideration of RCS depressurization (by automatic and manual actuation of the ADS) early in an event to prevent core damage. For those sequences that proceed to core uncovery at high RCS pressure, the Level 2 PRA further evaluates the potential to manually depressurize the RCS before the occurrence of thermally induced SGTR or HPME. Appendix D to the PRA and Section 19.2.3.3.7 of this report address the survivability of the ADS valves and related instrumentation within the early phase of a severe accident, during which late depressurization is viable. 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 (less than 1.14 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 the following additional thermal-hydraulic and probabilistic analyses:

- the likelihood of RCS piping versus SG tube overpressure failures in ATWS events
- the likelihood of containment failure from DCH pressure loads in high-pressure core melt accidents
- the relative challenge and timing of creep-rupture failures in RCS piping, hot-leg nozzles, pressurizer surge line, and SG 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-8/yr).

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)
- a ventilation shaft from the roof of the RCDT room that leads to the SG 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 airflow 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 employing the two-cell equilibrium model developed by Pilch, et al., under NRC sponsorship, which is 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 660 kPa (81 psig), which is below the applicant's estimated value for Service Level C for the 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 the AP1000, the staff judges the probability of containment

failure in the AP600 to apply to the AP1000 based on similar reactor cavity designs in the AP600 and the AP1000, similar ratios of containment volume to core debris mass (0.61 m^3/kg (9.78 ft^3/lb) for the AP1000 versus 0.66 m^3/kg (10.6 ft^3/lb) for the AP600), and higher ultimate pressure capacity for the AP1000 (e.g., the containment pressure corresponding to a 1E-3 probability of failure is approximately 756 kPa (95 psig) in the AP1000 versus 653 kPa (80 psig) in the AP600). The latter two factors would offset the effect of a higher core mass in the 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 an HPME event. These features adequately address all guidance identified in SECY-93-087 related to HPME. In the event of an RPV breach at high pressure, calculations performed by the applicant for the AP600 and applicable to the 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. This term 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 CPG. This section performs 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

DCD Tier 2, Section 19.34.2.2.1, and Section 34.2.2.1 of the AP1000 PRA, “In-Vessel Fuel-Coolant Interaction,” address in-vessel steam explosion. The applicant claimed 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 that for the AP600, and the molten core mass flow rate, superheat, and composition are expected to be “essentially the same” as that in the 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 the AP1000 DCD Tier 2 and Reference 34-3 in the AP1000 PRA), henceforth denoted as the IVR report. 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 summarizes the staff’s evaluation and conclusions presented in Section 19.2.3.3.5.1 of the AP600 FSER, NUREG-1512.

In addition to the IVR report, other reports used in the AP600 analysis include “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 include the following:

- 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, include the following:

- 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, include the following:

- 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 because of (1) a unique melt relocation scenario, (2) the bounding approach taken with regard to premixing and explosion calculations, and (3) nonintersecting 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 the 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 meltflow 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 the applicant made the staff unable to completely eliminate the downward scenario from further consideration.

Regarding quantification of premixtures (i.e., the initial condition for an energetic FCI), the staff found the applicant's method (i.e., the PM-ALPHA code) for quantifying premixtures, as applied to the AP600, to be 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 database supported the applicant's use of the PM-ALPHA code for this assessment. In particular, the staff agreed that the applicant 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 the applicant 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 the applicant, the staff found the methodology used, as applied to the AP600 and documented in DOE/ID-10503, and the analytical results to be acceptable.

Regarding structural failure criteria, the staff found the IVSE report, along with its companion reports, DOE/ID-10503 and DOE/ID-10504, to be 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 less likely to occur. In addition, although the staff did not review and approve the applicant's structural analyses, the staff believes that the safety margin is adequate to support the conclusion that, for the sideways melt release scenario, the probability of in-vessel steam explosions of sufficient magnitude to challenge the structural integrity of the AP600 lower head is sufficiently low as to be discounted from further consideration.

The applicant did not submit AP1000-specific in-vessel steam explosion analyses, but provided arguments in support of the assertion that the AP600 analyses can be extended to the AP1000. The staff did not perform an independent analysis of in-vessel steam explosions for the AP1000, nor did it perform one for the AP600. For the AP600, the staff reviewed extensive documentation of the in-vessel steam explosion analysis provided by the applicant, which supported the argument that the probability of lower head failure from in-vessel steam explosions was sufficiently low. The staff accepted the argument for the range of uncertainties associated with the late-phase core melt progression considered in the analysis. For the AP1000, the staff performed a review of the applicant's approach to the analysis of the AP1000 in-vessel steam explosions, which is based entirely on the argument of similarity between the AP1000 and the AP600. Because of a high degree of similarity between the AP600 and the AP1000 geometries, the staff believes that the range of uncertainties associated with the

physical processes involved in the in-vessel steam explosions is the 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 the AP1000.

19.2.3.3.5.2 Ex-Vessel Steam Explosion

DCD Tier 2, Section 19.34.2.2.2, and Section 34.2.2.2 of the AP1000 PRA, "Ex-Vessel Fuel-Coolant Interaction," supporting document address ex-vessel steam explosion. As stated, the in-vessel retention of the molten core debris provides the first level of defense for ex-vessel explosions. 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, the applicant claimed 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 facts that (1) the vessel failure modes are the same for both designs, (2) the initial debris mass, superheat, and composition are expected to be the same, and (3) because the AP1000 vessel lower head is closer to the cavity, resulting in less debris mass participating in the interaction with water. Therefore, the applicant concluded it is conservative to use the AP600 analysis.

DCD Tier 2, Appendix B, Reference 19.34-5, describes the performance of a structural response analysis of the reactor cavity during postulated AP600 ex-vessel steam explosions. The following summarizes the staff's evaluation and conclusions presented in Section 19.2.3.3.5.2 of the AP600 FSER.

The review was performed following the guidance given in Section J, "Containment Performance," of SECY-93-087. Therefore, within the context of the CPG, 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, RPV, and the containment liner using the TEXAS code. The applicant considered two reactor vessel failure modes—(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 (8.38 lb/sec)), localized flow of melt out of the vessel sidewall into the cavity water pool through an equivalent 6.0 cm (2.36 in.) diameter opening, while the second produces a massive flow (15,100 kg/s (33,300 lb/sec)) through a much larger opening (~100 cm (39.4 in.) diameter) caused by global creep rupture failure at the beltline (transition between the hemispherical and the cylindrical parts). Reference B-6, DOE/ID-10523, "Analysis of Melt Spreading in an AP600-Like Cavity," of Appendix B to the AP1000 PRA provides the details of each of the assumed reactor vessel failure modes. 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 RPV resulting from the impulse loads calculated for the hinged failure mode. The applicant concluded 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 was 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 the applicant'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 from ex-vessel steam explosions, the applicant used the loading associated with the hinged failure mode and found the containment capacity to have a 20 percent margin. The staff performed an independent evaluation and found the applicant's analysis to be acceptable. The staff also performed an evaluation of the reactor vessel uplift because of explosion loading and found that the uplift did not lead to containment failure.

The staff's acceptance of the applicant's containment integrity analysis during postulated ex-vessel steam explosions, performed for the AP600, was 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 CPG.

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," NUREG/CR-6849. The approach used in this study consisted 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 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 the AP600 and the 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 model of the entire reactor vessel lower head is based on the insights from the AP600 study by ERI (ERI/NRC 95-211, September 1998). The impulse loads on the reactor vessel are similar to those on the cavity wall because of the proximity of the explosion zone to both the reactor vessel and the cavity wall. A number of sensitivity studies were also performed for the AP1000. The results of the ex-vessel fuel-coolant interaction analyses for the AP1000 show that the impulse loads on the cavity wall remain below the calculated loads for the 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 the 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 the AP1000, based on the high degree of similarity between the two designs.

19.2.3.3.6 Containment Bypass

Severe accident containment bypass for the AP1000 includes (1) ISLOCAs outside containment, (2) SGTR events leading to offsite releases through the SG relief valves, and (3) containment integrity failure during a severe accident scenario. The following addresses the evaluation of design options to minimize containment bypass from SGTR events.
Section 5.4.2.3 of this report discusses containment bypass from SGTR events.
Section 19.2.2.1.5 of this report addresses ISLOCA, and Sections 19.2.3.3.7 and 19.2.6 of this report address maintenance of containment integrity during severe accidents.

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 staff identified the following design features as able to mitigate the releases associated with a tube rupture:

- a highly reliable (closed loop) SG shell-side heat removal system that relies on natural circulation and stored water sources

- a system that returns some of the discharge from the SG relief valve back to the primary containment

- increased pressure capacity on the SG shell side with a corresponding increase in the safety valve setpoints

In its July 21, 1993, SRM, the Commission approved the staff's position.

The applicant evaluated the following design options as part of its assessment of SAMDAs for the AP1000:

- A passive safety-related heat removal system to the secondary side of the SGs 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 SFW and the passive RHR HX. The applicant estimated the system to cost $1.3 million.

- Redirecting the flow from all SG 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 an SGTR event. The applicant estimated the system to cost $0.6 million.

- Increasing the design pressure of the SG secondary-side and safety-valve setpoint to the degree that an SGTR will not cause the secondary system safety valve to open would also prevent the release of fission products that bypass the containment via an SGTR. The applicant estimated the system 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 would eliminate all offsite consequences. If the baseline CDF 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 the AP1000 and the significant costs associated with the aforementioned design changes, the staff concludes that the design changes do not offer a significant reduction of risk, and that they 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 reduce the estimated CDF for SGTR sequences to about 7E-9/yr. 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 guidance 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. The applicant addressed equipment survivability in DCD Tier 2, Appendix 19D, “Equipment Survivability Assessment,” which contains general requirements and equipment classification. Appendix D to the AP1000 PRA supporting document presents the analysis performed to determine the severe accident environmental conditions.

Severe Accidents

The requirements for equipment survivability differ from those for equipment qualification. The latter requires that the safety-related equipment, both electrical and mechanical, must perform its safety function during design-basis events. DCD Tier 2, Section 3.11, "Environmental Qualification of Mechanical and Electrical Equipment," and DCD Tier 2, Appendix 3D, "Methodology for Qualifying AP1000 Safety-Related Electrical and Mechanical Equipment," 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-basis 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., a 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-basis 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 timespan 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 its position that passive plant design features provided only for severe accident 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 to 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.

Title 10, Section 50.34(f) of the Code of Federal Regulations (10 CFR 50.34(f)) provides the applicable criteria for equipment, both mechanical and electrical, required for recovery from in-vessel severe accidents:

- 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 a 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 intervening in an in-vessel severe accident. The sections of SECY-90-016 and SECY-93-087 on equipment survivability discuss the applicable guidance for mitigating the consequences of ex-vessel severe accidents.

In DCD Tier 2, Appendix 19D, the applicant discusses the NRC requirements regarding equipment survivability, various phases of accident 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 the consequences of severe accidents. The applicant had not included information regarding severe accident conditions in the DCD Tier 2. However, Appendix D to the AP1000 PRA supporting document did provide such information.

Both DCD Tier 2, Appendix 19D and Appendix D to the AP1000 PRA supporting document provide the basis for the following evaluation.

The applicant defined four phases of accident progression:

(1) Timeframe 0—Pre-Core Uncovery
(2) Timeframe 1—Core Heatup
(3) Timeframe 2—In-Vessel Severe Accident Phase
(4) Timeframe 3—Ex-Vessel Accident Phase

The applicant claimed that requirements for equipment to survive and function vary as accidents progress. During Timeframes 0 and 1, the design-basis equipment qualification program covers equipment survivability. During Timeframe 2, the equipment is designed to fulfill the recovery actions under the severe accident management strategies, while during Timeframe 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 it is intended that the operators can recover from the in-vessel severe accident and implement a safe shutdown with containment integrity maintained. The ERGs direct specific manual operator actions determined by instrumentation readings; therefore, all instrumentation should exist where manual operator actions are specified within the ERGs.

Severe Accidents

The section of SECY-93-087 on equipment survivability discusses the applicable guidance for equipment, both electrical and mechanical, required to mitigate the consequences of ex-vessel severe accidents. 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 timespan 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 it is needed to perform its intended function. In addition, 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. DCD Tier 2, Tables 19D-1 through 19D-7 summarize the results. Appendix D to the AP1000 PRA supporting document provides the severe accident environment conditions (i.e., pressure, temperature, and radiation) in which the equipment is relied upon to function.

Of particular interest is the issue of hydrogen control (i.e., maintaining hydrogen concentration in containment below a globally flammable limit). Hydrogen igniters perform this function. The ERGs require activating the igniters in Timeframe 1, even though a significant amount of hydrogen is not generated until Timeframe 2. The staff's analyses performed by its contractor, ERI, using the MELCOR computer program indicate that hydrogen burn during postulated severe accidents does not challenge the integrity of the AP1000 containment, as discussed in Section 19.2.6 of this report. That conclusion applies also to the case, presented by the applicant, of a global hydrogen burn (i.e., a burn of the 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 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 the AP1000. Therefore, the staff accepts the AP1000 hydrogen control measures as adequate.

In general, the applicant claims that the AP1000 provides reasonable assurance that equipment, both electrical and mechanical, designed for mitigating the consequences of severe accidents will perform its functions as intended. Based on the review of information provided in DCD Tier 2, Chapter 19, and Appendix 19D to the AP1000 PRA supporting document, as well as the staff's independent severe-accident analyses, the staff finds this to be 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 (Reference 19D-2), and WCAP-13914, Revision 1, "Framework for AP600 Severe Accident Management Guidance (SAMG)," issued November 1996 (Reference 19D-1), to apply directly to the AP1000 design. The staff performed an independent

comparison between the two designs, including independent analyses of the AP1000 response to various severe accident scenarios, and concurs with such an approach.

In WCAP-13914, the applicant defined 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 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 IC to a long-term heat sink, such as the PCS. 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, the applicant identified four equipment survivability timeframes. Timeframe 0 is defined as the period of time in the accident sequence after accident initiation and before core uncovery. Timeframe 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. Timeframe 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 before reactor vessel failure. Timeframe 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. DCD Tier 2, Tables 19D-3 through 19D-5 summarizes the equipment and instrumentation needed for each timeframe.

The equipment listed provides the operator with the ability to (1) inject into the RCS, SGs, and containment, (2) depressurize the RCS, SGs, 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 chosen allows the operator to confirm and trend the results of actions taken and ensures that adequate information would be available for those responsible for making accident management decisions.

The staff performed an independent assessment of the lists of equipment and instrumentation provided in DCD Tier 2, Tables 19D-3 through 19D-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 are 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

Appendix D to the AP1000 PRA supporting document discusses the severe accident environmental conditions.

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. Appendix D, Figures D.1 and D.2, of the AP1000 PRA provide

the instantaneous gamma and beta dose rates, respectively. The source term is based on the emergency safeguards system core thermal power rating of 3468 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. The applicant 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 LBB 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 RPV 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 late in-vessel release phases consistent with NUREG-1465, and, therefore, acceptable.

The applicant evaluated containment thermal-hydraulic conditions following selected severe accidents using the MAAP 4.04 computer code. The applicant analyzed five cases:

(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 igniters
(4) CCI—large LOCA with igniters, no vessel or cavity reflood
(5) GLOB—global burning of hydrogen from 100-percent cladding reaction

Appendix D of the AP1000 PRA, Table D-6, presents the timing for each case. The key elements relate to the equipment survivability timeframes, as defined above.

The staff, through its contractor, 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 CDF. Four scenarios were selected that constitute about 56 percent of the total AP1000 CDF. These scenarios include the following:

(2) 3BE—DVI line break with PRHR unavailable (29 percent of CDF)
(3) 3BR—hot-leg large-break LOCA (18 percent of CDF)
(4) 3D—spurious ADS actuation (Stages 1, 2, and 3) (9 percent of CDF)
(5) 1A—transient initiated by loss of MFW (0.6 percent of CDF)

Temperature is the most important parameter for equipment survivability. The two sets of analyses are not directly comparable because the risk-dominant scenarios, selected by the 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 the 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 is 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 the AP1000 PRA) of 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 the 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 acceptably approximate 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 guidance 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 performed this evaluation and concludes that the equipment and instrumentation identified by the applicant in DCD Tier 2, Tables 19D-3 through19D-5, and the applicable environments described in Appendix D to the AP1000 PRA supporting document, meet 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. The environmental qualification ITAAC and completion of a COL action item provide 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 timespan for which they are needed. 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 19.2.3.3.7.3-1.

19.2.3.3.8 Containment Vent Penetration

A containment vent to prevent containment overpressure failure can be used to mitigate 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 guidance, such as the Commission's CPG 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 CPG in Section 19.2.4 of this report for determining the need to include 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 the PCS. Accordingly, containment venting will not be required for the more likely severe accident sequences because they do not result in overpressure failure.

The staff identified two situations in which it would eventually require venting, specifically, events involving either failure of the 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 of this report). The baseline PRA estimates the frequency of core damage events involving failure of PCS water delivery to be about 3E-13/yr. 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-4. The AP1000 PRA does not model this failure mechanism, but the staff estimates that, given the same failure probability as assumed in the AP600, this mechanism would result in a containment failure frequency of about 2E-11/yr for the AP1000. Containment pressurization will be limited initially by PCS water delivered to the containment shell. However, following depletion of the PCS water inventory (at approximately 72 hours), containment pressure will increase and eventually exceed Service Level C because of blockage of the air cooling path.

In the event of RPV failure followed by unmitigated CCI, containment pressure (from noncondensable gas buildup) 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 of this report). The frequency of core damage with RPV failure and relocation of core debris to the reactor cavity is 5E-9/yr in the baseline PRA, assuming 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 of this report, 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 because 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-8/yr founded on the PRA for internal events, and venting would be required at 24 hours or later. This frequency could increase substantially if ERVC does not prevent RPV failure. However, even with no credit for ERVC, the frequency of events requiring venting would be on the order of 1E-7/yr, and well below the 1E-6/yr general plant performance guideline for a large release of radioactive material. The staff concludes that the CPGs regarding LRF and CCFP are met without a containment vent; therefore, a containment vent is not required for the AP1000 design.

Although containment venting capability is not required to meet the CPGs, it may be beneficial to depressurize the containment in a controlled manner under certain conditions during a severe accident. The applicant considered the impact of venting the AP1000 through penetrations with effective sizes of 10, 15, 25.4, and 45.7 cm (4, 6, 10, and 18 in.) in diameter. The results of the analysis show that overpressure failure can be successfully mitigated using any of these vent sizes. The applicant 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

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 RCS, 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, uncertainties exist regarding the performance of passive safety systems. Net driving forces are small compared to active systems. For example, the reliability and functionality of CVs can no longer be taken for granted in passive designs. While the forces developed by a pump can easily overcome a

sticking CV in an active system, there is less assurance that the low driving head developed by gravity injection in a passive design will similarly overcome a sticking CV. In addition, the parallel flowpaths 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 of a severe accident in the AP1000, 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 PXS 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 depend upon mass condensation onto cool surfaces, predominantly the walls inside containment. Given a severe accident, existing analytical tools cannot assess the long-term buildup and distribution of noncondensable gases within the containment and their effects (as a result of stratification and increasing concentration gradients within the inner containment boundary layer).

In view of the uncertainties associated with the reliance on passive systems in mitigating severe accidents, the applicant included a containment spray function as part of the AP1000 fire protection system design. DCD Tier 2, Section 6.5.2, “Containment Spray System,” describes the spray system. This design feature is not safety-related and is not credited in any accident analysis, including the dose analysis provided in DCD Tier 2, Section 15.6.5, ‘Loss-of-Coolant Accidents Resulting from a Spectrum of Postulates Piping Breaks Within the Reactor Coolant Pressure Boundary.” The existence of the Non-Safety spray system introduces additional possibility for operator intervention as part of the design’s accident management strategy.

Section 6.2.1.1 of this report evaluates the possibility of inadvertent actuations of the containment spray system.

The staff finds that the containment spray system proposed by the applicant provides the following benefits and, thereby, satisfies the staff’s recommendation in SECY-97-044:

- the capability for site personnel to quickly and substantially remove aerosol fission products following activation, upon recognition of elevated radiation levels in the containment atmosphere

- the mixing of the containment atmosphere following a severe accident, especially the boundary layer inside the containment shell

- the short-term reduction of pressure upon injection because of the heat capacity of the subcooled spray water

19.2.4 Containment Performance Goal

The CPG is intended to ensure that the containment structure has 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 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 CPG 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 CPG 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 a probabilistic CPG 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):

- The 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.
- The containment seal materials fail as a result of overtemperature.
- The molten core debris melts through the concrete basement into the subsoil.

Controlled venting of containment would not constitute containment failure, provided that venting occurs after approximately 24 hours following the 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 CDF). Each of these sequence characteristics is directly attributable to corresponding safety-grade features incorporated in the AP1000 design, and the very low contribution of SBO sequences to CDF. The peak containment pressure for these sequences would be on the order of 308 kPa (30 psig), and the long-term pressure would be on the order of 170 kPa (10 psig) to 239 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 SG tubes, FCI, and CCI. These phenomena do not contribute to containment overpressure or overtemperature 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 the reactor vessel will retain core debris, thereby preventing ex-vessel FCIs, CCI/basemat melt-through, and long-term overpressurization 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 overtemperature failure would be a concern. Finally, core damage events involving failure of containment isolation account for less than 1 percent of the total CDF in the baseline PRA.

For the less likely events in which these safety-grade systems do not operate, the Level 2 PRA assesses the probability of containment failure from the associated severe accident phenomena. Other parts of Section 19.2 of this report provide deterministic calculations of

each phenomena (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 CCIs (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 following section addresses the probability of containment failure in the context of the probabilistic CPG. Section 19.1.3.2.2 of this report further describes the contribution of the various phenomena to the overall containment failure frequency.

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 CPG.

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 overpressure 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-6/yr for a large release of radioactive material (as proposed in the Safety Goal Policy Statement) and a CCFP 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 of this report, essentially all of the containment failure frequency (99 percent) results from 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-8/yr 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 of this report, 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-7/yr. Also, modest changes in the containment failure probability distribution used in the analysis would not noticeably impact the containment failure frequency because 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, drive the bulk of the containment failures in the existing analyses.

The staff concludes that the AP1000 containment design satisfies the Commission's probabilistic CPG. Specifically, the estimated containment failure frequency in the baseline

PRA is well below the large release guideline of 1E-6/yr. The CCFP 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-6/yr. In view of the approximate nature of the CPG, 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 LRF 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. In effect, AM 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 improvements to utility accident management capabilities could further reduce the risk associated with severe accidents. 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), the need for human intervention and accident management will continue.

The nuclear power industry initiated a coordinated program on accident management in 1990. This program involves the development of (1) a structured method by which utilities may systematically evaluate and enhance their abilities to deal with potential severe accidents, (2) vendor-specific accident management guidelines for use by individual utilities in establishing plant-specific accident management procedures and guidance, and (3) guidance and material to support utility activities related to training in severe accidents. Using the guidance developed through this program, each operating plant has implemented a plant-specific accident management plan as part of an industry initiative.

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, because the utility bears ultimate responsibility for the safety of the plant and for establishing and maintaining an emergency response organization capable of effectively responding to potential accident situations. 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 must still be developed (such as the balance of plant equipment and final piping layout). The plant designer develops the technical bases for the plant-specific accident management program or plan, whereas the owner/operator develops and implements 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 decisionmaking responsibilities at a plant-specific level.

In DCD Tier 2, Section 19.59.10.5, "Combined License Information," the applicant specifies that the COL applicant will develop and submit an accident management plan. 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. The plan will address (1) accident management strategies and implementing procedures, (2) training in severe accidents, (3) guidance and computational tools for technical support, (4) instrumentation, and (5) decisionmaking responsibilities.

The COL applicant's accident management plan should specifically address all AP1000 PRA insights and COL action items that fall within the scope of accident management, including the following:

- 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 an SGTR event

  – using the containment spray system and associated water sources for containment fission product scrubbing in events with intact or vented containments

  – 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 postaccident monitoring system, MCR lighting, and the PCS recirculation pumps
  - aligning and using the PCS recirculation pumps to refill the passive containment cooling water storage tank from a mobile water source using power from the ancillary diesel generators
  - changing the MCR habitability system from air bottles to circulation using diesel-powered ancillary fans
  - making up water to the spent fuel pool and containment
  - reflooding a damaged core which is retained in-vessel

- development of guidance and procedures for actions that may need to be taken 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 decisionmaking 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 its 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. The COL applicant should develop this plan 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.

19.2.6 Conditional Containment Failure Probability Distribution

Chapter 42 of the AP1000 PRA, “Conditional Containment Failure Probability Distribution,” provides the basis for this evaluation.

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 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 the 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. Among the various containment failure modes, the two buckling failure modes are local buckling and global buckling. At Service Level C, a factor of safety of 1.67 applies to the local buckling capacity in accordance with the ASME Code Case N-284; a factor of safety of 2.5 applies to the global buckling mode in accordance with ASME Code Section III, Subsection NE, paragraph 3222. The following paragraphs evaluate the applicant's use of the factors of safety associated with the two buckling modes.

The probability distribution of containment failure is generated to evaluate containment fragility from 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 one another. Chapter 42 of the AP1000 PRA describes the limiting containment failure modes as follows:

- general yielding of the cylindrical shell
- buckling of the ellipsoidal upper head
- buckling of 16-ft-diameter equipment hatch covers
- yielding of personnel airlocks

The applicant did not develop other containment failure modes further (e.g., yielding of the ellipsoidal head, piping penetrations, mechanical penetration bellows, functional loss of containment because of ovalization of the equipment hatches), 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

DCD Tier 2, Section 3.8.2.4.2, "Evaluation of Ultimate Capacity," presents the evaluation of ultimate capacity of the AP1000 containment. In this section, the applicant evaluated the containment capacity at the 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 psi) at 149 °C (300 °F), and

the capacity of the equipment hatch covers is 558 kPa (81 psi) at 149 °C (300 °F) using ASME Code Section III, Subsection NE 3222. Using Code Case N-284, the applicant determined the capacity of the equipment hatch covers to be 834 kPa (121 psi) at 149 °C (300 °F). The staff has always maintained that the provisions of Code Case N-284 apply only to local buckling cases. The equipment hatch cover buckling is a global buckling phenomenon, and therefore the use of Code Case N-284 is not appropriate. The Service Level C capacity of the AP1000 containment structure should be the lowest value, 558 kPa (81 psi) at 149 °C (300 °F). In Section 42.3.1 of the PRA, the applicant stated, "The 90 psig [621 kPa] is the Service Level C containment failure pressure at 300 °F." The staff did not agree with this assessment, and asked the applicant to address why 558 kPa (81 psi) at 149 °C (300 °F) is not the limiting severe-accident pressure for the AP1000 containment. This was Open Item 19.2.6-1 in the DSER.

The applicant responded to this open item by a letter dated July 31, 2003, and addressed it in Section 42.3.1 of the PRA report, "Median Values for Containment Failure," which provides the technical basis for concluding that the requirements of 10 CFR 50.34 and the guidance of SECY-93-087 are satisfied.

The 10 CFR 50.34(f)(3)(v)(A)(*1*) criteria require the following:

> Containment integrity will be maintained (i.e., for steel containments by meeting the requirements of the ASME Boiler and Pressure Vessel Code, Section III, Division 1, Subarticle NE-3220, Service Level C Limits, except that evaluation of instability is not required, considering pressure and dead load alone during an accident that releases hydrogen generated from 100 percent fuel clad metal-water reaction accompanied by either hydrogen burning or the added pressure from post-accident inerting assuming carbon dioxide is the inerting agent.

In the absence of buckling, tensile hoop membrane stress due to internal pressure controls failure of the containment shell. This pressure capacity, based on Service Level C limits, is 808 kPa (117.2 psi), compared to the applicable maximum calculated pressure of 620 kPa (90 psi).

However, SECY-93-087 requires satisfaction of Service Level C limits, including consideration of structural instability, for the more likely severe accident challenges. In this case, the pressure capacity is 558 kPa (81 psi) and is controlled by the buckling of the equipment hatch covers, calculated in accordance with Subsection NE-3220. This capacity just meets the predicted pressure at 24 hours following the onset of core damage for the more likely severe accident challenges. The staff reviewed this information and concurs with the applicant's conclusion that the requirements of 10 CFR 50.34 and the guidance of SECY-93-087 are satisfied. Therefore, Open Item 19.2.6-1 is resolved.

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 because it can represent the statistical variation of many material properties well, provided that one is not primarily concerned with extreme tails of the distribution. The engineering calculations to determine the strength of the containment are multiplicative because 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 the following:

$$P = P_m \cdot M \cdot S$$

where

- P_m is the median pressure capacity representing the internal pressure level for which there is a 50-percent probability of failure
- 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
- 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 resulting from the product of several other random variables, a lognormal distribution represents the pressure capacity well. 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, employing the expected material yield stress to arrive at the median values of the containment failure pressure (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 four sources of uncertainty that can influence the median value of the CFP, 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 of the geometric property to the CFP. 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 (see L. Greimann and F. Fanous, “Reliability of Containments under Overpressure,” Pressure Vessel and Piping Technology, 1985, pages 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 to be acceptable.

In its previous reviews of standard designs, the staff has found modeling uncertainties to have a significant effect in the probability of the containment structure failure. NUREG/CR-2442 recommends a coefficient of variation (COV) of 0.12 for all practical instances of modeling error. The applicant has used a value of 0.12 for the consideration of structural uncertainty; therefore, 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) L. Greimann and F. Fanous (see above) and (2) "Development of a Probability Based Load Criterion for American National Standard A58," National Bureau of Standards Special Publication 577, U.S. 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. Because design and construction errors can lead to structural deficiencies, 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 before placement in service. The applicant did not explicitly consider uncertainty because of construction and design error in developing its containment fragility curves. The approach used by the applicant is consistent with the current practice and is acceptable.

19.2.6.4 Containment Fragility Evaluation

As discussed in Section 19.2.6.1 of this report, 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 psi) at 166 °C (331 °F) and 0.93 MPa (135 psi) at 204 °C (400 °F) using realistic material property and nominal design thickness. Therefore, the staff finds the median capacity value to be 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 1.15 MPa (166 psi) at 166 °C (331 °F) and 1.1 MPa (159 psi) at 204 °C (400 °F) using realistic material property, nominal design thickness, and appropriate analytical methods for the prediction of buckling. Therefore, the staff finds the median capacity value to be 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 1.46 MPa (211 psi) at ambient condition, as discussed in DCD Tier 2, Section 3.8.2.4.2.3, "Equipment Hatches." Section 42.4.3 of the AP1000 PRA, "Equipment Hatches," shows that a factor of 1.5 was used as a multiplier to the calculated buckling pressure at the 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 because of 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 psi) at 166 °C (331 °F) and 2.05 MPa (297 psi) 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 considered that the use of the multiplier of 1.5 was not justified. Consequently, the staff did not agree with the values shown in Tables 42-1 and 42-2 of the PRA. This was Open Item 19.2.6-2 in the DSER.

The applicant responded to this open item by letters dated July 8, 2003, and September 19, 2003, which provided the technical justification for use of the 1.5 factor to estimate the median buckling pressure capacity. The applicant's response inferred that the 1.5 factor is applied to the lower bound prediction from ASME Code Case N-284. The staff understands that the Code Case N-284 prediction is the classical buckling pressure prediction times the capacity reduction factor to account for the imperfection sensitivity determined from tests on spherical steel caps. In this case, the reduction factor is less than 0.2. Therefore, the estimated median buckling pressure is less than 0.3 times the classical buckling pressure prediction. However, the first response was not clear, because it did not clarify that the tests on spherical caps were related to the development of the Code Case N-284 capacity reduction factor, and that the prediction calculation was not based on the BOSOR-5 model. In order to more clearly and concisely present the derivation of the median capacity, the applicant revised its response to this open item in its second letter dated September 19, 2003. The staff also reviewed the applicant's calculations to confirm that the use of the 1.5 multiplier factor to derive the median value of buckling capacity of the equipment hatch cover is based on the Code Case N-284 capacity. The staff concluded that the applicant has provided sufficient basis to support the determination of the containment buckling capacity. Therefore, Open Item 19.2.6-2 is resolved.

19.2.6.4.4 Yielding of Personnel Airlocks

The applicant estimated the failure pressure of the personnel airlock to be at least 2.07 MPa (300 psi). Therefore, the applicant considers the contribution of the personnel airlocks to the CCFP to be negligible. The staff agrees with this assumption because the capacities of the personnel airlocks far exceed 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 psi) 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, the staff asked the applicant to revise Chapter 42 of the PRA to clarify the approach used by the applicant. This was Open Item 19.2.6-3 in the DSER.

The applicant responded to this open item by a letter dated July 7, 2003, and addressed it in Section 42.4.3 of the PRA, which clearly states that the contribution to the CCFP from each equipment hatch is taken as independent. This is acceptable to the staff; therefore, Open Item 19.2.6-3 is resolved.

19.2.6.6 Conclusions

Using the lower value of 558 kPa (81 psi) at 149 °C (300 °F) as the deterministic capacity of the containment structure, the probability of failure is less than 9.6E-5.

Therefore, the staff concludes that the analysis methodology and the procedures used by the applicant 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, that concerns about shutdown operations should be addressed satisfactorily before it issues the final design approval on the ALWR. 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 apply to the plant design. The assessment should include the following:

- 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)

- 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 staff's review ensures 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 the areas of outage planning and control, fire protection, and instrumentation. The staff reviewed design improvements to ensure that they appropriately address insights from shutdown operation experiences, reduce the likelihood of core damage, and enhance public health and safety. The staff also evaluated vulnerabilities that may result from new design features (i.e., DHR 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 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, Appendix 19E. The following sections of this report discuss these features.

19.3.2.1 Decay Heat Cooling System

The AP1000 design includes a redundant RNS, which is used to perform normal plant cooldown. DCD Tier 2, Section 5.4.7, "Normal Residual Heat Removal System," discusses the detailed RNS design. The RNS is a non-safety-related, defense-in-depth system that consists of two mechanical trains of DHR. Each train, located in the auxiliary building, includes a pump, a HX, and the system piping and valves. 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, a passive safety-related injection system, using the IRWST, that injects water into the RCS via the DVI line provides an alternate core cooling capability. As discussed in DCD Tier 2, Section 6.3, "Passive Core Cooling System," and Appendix 19E, the accumulators, the CMTs, and the PRHR can also provide alternative core cooling capabilities.

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 the pressurizer water level is reduced. Because the RCS temperature and pressure and the low steamline pressure signals are blocked in Mode 3 before cooling and depressurizing the RCS, the actuation of the CMTs during a loss of inventory event relies on a

low-pressurizer-level signal in Modes 3 through 5. In Mode 5, with the RCS open for reduced inventory operations, the low-pressurizer-level signal is blocked before draining the RCS; therefore, the CMTs are not available, and the RCS makeup is provided by the IRWST.

The PRHR is available for DHR in Modes 1 through 5 with the RCS intact. A CMT actuation signal triggers the PRHR. In Modes 5 and 6 with the RCS open, feeding water from the IRWST and bleeding from the ADS provides DHR.

In DCD Tier 2, Section 16.1, "Technical Specifications," the TS 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 included insights from DCD Tier 2 Appendix 19E, which indicate 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, and 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 reserve auxiliary transformer provides a maintenance source.

- Two non-safety-related onsite standby diesel generators are furnished with their own support subsystems.

- A Class 1E dc power and UPS 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 design features into the AP1000 that address issues related to low-power and shutdown operations, especially during mid-loop operations. These design features include (1) the RNS self-venting path, (2) the RCS loop piping offset, and (3) the RNS step-nozzle connection. The shutdown operation discussions of the AP1000 design integrally describe these design features.

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 (midloop) 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. Air entrained in the RNS piping may also

hinder the ability to provide adequate shutdown cooling during midloop 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 midloop operation; 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)

For nozzle dam installation, 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 in existing operating plants. The AP1000 RCS hot-legs 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 midloop operation. In DCD Tier 2, Chapter 16, Table B 3.0-1, the TS specify that ADS Stages 1, 2, and 3 valves be open and Stage 4 valves be operable, with the reactor vessel upper internals in place, whenever the CMTs are blocked during shutdown conditions. In accordance with Items 10.c and 22.c of TS Table 3.3.2-1, the IRWST injection valves and ADS Stage 4 valves must 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 DHR; they also allow the IRWST to inject water into the RCS following a sustained loss of DHR. 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 midloop operation because of air entrainment. The availability of the ADS for RCS venting also 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 to no greater than 5 percent, should a vortex occur, while continuing to provide decay heat cooling. The applicant relied on the test data and analysis included in the test report, APWR-0452, "AP600 Vortex Mitigation Development Test for RCS Mid-Loop Operation," dated September 1988, 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.

The staff requested, via RAI 440.122, that the applicant justify how APWR-0452 applies 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. Because 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 exceeds the predicted critical vortexing level. In addition, 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. Because 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 applies to the step-nozzle design for the AP1000. Therefore, the staff concludes that a step-nozzle improves 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 DHR 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,"Containment Systems," 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-resistant barriers will have a design pressure equal to the containment design pressure of 508 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 exceeds 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, “Spent Fuel Pool Cooling System,” 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 five piped connections to the refueling cavity at levels below that which 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 that the spent fuel cooling system is unavailable, the heat capacity of the water in the pool provides spent fuel cooling. 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 HX, 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 includes the piping, valves, and instrumentation necessary for system operation.

Either train of equipment can operate independently of the other train to perform any of the functions required of the spent fuel pool cooling system. One train continuously cools and purifies 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 HX. 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. Section 9.1.3 of this report provides an evaluation.

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 to temporarily isolate fluid systems) can lead to a rapid nonisolable loss of reactor coolant. In RAI 440.123, the staff requested the applicant to 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 TS identify when the various portions of passive safety systems must 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) 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 an RCS pressure of 275 kPa (40 psia), compared to that of the AP600 pressure of 221 kPa (32 psia). The staff requested the applicant, via RAI 440.110, 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 was consistent with the approach used in the AP600 loss of RNS cooling analysis presented for the AP600 in WCAP-14837, Revision 3.

  The initial conditions were assumed to be at Mode 5 with the RCS open through the ADS Stages 1 through 3 valves. Following the loss of RNS cooling, the RCS pressure increases. During the transient, operator action is credited to manually open the ADS Stage 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 operator action and the associated time is consistent with Item 10.c in DCD Tier 2, Chapter 16, TS Table 3.3.2-1, which specifies CMT actuation when the RCS water decreases to the bottom of the hot-leg; therefore, the assumption is acceptable.

The result of the analysis shows that the maximum pressure is 303 kPa (44 psia). The applicant revised the design pressure for the SG nozzle dam from 276 kPa (40 psia) to 345 kPa (50 psia). Because 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 resulting from the loss of RNS cooling event for the AP1000, the staff concludes that the revised design pressure for the SG nozzle dam is adequate and acceptable.

- The AP1000 design eliminates the use 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 in-core system with penetration through the top head, rather than the bottom head.

- The AP1000 design also eliminates temporary plugs related to the ex-core detectors. Current plants remove the ex-core detectors from above the ex-core 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 ex-core instrumentation to be inserted from below the ex-core housings.

- The AP1000 has a 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 in 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 TS (DCD Tier 2, Chapter 16, Table B 3.0-1) to be available; 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 a fixed in-core system, and a 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 the COL applicant to prepare plant procedures for each plant. However, the COL applicant was requested to develop plant-specific guidelines that would reduce the potential for loss of RCS boundary and inventory when using freeze seals. The DCD did not specify this COL information. This was Open Item 19.3.3-1.

In response to DSER Open Item 19.3.3-1, the applicant stated in a letter dated July 1, 2003, that it will add the required COL information in DCD Tier 2, Section 13.5. Specifically, it stated

that "... [i]f freeze seals are to be used, the Combined License applicant must develop plant-specific guidelines to reduce the potential for loss of RCS boundary and inventory when they are in use." The staff confirmed that the applicant added the required COL information to DCD Tier 2, Section 13.5. This is COL Action Item 19.3.3-1. Therefore, Open Item 19.3.3-1 is resolved.

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. The operator must also 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 I&C systems in DCD Tier 2, Section 19E.2.1.2.2, "RCS Instrumentation," and the response to RAI 440.121 in a letter dated October 2, 2002. The following sections discuss the staff's evaluation.

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 channels are independent of one another. One level tap connects 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 MCR. These channels generate the alarms on the low hot-leg water level. They also provide signals for protection functions, including (1) isolation of letdown on the low-level signal (in accordance with Item 28.a of DCD Tier 2, Chapter 16, TS 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 the ADS Stage 4 valve on the 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 ADS Stage 4 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 it designed the accuracy and response time of the hot-leg level instruments to be consistent with the standard ESF actuation discussed in DCD Tier 2, Section 7.3, "Engineered Safety Features." The staff requested, via RAI 440.126, that the applicant address concerns of noncondensable gases in the water level instrument, discussed in NRC Information Notice (IN) 92-54, "Level Instrumentation Inaccuracies Caused by Rapid Depressurization." In a letter dated October 2, 2002, the applicant responded, stating that the layout of the instrumentation lines address issues relating to NRC IN 92-54. In addressing issues related to noncondensable gases, the hot-leg level instrument lines slope downward 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, low levels of dissolved gases are present in the fluid in the instrument lines; thus, the quantity of the noncondensable gases which could be released is small. Therefore, the noncondensable gases do not significantly affect the accuracy of the hot-leg level measurement during the period of the intended use.

DCD Tier 2, Section 19E.2.1.2.4, "Improved RCS Draindown Method," discusses the controlled manner by which draining the RCS to mid-loop condition is achieved in the AP1000. DCD Tier 2, Section 19E.3.1.3.5, "Reduced-Inventory Operations," discusses the low RCS drain rates to which the reduced inventory operations are limited. 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 midloop operation. Therefore, the reliability of an accurate level indication is high. The offset design of the AP1000 RCS hot-leg and cold-leg piping also provides additional margin for midloop operation as compared with the hot-leg centerline.

As shown in DCD Tier 2, Figure 19E.2-1, the AP1000 includes a non-safety-related independent pressurizer level transmitter that provides water-level indication during startup, shutdown, and refueling operations. 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 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 the aid of the pressurizer level indication, reduce the potential for loss of RNS from air entrainment into the pump suction during midloop operation. The low hot-leg-level signal and automatic isolation prevents the operator from overdraining 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 in-core thermocouples used to measure RCS temperature. The in-core thermocouples 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 wide-range hot-leg RTDs measure the RCS temperature. 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 midplane 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 midloop operations, the wide-range RTDs provide a backup indication of the RCS coolant temperature when the RNS is operating, because the RNS HX 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 in-core thermocouples are used in the current operating PWRs for RCS temperature measurement. Therefore, the staff concludes that they are an acceptable 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 RNS performance. As described in DCD Tier 2, Section 5.4.7, the system parameters monitored for system performance include (1) RNS pump flow/discharge pressure, (2) RNS HX 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, “RNS Pump Evaluation and NPSH Characteristics,” the AP1000 RNS pumps are located at the lowest elevation in the auxiliary building in order to maximize the available 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 the applicant to discuss the NPSH requirements for the RNS pumps. In a letter dated October 2, 2002, the applicant responded 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 the capability to operate during most midloop conditions without throttling the RCS flow. If the RCS is at the midloop 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 time needed to uncover the core following an extended loss of residual heat removal capability significantly influences the safety margin that is available during these modes of operation. 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 the reactor vessel head, the number and size of openings in the cold-legs, the existence of hot-leg vents, and the availability of alternate methods of DHR in case of a loss of DHR systems. The applicant discusses the TS provisions, including specifications for shutdown operations in DCD Tier 2, Section 16.1. DCD Tier 2, Chapter 16, TS Table B 3.0-1, summarizes the shutdown specifications. For events that occur in Mode 4, safe shutdown, the TS 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 Stages 1, 2, and 3 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. Because the safety analysis, discussed in Section 19.3.6 of this report, assumes the TS LCOs for shutdown operations, and the results of the analysis are acceptable, the staff concludes that the shutdown TS are acceptable. However, the TS do not include the RNS in the AP1000 in shutdown modes.

The requirements of 10 CFR 50.36 specify the contents of the TS. 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, (2) a process variable, design feature, or operating restriction that is an initial condition of a DBA or transient analysis that either assumes the failure of, or presents a challenge to, the integrity of a fission product barrier, (3) an SSC that is part of the primary success path and which functions or actuates to mitigate a DBA or transient that either assumes the failure of, or presents a challenge to, the integrity of a fission product barrier, and (4) an SSC which operating experience or probabilistic safety assessment 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 the PRA has shown to be significant to public health and safety (criterion 4)). 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 Systems 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.

WCAP-15985, Revision 1, "AP1000 Implementation of the Regulatory Treatment of Non-Safety-Related Systems Process," issued April 2003, discusses the applicant's evaluation of the RTNSS implementation. 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 onsite 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 does not meet any of the criteria specified in 10 CFR 50.36(c)(2)(ii), 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)

In DCD Tier 2, Section 19E.4, "Safety Analyses and Evaluations," the applicant discussed applicable DCD Tier 2, Chapter 15, non-LOCA and LOCA transients postulated to occur in shutdown operations. 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 ESFs on plant transient responses, 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. In DCD Tier 2, Sections 15.1.1, "Feedwater System Malfunctions That Result in a Decrease in Feedwater Temperature," and 15.1.2, "Feedwater System Malfunctions That Result in an Increase in Feedwater Flow," discuss the analyses of the feedwater system malfunction initiated from Modes 1 and 2. The protection and safety monitoring system provides protection against feedwater system-induced cooldown events 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 becomes less severe as the power level decreases. 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. In addition, 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 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.

- 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 increased power because of the effects of the negative moderate coefficient of reactivity. DCD Tier 2, Section 15.1.3, "Excessive Increase in Secondary Steam Flow," discusses the excessive load increase event, initiated from full-power conditions. 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 a simple steam release, because there can be no load when the turbine is offline 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 cases initiated from full-power conditions bound the excessive load events at low powers and shutdown modes. 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 (DCD Tier 2, Section 19E.4.2.3)

The steam released from a steamline break (SLB) causes a decrease in the RCS temperature. 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 posttrip core with the most reactive rod cluster control assembly (RCCA) stuck in the fully withdrawn position, leading to high local power levels and causing the concern of low DNBRs. In DCD Tier 2, Sections 15.1.4, "Inadvertent of Steam Generator Relief or Safety Valve," and 15.1.5, "Steam System Piping Failure," the applicant showed that if the event occurs in Mode 2, it results in a more severe posttrip transient than that initiated from Mode 1, because the decay heat level for Mode 1 is higher and reduces the effect of cooldown.

An SLB initiated from Modes 3 and 4 is not worse than that from Mode 2, because the pressure, temperature, and steamflow through the affected SG are less limiting. Automatic safeguard 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 TS 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 RNS not cooling the RCS (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. DCD Tier 2, Section 15.1.6, "Inadvertent Operation of the PRHR Heat Exchanger," discusses the analysis of this event for Modes 1 and 2. The PRHR HX heat transfer rate is a function of the HX's inlet temperature and flow rate. The 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 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, before blocking the safeguards signals, the RCS is borated to the shutdown margin requirements at cold shutdown (93 °C (200 °F)) (in accordance with Note (a) to Item 1 of TS 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)

DCD Tier 2, Section 15.2, “Decrease in Heat Removal by the Secondary System,” discusses the consequences of a decrease in heat removal by the secondary system in Modes 1 and 2. The events analyzed include (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. Rapid reductions in the heat removal capability of the SGs characterize these events. 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.

An inadvertent MSIV closure or loss of condenser vacuum event may occur during Modes 2 through 4, because the plant may dump steam to the condenser to remove decay heat in these modes of operation. The turbine trip analysis from full power bounds their transient responses because the power mismatch is low. The SGs can remove decay heat through SG safety valves, which are available through Mode 4 (in accordance with TS LCO 3.7.1), and the PRHR HX can also removed decay heat through Mode 5 with the RCS intact (in accordance with TS LCOs 3.5.4 and 3.5.5.)

Severe Accidents

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 Modes 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 2, Section 19E.4.4)

DCD Tier 2, Section 15.3, "Decrease in Reactor Coolant System Flow Rate," discusses the consequences of a decrease in RCS flow in Modes 1 and 2. The events analyzed include (1) partial loss of forced RCS flow, (2) complete loss of forced RCS flow, (3) RCP shaft seizure, and (4) RCP 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. DCD Tier 2, Section 15.4.2, "Uncontrolled Rod Clusters Control Assembly Bank Withdrawal," discusses the analysis of this event for Mode 2. The analysis used the most limiting operating conditions specified by the TS to bound the event from Modes 2 through 5. The assumptions related to the limiting operating conditions include (1) crediting the power range (low setting) high neutron flux for the reactor trip to delay the trip, (2) crediting the flow from three RCPs to calculate the minimum DNBR, and (3) using the RCS temperature at Mode 2 to calculate the minimum DNBR and core kinetics feedback.

LCO 3.3.1 of the AP1000 TS specifies the operation of the source-range high neutron flux trip in Modes 3, 4, and 5 when the reactor trip breakers are closed. If the reactor trip breakers are open, then an 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 for the power range (low setting) high neutron flux, instead of the source-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 concludes that the assumption is acceptable.

LCO 3.4.4 of the AP1000 TS specifies the operation of all four RCPs 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 TS, 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 determines that this is a conservative assumption because it results in a lower calculated DNBR. Therefore, the staff concludes that the assumption is 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)

DCD Tier 2, Section 15.4.2, discusses the analysis for this event. This event does not apply to Modes 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 RCCAs, and (3) withdrawal of a single RCCA. DCD Tier 2, Section 15.4.3, “Rod Cluster Control Assembly Misalignment (System Malfunction or Operator Error),” discusses the analyses of these events for full-power conditions. 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 misaligned RCCA events will not result in any power transient in the absence of a critical neutron flux. In addition, LCO 3.1.1 of the AP1000 TS 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, which specifies the operation of four RCPs in Modes 1 and 2. Startup of an inactive RCP while in any of the subcritical modes will have a relatively small effect upon the core temperature because there will be little 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. DCD Tier 2, Section 15.4.6, "Chemical and Volume Control System malfunction that Results in a Decrease in the Boron Concentration with Reactor Coolant," provides the analyses of the boron dilution event in Modes 1 through 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, "Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position," for Mode 1 at full-power conditions bound the results for lower power, 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 TS specifies the maintenance of an 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)

DCD Tier 2, Section 15.5.1, "Inadvertent Operation of Core Makeup Tanks During Power Operation," discusses the analysis of the inadvertent actuation of the CMTs, which is performed with the plant initially in full-power conditions (Mode 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 water will not overfill the pressurizer, and the release of water loss from the pressurizer safety valves will not occur. When the reactor is at part power or in the subcritical modes, the amount of the stored energy and decay heat will be significantly reduced, and the full-power case bounds the increase in water inventory in the pressurizer.

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. Decay heat removal through the PRHR HX counteracts the expansion. 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. DCD Tier 2, Section 15.5.2, "Chemical and Volume Control System Malfunction That Increases Reactor Coolant Inventory," discusses the analysis of CVS malfunction, performed with the plant initially in Mode 1. In the full-power analysis, a worst combination of makeup boron concentration, reactivity feedback conditions, and plant system interactions is used for the limiting case. For the full-power 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, which 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 which causes an "S" signal for the full-power cases do 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 requires isolation of CVS on the high-2 pressurizer-level signal when the plant is in Modes 1 through 3, and Mode 4 before 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 full-power case bounds the events initiated from operations at shutdown modes. In Modes 4 through 6 when the RNS is in operation, the RNS relief valve provides low-temperature overpressure protection (LTOP) of the RCS pressure boundary. DCD Tier 2, Section 5.2.2, "Overpressure Protection," and Section 5.2.2.2 of this report, include a discussion of the LTOP analysis.

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)

DCD Tier 2, Section 15.6.1, "Inadvertent Opening of a Pressurizer Safety Valve or Inadvertent Operation of the ADS," discusses the analysis of inadvertent opening of pressurizer safety valves or ADS valves with the plant initially at full-power conditions. 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)

DCD Tier 2, Section 15.6.2, "Failure of Small Lines Carrying Primary Coolant Outside Containment," discusses the analysis of radiological consequences for breaks of small lines carrying primary coolant outside containment. 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)

DCD Tier 2, Section 15.6.3, "Steam Generator Tube Rupture," discusses the analysis of the SGTR events with the plant initially at full-power conditions. 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 (which are the major factors affecting dose releases) are less limiting. In DCD Tier 2, Section 15.6.3, the applicant indicated that an analysis at full power is performed to demonstrate the margin to SG overfill and thus assures that the SG safety valves can reset after opening. The dose calculations for the SGTR event are based on the assumption that the SG safety valves will reset after opening.

The applicant indicated, 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 the 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. The staff requested, via RAI 440.185, that the applicant perform an analysis to show the adequacy of the AP1000 design for SG overfill prevention during an SGTR event in shutdown modes. The analysis should include the limiting cases of (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 °C (420 °F), the initial pressure of 13.2 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 7.0 MPa (1000 psig) is the maximum expected RCS pressure that may exist when the RCS temperature is at 157 °C (350 °F).

The results of the analysis show 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 are consistent with lower modes of operation, and the results show that the DCD results for the SGTRs at full-power conditions bound the consequences of the SGTR events, the staff concludes that 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)

DCD Tier 2, Section 15.6.5, “Loss-of-Coolant Accidents Resulting from a Spectrum of Postulated Piping Breaks Within the Reactor Coolant Pressure Boundary,” discusses the analyses of LOCAs performed with the plant initially at full-power conditions. With other parameters being the same as those 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 7.0 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, which addresses LOCA analyses initiated from full-power conditions. DCD Tier 2, Section 15, demonstrates that the AP1000 provides 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 break, which is identified in DCD Tier 2, Section 15.6.5.4A, “Large-Break LOCA Analysis Methodology and Results,” 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 TS once the pressurizer pressure has been reduced to less than 7.0 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 7.0 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 7.0 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 nonlimiting relative to the DCD Tier 2, Section 15.6.5, analyses because the accumulators remain available. The analysis used the required 10 CFR Part 50, Appendix K decay heat and the TS maximum peaking factors (or the core operating limits report)

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. In addition, 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 the RNS cooling event. The applicant stated in DCD Tier 2, Section 19E4.8.1, that the results of the loss of RNS for the AP1000 plant are similar to the AP600 plant response because the RNS design and the availability of the accident mitigating system components in shutdown modes are the same for both the AP600 and the AP1000. However, the staff noted that the licensee performed no analysis of the loss of RNS cooling event for the AP1000. The staff requested, via RAI 440.119, that the applicant provide an analysis demonstrating that the equipment available during shutdown, as prescribed by the AP1000 TS, are sufficient to protect the plant from a loss of RNS cooling event during shutdown. In a letter dated December 2, 2002, the applicant provided the results of the requested analysis in DCD Tier 2, Sections 19E.4.8.2, “Loss of Normal Residual Heat Removal

System Cooling in Mode 4 with Reactor Coolant System Intact," and 19E.4.8.3, "Loss of Normal Residual Heat Removal System Cooling in Mode 5 with Reactor Coolant System Open," for the staff to review. The analysis calculated the plant responses for 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 LOOP, 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 losses 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 Modes 4 and 5 with RCS intact, the analysis used an initial decay heat corresponding to the decay heat level at 4 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 3.2 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 5.68 MPa (832.7 psia), with corresponding relief capacity of 41L/s (650 gpm). Both CMTs are assumed to be available. The staff found that the assumption is inconsistent with the requirements of TS LCO 3.5.3, which require only one operable CMT. The staff requested, via RAI 440.119, that the licensee analyze both cases with one or two operable CMTs. In a letter, dated April 2, 2003, the applicant responded to RAI 440.119 by performing the requested analysis. The results of the analysis show similar plant response for cases with one CMT or two CMTs available. Because 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. Case 2 assumes that the operator takes actions to actuate the CMT and PRHR HX 1800 seconds after the loss of RNS cooling. The staff discusses its evaluation as follows.

Case 1— Automatic Safety System Actuation

DCD Tier 2, Table 19E.4.8-2, discusses the sequence of the event. 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. Because 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, as well as the pressurizer level. 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 and liquid begin to flow through the relief valve, the system pressure begins to decrease. The pressurizer level 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 Stage 4 valves opens the IRWST injection line valve. The vapor and liquid flow through the ADS valves reducing 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 (1) the NRC-approved NOTRUMP code is used for the analysis, (2) the input parameters used in the analysis are representative of the plant conditions at Modes 4 and 5 with the RCS intact, and (3) 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. DCD Tier 2, Table 19E.4.8-2, discusses the sequence of the event. 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.

The applicant stated in a letter dated November 13, 2003, that the resolution to Open Item 5.3.3-1, related to low-temperature overpressure protection, required a revision to the RNS relief valve setpoint from 5.68 MPa (832.7 psia) to 3.55 MPa (514.7 psia). The corresponding relief capacity of 41L/s (650 gpm) changed to 53.6 L/s (850 gpm). The applicant identified that the event affected by the RNS relief valve design changes was a loss of the RNS in Mode 4 with the RCS intact. The applicant reanalyzed the event for both cases with automatic safety system actuation (Case 1) and manual safety system actuation (Case 2), and presented its results in revised DCD Tier 2, Section 19E.4.8.2, as well as the applicant's letter dated November 13, 2003. The staff reviewed the results of the reanalysis and found that although the timing of actuation of the consequence mitigation systems in DCD Tier 2, Table 19E.4.8-2, for the sequence of the events changed, the results and conclusions discussed in Section 19.3.6.20.1 of this evaluation remained valid. Therefore, the staff concludes that the analysis for a loss of the RNS cooling initiated form Mode 4 with the RCS intact 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)

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 Stages 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 unavailable. 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.

DCD Tier 2, Table 19E.4.8-3, discusses the sequence of the event. 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 the IRWST flowpath 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 the RCS open. The staff concludes that 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 midloop 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 midloop conditions is similar to the plant response to the loss of RNS cooling in Mode 5 with the 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. Because the analysis for midloop 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 provided 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 the AP600 will be used for the AP1000 for accident mitigation.

- A sufficient operator time (several days for Mode 6 vs. 100 minutes for the Mode 5 midloop 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 requires that all ADS Stages 1–3 valves 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 flowpaths, 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 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.4.8.2 and 19E4.8.3, and Section 19.3.6.20 of this report, the analyses of the loss of the RNS for Modes 4, 5, and 6, with upper internals in place show that the ADS valves and IRWST flowpath provide sufficient venting and injection flow capacity to avoid the core uncovery during a loss of the RNS event. The TS requires the AP1000 ADS valves and the IRWST path 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 the 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 applicant to develop plant procedures for normal and abnormal operations, emergency operation, refueling and outage planning, alarm response, maintenance, inspection, and test and surveillance, as well as administrative controls. This is part of COL Action Item 19.3.2.1-1.

The staff will review the COL applicant's outage planning and control program, and the COL applicant 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 and 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 and an available alternate or backup system if a safety system or a defense-in-depth system is removed from service
- provisions to ensure that all personnel involved in outage activities are adequately trained, including operator simulator training, to the extent practical, and training for other plant personnel, including temporary personnel, is commensurate with the outage tasks they will be performing

The DCD did not specify this COL information. This was Open Item 19.3.7-1 in the DSER.

In response to DSER Open Item 19.3.7-1, the applicant stated in a letter dated July 1, 2003, that it will add the required COL information in DCD Tier 2, Section 13.5. Specifically, it indicated that the COL applicant should, at a minimum, address all elements discussed above in its outage plans. The staff confirmed that the required COL information was added to DCD Tier 2, Section 13.5. This is COL Action Item 19.3.7-1. Therefore, the staff concludes that DSER Open Item 19.3.7-1 is resolved.

19.3.8 Fire Protection

The fire protection program should address protection of safe shutdown functions, specifically, DHR during shutdown and refueling operations. This is to ensure that adequate protection is provided for systems necessary to remove decay heat and to maintain the RCS below saturation conditions.

Severe Accidents

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 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 that are 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. Additionally, 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. 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 specified that the fire protection analysis should demonstrate 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 defined 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 an RCS temperature of 176.7 °C (350 °F) and 3.2 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 HX 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 the 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 the 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 the RNS. The IRWST gutter isolation AOVs(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. Redundant RNS components are separated to limit fire damage. RNS pumps

and 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 that 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 HXs. This configuration will allow the RNS to continue to remove decay heat without the use of 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, the applicant is to maintain the integrity of these fire protection features (i.e., fire barriers, sprinkler systems, storage locations, and transient combustible amounts). The applicant's administrative controls of combustible 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 0.1 kPa (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, the IRWST can supply water for DHR. The 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 the IRWST. In this configuration, the plant will remain in a stable condition until the 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, "Procedure Development," indicates, as the applicant stated 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 EOPs. The applicant indicated that WCAP-14690 is directly applicable to the AP1000. DCD Tier 2, Sections 19E.1.2, "Scope," and 19E.3.3, "Background," indicate that the AP600 ERGs are applicable to the AP1000 ERGs, including shutdown operations.

The staff requested via RAI 440.109 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. As necessary, the capacity of the passive safety systems and active non-safety-related systems are increased 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 is the same. The AP600 ERGs use both non-safety-related systems and the passive safety systems to maximize the protection of the plant for design-basis and beyond DBAs. The application of the AP600 ERGs for the AP1000 is similar to the implementation of the standard ERGs for Westinghouse operating plants. Because the applicant's 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 systems, as well as balance of plant system design features. Because the AP600 and AP1000 designs are similar in functional performance and the AP600 ERGs provide symptom-oriented guidance, the staff finds that the use of the AP600 ERGs as 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, "Flood Protection," the applicant discussed the flood protection measures that are applicable to the AP1000 plant for postulated external flooding and internal flooding from plant system and component failures.

The seismic Category I containment and auxiliary buildings house all safety-related systems for the AP1000 design. Seismic Category I structures are located such that the land slopes away from the structures. This slope assures that external flood water will drain away from the building and prevent pooling near the building. Additionally, 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 well as 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 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 the following:

- structural enclosures
- structural barriers
- curbs and elevated thresholds
- leakage detection systems
- drainage systems

The flood sources that were considered in the internal flooding analysis include the following:

- 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 identified seven compartments inside containment that are subject to full or partial flooding. These compartments 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 to prevent flooding in one compartment from propagating into the other compartment. Inside these compartments, all the automatically actuated 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 identified safety-related equipment in the auxiliary building that requires 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 m to 0.91 m (2 ft 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 (I&C cabinets), the Class 1E dc system (Class 1E batteries and dc electrical equipment), and containment isolation. NRCAs are 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 the 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. This defense-in-depth feature results in a small probability that flooding would affect more than one safety-related system or division. 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. Compensatory measures are expected to be taken to maintain the flood 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 the equipment needed for the normal DHR function.

Based on the staff's preliminary review of this letter, it appeared to have errors in the calculated CDF for two of the eight sequences. The applicant was requested to address these errors in order for the staff to complete its review. This was Open Item 19.3.10-1 in the DSER.

The results from the shutdown flooding study appear to confirm that the inherent design characteristics of the AP1000 provide 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 affected by flooding in any area, and taking no credit for operator actions to mitigate the consequences of flooding.

The applicant revised their analysis to correct the errors discussed above. The analysis identified eight internal flooding scenarios at shutdown. The total calculated contribution to CDF from internal flooding during safe shutdown is 3.22E-9/yr. Therefore, Open Item 19.3.10-1 is resolved.

DCD Tier 2, Section 19.59.6.1, "Results of Internal Flooding Assessment," provides the results of the internal flooding analyses. The CDF from internal flooding during power events is 8.82E-10/yr, with a large early release fraction (LERF) of 7.14E-11/yr. The CDF from internal flooding events during low-power and shutdown events is stated to be 3.33E-9/yr, with a LRF of 5.37E-10/yr.

The results of the AP1000 study for internal flooding show that the AP1000 design is adequate because internal floods during shutdown do not represent a significant risk contribution. The results 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.

19.4 Consideration of Potential Design Improvements Under Requirements of 10 CFR 50.34(f)

19.4.1 Introduction

In 10 CFR 50.34(f)(1)(i), the NRC requires an applicant to "perform a plant/site specific PRA, the aim of which is to seek such improvements in the reliability of core and containment heat removal systems as are significant and practical and do not impact excessively on the plant." The applicant provided an initial evaluation of potential design improvements (severe accident mitigation design alternatives, or SAMDAs) for the AP1000 in response to RAI 720.60. 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. In a revised RAI response dated March 31, 2003, the applicant provided an updated evaluation addressing these concerns. The staff had not completed its evaluation of the SAMDAs at the time of the DSER. This was Open Item 19.4-1 in the DSER.

A revised evaluation was subsequently provided by letter dated February 18, 2004, and incorporated as Appendix 1B to the AP1000 DCD. On the basis of this evaluation, the applicant concluded that because of the small risk associated with the AP1000 design, none of the design improvements considered were cost beneficial. The staff's review of the evaluation is presented below.

19.4.2 Estimate of Risk for the AP1000

19.4.2.1 Westinghouse Estimates

Risk was defined in terms of person-rem and was calculated by multiplying the yearly frequency of an event by its consequences. The consequences were defined as the effective whole body

equivalent dose (50 year committed) to the total population within a 50 mile radius of the plant, assuming a 24-hour exposure following the onset of core damage. The applicant used the MELCOR Accident Consequence Code System (MACCS2), Version 1.12, to estimate accident consequences. Effective doses were estimated for each of six different RCs. The AP1000 Level 1 and Level 2 PRA models were used to provide pertinent data related to accident sequences, accident progression, and source terms. The ALWR site information described in the ALWR URD, Volume III, Annex B of Appendix A to Chapter 1, Revisions 5 and 6, was used to provide the meteorological and population data for the analysis. EPRI developed the ALWR reference site data to conservatively represent or bound the consequences at approximately 80 percent of the reactor sites in the United States. Because the EPRI URD did not provide sufficient topographical data to define the MACCS2 site input file, the site land use and crop data are based on representative site data for the Surry plant site provided in the MACCS manual (NUREG/CR-6613, "Code Manual for MACCS2, Users Guide").

The applicant's estimate of the offsite risk to the population within 80.5 km (50 miles) of the site is provided in DCD Tier 2, Table 1B-1. The total risk for at-power internal events is 0.043 person-rem per year for the AP1000 plant. This extremely low level of risk calculated by the applicant is primarily because of the low value predicted for the internal events CDF, specifically 2.41E-7 per reactor-year. Risk assessment studies for operating commercial PWRs typically estimate CDFs that are one to two orders of magnitude higher than the AP1000 CDF. These same commercial reactor studies typically predict LRFs that are one to two orders of magnitude larger than the applicant's LRF estimate for the AP1000 of 1.95E-8 per reactor-year for at-power internal events.

As part of the AP1000 risk assessment, the applicant estimated the CDF from external events (limited to fire and not including seismic events), internal flood, and shutdown events. The combined CDF from the evaluated internal and external events at power and at shutdown is about 5E-7/yr, as shown in DCD Tier 2, Table 1B-2. The applicant assumed the person-rem exposure per event from the internal event analysis to be applicable to all of these events. The corresponding risk reduction for all evaluated events is about 0.09 person-rem per year.

For purposes of estimating the risk reduction associated with potential design improvements, the applicant assumed the change in CDF (associated with implementation of a SAMDA) to be equal to the sum of the CDF from all the evaluated internal, external, and shutdown events. Thus, the consequences from all events (except seismic) are included in the risk reduction calculations.

19.4.2.2 Staff Review of Westinghouse Estimates

The staff reviewed the major models and assumptions entering into the applicant's risk estimate. The applicant based its risk estimate on the following three major elements:

(1) the mean value CDF estimates from the Level 1 PRA and supplementary analyses for external and shutdown events

(2) the MAAP computer code and supporting deterministic analyses for evaluating accident progression, containment performance, fission-product releases (source terms)

(3) the MACCS2 computer code, combined with meteorology and population data for a bounding reactor site, for estimating offsite consequences

As discussed in Section 19.1 of this report, the staff finds the approach used by the applicant for assessing CDF and containment performance to be logical and sufficient for describing and quantifying potential core damage sequences. The applicant estimated the uncertainty inherent in the CDF estimate, which has been considered by the staff in assessing the merit of the design alternatives. The NRC staff has performed a number of severe-accident confirmatory calculations, as described in Section 19.2 of this report. On the basis of the applicant and NRC calculations described therein, the staff concludes that Westinghouse's characterization of accident progression and containment performance is acceptable.

As part of the review of issues related to the Level 2 PRA (Section 19.1.10 of this report), the staff has reviewed the applicant's source term estimates for the major RCs and finds the process for assigning source terms acceptable. The staff has considered the applicant's use of the MACCS2 code, in conjunction with the site data in the EPRI URD, and concludes that this provides an acceptable basis for estimating the consequences associated with severe accident releases for the AP1000 design.

Theapplicant's dose estimates are based on exposure during the initial 24 hours following core damage. However, the applicant estimated the population dose risk for a 72-hour exposure. The 72-hour, point-estimate population dose risk is about 20 percent higher than the corresponding 24-hour dose risk. Given that the overall uncertainty in the PRA results is much greater than 20 percent, the staff considers the dose estimates for a 24-hour mission time adequate for the design alternative evaluations.

In summary, the staff considers the applicant's overall approach for quantifying the risk of severe accidents to be acceptable. Accordingly, the staff has based its assessment of the risk reduction potential for potential design improvements on the applicant's estimate of risk (3.6 person-rem over a 40-year plant life for all events). However, in view of the significant uncertainties inherent in risk estimates, the validity of the conclusions of this analysis were tested by considering the uncertainties in CDF and in containment performance. Section 19.4.6 of this report further discusses this aspect of the review.

19.4.3 Identification of Potential Design Improvements

Section 19.4.3.1 of this report describes the applicant's process for identifying potential design enhancements and the resulting set of potential enhancements. Section 19.4.3.2 of this report provides the staff's review of the applicant's design alternatives.

19.4.3.1 Potential Design Improvements Identified by Westinghouse

The process used by the applicant to identify candidate design alternatives included a review of design alternatives for other plant designs, including CE System 80+. The applicant also reviewed the results of the AP1000 PRA to assess possible design alternatives. Other design alternatives came from suggestions from AP1000 design personnel.

The applicant eliminated certain design improvements from further consideration on the basis that they are already incorporated into the AP1000 design. Examples of design features already included in the design are the following:

- hydrogen ignition system
- reactor cavity flooding system
- RCP seal cooling (AP600 has canned-motor pumps)
- RCS depressurization
- external reactor vessel cooling
- non-safety-grade containment sprays

Several risk-significant enhancements to the AP600 design have also been incorporated within the AP1000 design, and were therefore not further considered. DCD Tier 2, Section 1B.1.5, "Summary of Risk Significant Enhancement," discusses further noteworthy modifications which are summarized below and include the following:

- a change in the normal position of the two containment motor-operated recirculation valves (in series with squib valves) from closed to open to improve the reliability of opening these flowpaths

- a change in the EOPs to call for IRWST draining earlier in an event to improve the probability of successful operator action

- a change in the design of the IRWST vents to preferentially direct hydrogen releases to the IRWST pipe vents where diffusion flames will not adversely impact the containment

- incorporation of a low-boron core to reduce the potential contribution of ATWS events to plant risk

- addition of a third PCS drainline with a MOV that is diverse from the AOVs used in the other two drainlines to improve PCS reliability

- specification that two of the four squib valves in the recirculation lines be of a low-pressure type, and the remaining two squib valves be of a high-pressure type to reduce the contribution to CDF from CCF of recirculation squib valves

On the basis of the applicant's screening, 14 potential design improvements were retained for further consideration. This set of SAMDAs is the same as that considered for the AP600. DCD Section 1B.1.3, "Selection and Description of SAMDAs," describes further the 14 design improvements which are summarized below and include the following:

(1) Upgrade the CVCS for Small LOCAs: The CVCS is currently capable of maintaining the RCS inventory for LOCAs for effective break sizes up to 0.97 cm (3/8 in.) in diameter. A design alternative involving the upgrade of the CVCS for small LOCAs would extend the capability of the CVCS, enabling it to maintain RCS inventory during small- and intermediate- size LOCAs (up to an effective break size of 15.2 cm (6 in.) in diameter). Implementation of this design alternative would require installation of IRWST and

containment recirculation connections to the CVCS, as well as the addition of a second line from the CVCS pumps to the RCS.

(2) Filtered vent is design alternative would involve the installation of a filtered containment vent, including all associated piping and penetrations. This modification would provide a means to vent containment to prevent catastrophic overpressure failures as well as a filtering capability for source term release. The filtered vent would reduce the risk associated with late containment failures that might occur after failure of the PCS. Note, however, that even if the PCS fails, it is expected that air cooling will limit the containment pressure to less than the ultimate pressure under most environmental conditions.

(3) Self-Actuating Containment Isolation Valves: Self-actuation of CIVs could be used to increase the likelihood of successful containment isolation during a severe accident. This design alternative would involve the addition of a self-actuating valve or enhancement of the existing CIVs on normally open containment penetrations (specifically, those penetrations that provide normally open pathways to the environment during power and normal shutdown conditions). The design alternative would provide for self-actuation in the event that containment conditions are indicative of a severe accident. Closed systems inside and outside containment, such as the RNS and component cooling, would be excluded from this design alternative. The actuation of CIVs CIVs would be automatically initiated in the event that containment conditions are indicative of a severe accident.

(4) Passive Containment Sprays: This SAMDA involves adding a passive, safety-related spray system and all associated piping and support systems to the AP1000 design (in lieu of the non-safety-related active containment spray capability currently included within the AP1000 design). Installation of the safety-grade containment spray system could result in an increase in the following three risk benefits:

- scrubbing of fission products, primarily for containment isolation failure
- alternative means for flooding the reactor vessel (in-vessel retention)
- control of containment pressure for cases in which the PCS has failed

(5) Active High Pressure Safety Injection System: A safety-related, active HPSI system could be added that would be capable of preventing a core melt for all events except excessive LOCA and ATWS. Note, however, that this design alternative is not consistent with the AP1000 design objectives. The AP1000 would change from a plant with passive systems to a plant with passive and active systems.

(6) Steam Generator Shell-Side Heat Removal System: This design alternative would involve the installation of a passive, safety-related heat removal system to the secondary side of the SGs. This enhancement would provide closed-loop, secondary-system cooling by means of natural circulation and stored water cooling, thereby preventing the loss of the primary heat sink given the loss of SFW and the passive RHR HX.

(7) Direct Steam Generator Relief Flow to the IRWST: To prevent or reduce fission product release from bypassing containment during an SGTR event, flow from the SG safety and relief valves could be directed to the IRWST. An alternative, lower-cost option of this design alternative would be to redirect flow only from the first stage safety valve to the IRWST.

(8) Increased Steam Generator Pressure Capability: As an alternative to design alternative 7 above, another method could be used to prevent or reduce fission product release from bypassing containment during an SGTR event. This alternative method would involve an increase of the SG secondary-side and safety-valve setpoint to a level high enough to not allow an SGTR to cause the secondary-system safety valve to open. Although detailed analyses have not been performed, it is estimated that the secondary-side design pressure would have to be increased by several hundred psi.

(9) Secondary Containment Filtered Ventilation: This design alternative involves the installation of a passive charcoal and high-efficiency particulate air filter system for the middle- and lower- annulus region of the secondary concrete containment (below Elevation 135'-3"). Drawing a partial vacuum on the middle annulus via an eductor with motive power from compressed gas tanks would operate the filter system. This design alternative would reduce particulate fission product release from any failed containment penetrations.

(10) Diverse IRWST Injection Valves: In the current design, a squib valve in series with a CV isolates each of the four IRWST injection paths. To provide diversity, a modification could be made to allow for a different vendor to provide the valves in two of the lines. Such diverse IRWST injection valves would reduce the likelihood of CCFs of the four IRWST injection paths.

(11) Diverse Containment Recirculation Valves: In both the AP600 and AP1000 designs, two of the four recirculation lines contain a squib valve in series with a CV, and the remaining two recirculation lines contain a squib valve in series with a MOV. This SAMDA involves changing the recirculation valve specification to enable two of the four lines to use diverse squib valves. To provide diversity, a modification could be made to allow for a different vendor to provide the squib valves in two lines. Alternatively, in the AP1000 design, the applicant has specified that two of the four recirculation squib valves be designated as the low-pressure type and the remaining two squib valves as the high-pressure type. Diverse containment recirculation valves, which have been implemented within the AP1000 design, are responsive to the intent of this SAMDA and will reduce the frequency of core melt because of CCF of the four containment recirculation lines.

(12) Ex-Vessel Core Catcher: This design alternative would inhibit CCI, even in cases where the debris bed dries out. The enhancement would involve the design of a structure in the containment cavity or the use of a special concrete or coating. The current AP1000 design incorporates a wet cavity design in which ex-vessel cooling is used to maintain core debris within the vessel. In cases where reactor vessel flooding has failed, the PRA assumes that containment failure occurs from an ex-vessel steam explosion or CCI.

(13) High-Pressure Containment Design: A high-pressure containment design would prevent containment failures from severe accident phenomena, such as steam explosions and hydrogen detonation. This proposed containment design would have a design pressure of approximately 2.17 MPa (300 psig) and would include a passive cooling feature similar to the existing containment design. Although it would not reduce the frequency or magnitude of releases from an unisolated containment, the high-pressure containment would reduce the likelihood of containment failures.

(14) Increase Reliability of Diverse Actuation System: The DAS is a non-safety system that can automatically trip the reactor and turbine and actuate certain ESF equipment if the PMS is unable to perform these functions. The DAS provides diverse plant monitoring of selected plant parameters to guide manual operation and to confirm reactor trip and ESF actuations. Increasing the reliability of the DAS involves adding a third I&C cabinet and a third set of DAS instruments to allow the use of two-out-of-three logic instead of two-out-of-two logic.

The applicant considered an additional SAMDA that would involve relocating the entire RNS and piping inside the containment pressure boundary. This would prevent containment bypass due to ISLOCAs in the RNS. However, in the AP1000, the RNS has a higher design pressure than the systems in current PWRs, and an additional isolation valve is provided. As a result, ISLOCAs do not contribute significantly to the CDF in the AP1000 PRA. Because this change provides virtually no risk reduction, it was not investigated further.

19.4.3.2 Staff Evaluation

The set of potential design improvements considered for the AP1000 is the same as those considered for the AP600. As part of the review for the AP600, the staff reviewed the set of potential design improvements identified by the applicant and found it to be reasonably complete. The activity was accomplished by reviewing design alternatives associated with the following plants: Limerick, Comanche Peak, CE System 80+, Watts Bar (NUREG-0498), and the advanced boiling-water reactor (ABWR). Accident management strategies were surveyed (NUREG/CR-5474), and alternatives identified through the Containment Performance Improvement (CPI) Program (NUREG/CR-5567, -5575, -5630, and -5562). The results of this assessment are summarized in Appendix A to “Review of Severe Accident Mitigation Design Alternatives (SAMDAs) for the Westinghouse AP600 Design,” Science and Engineering Associates Inc., SEA 97-2708-010-A;1, August 29, 1997. Given the similarity between the AP1000 and the AP600 design features and risk profile, the staff considers this prior evaluation for the AP600 to be applicable to the AP1000 as well.

The staff notes that the AP1000 design is less tolerant of equipment failures than the AP600 in regards to (1) the large LOCA success criteria for the AP1000 which requires operation of two of two accumulators whereas only one of two accumulators is required for the AP600, and (2) the LOCA success criteria for the AP1000 which requires operation of three of four ADS Stage 4 valves whereas only two of four ADS Stage 4 valves are required for the AP600. At the staff’s request, the applicant performed an evaluation of the following two additional alternatives:

Severe Accidents

(1) Larger accumulators: An increase in the size of the accumulators to sufficiently change the large LOCA success criteria from two of two accumulators to one of two accumulators. The applicant estimates that the accumulator tanks would have to increase in size from 56.6 m^3 to 113.2 m^3 (2000 ft^3 to 4000 ft^3). This increase would likely require a change to the design of the DVI piping subsystem and significant reanalysis of the DVI piping.

(2) Larger ADS Stage 4 valves: An increase in the size of the ADS Stage 4 valves to sufficiently change the LOCA success criteria from three of four valves to two of four valves. The applicant estimates that the valves would have to increase in size from 35.6 cm to 45.7 cm (14 in. to 18 in.), and that common fourth stage piping that connects to the hot-leg would have to increase in size from 45.7 cm to 50.8 cm (18 in. to at least 20 in.). This increase would require a significant redesign of the squib valve and the ADS Stage 4 piping, which in turn would impact the design of the reactor coolant loop piping. Such a redesign would necessitate additional confirmatory testing to verify that the behavior of the passive safety systems was not adversely impacted.

For both these alternatives, the applicant estimated that the redesign and reanalysis costs associated with the changes would be significantly greater than the benefits associated with completely eliminating all severe accident risk for the AP1000. Therefore, these design changes were not pursued further.

Although several design alternatives were not included in the applicant's analysis, in most instances these design alternatives are either already included in the AP1000 design or bounded in terms of risk reduction by one or more of the design alternatives that were included in the applicant's analysis. In some other cases, design alternatives were pertinent only to BWRs. The staff's review did not reveal any additional design alternatives that obviously should have been given consideration by the applicant. The applicant considered some of the potential design alternatives identified in the above references as appropriate for accident management strategies, rather than as design alternatives. The staff notes that the set of design improvements is not all inclusive, in that additional, perhaps less-expensive design improvements could be postulated. However, the benefits offered by any additional modifications would not likely exceed those for the modifications evaluated. Also, the costs of alternative improvements are not expected to be less than those of the least expensive improvements evaluated, when the subsidiary costs associated with maintenance, procedures, and training are considered.

The discussions in DCD Tier 2, Appendix 1B, do not provide the basis or the process used by the applicant for screening the many possible design alternatives to arrive at the final list of 14 selected for evaluation. Although the information provided does not demonstrate that the search for design alternatives was necessarily comprehensive, the staff's review of the more than 120 candidate design alternatives considered for the AP600 did not identify any new alternatives more likely to be cost-beneficial than those included in the AP1000 design alternative evaluations. The staff notes that the applicant has incorporated several risk-significant enhancements to the AP600 design within the AP1000, as discussed in Section 19.4.3.1 of this report, and has considered potential design changes to improve the

AP1000 success criteria. On this basis, the staff concludes that the set of potential design improvements evaluated by the applicant is acceptable.

19.4.4 Risk Reduction Potential of Design Improvements

19.4.4.1 Westinghouse Evaluation

The applicant assumed that each design alternative would work perfectly to completely eliminate all severe accident risk from evaluated internal, external, and shutdown events. This assumption is conservative, as it maximizes the benefit of each design alternative. The design alternative benefits were estimated on the basis of the reduction of risk expressed in terms of whole body person-rem per year received by the total population within a 80.5-km (50-mile) radius of the AP1000 plant site, as discussed in Section 19.4.2 of this report.

The applicant used the cost-benefit methodology of NUREG/BR-0184 to calculate the maximum attainable benefit associated with completely eliminating all risk for the AP1000. This methodology includes consideration of replacement power costs. The applicant estimated the present worth of eliminating all risk to be $21,000. Even if the AP1000 CDF and LRF were a factor of 10 higher, this value would increase to only about $200,000.

19.4.4.2 Staff Evaluation

The staff reviewed the applicant's bases for estimating the risk reduction associated with the various design improvements. The applicant conservatively assumed that each design alternative is completely effective in eliminating all risk. The staff concludes that this treatment is bounding and conservative.

The applicant's risk reduction estimates are on the basis of point-estimate (mean) values, without consideration of uncertainties in CDF or offsite consequences. Although this is consistent with the approach taken in previous design alternative evaluations, further consideration of these factors could lead to significantly higher risk reduction values, given the extremely small CDF and risk estimates in the baseline PRA. In assessing the risk reduction potential of design improvements for the AP1000, the staff has based its evaluation on the applicant's risk reduction estimates for the various design alternatives, in conjunction with an assessment of the potential impact of uncertainties on the results. This assessment is discussed further in Section 19.4.6 of this report.

19.4.5 Cost Impacts of Candidate Design Improvements

DCD Tier 2, Section 1B.1.8, "Evaluation of Potential Improvements," discusses capital cost estimates for the design alternatives evaluated by the applicant for the AP1000. DCD Tier 2, Table 1B-5, presents the results of the cost evaluations. The cost evaluations did not account for factors such as design engineering, testing, and maintenance associated with each design alternative. These factors, if included, would increase the overall costs and decrease the capital benefits of each alternative. Thus, this approach is conservative.

Severe Accidents

As mentioned previously, the set of SAMDAs considered for the AP1000 is the same as that considered for the AP600. The staff compared the capital costs for the AP600 design alternatives with those evaluated for the ABWR and CE System 80+. This comparison was performed to determine the reasonableness of the cost estimates presented by the applicant. Because there was not an exact match in the design alternatives among the reactor designs, only rough comparisons were possible. Based on these comparisons, the staff concludes that the cost estimates for the AP600 design alternatives are in reasonable agreement with the costs for roughly similar design alternatives evaluated for other plants. Given the similarity between the AP1000 and the AP600 design features and risk profile, the staff considers this prior evaluation for the AP600 to be applicable to the AP1000 as well.

On the basis of the staff's prior audit, the staff views the applicant's approximate cost estimates for the AP1000 as adequate, given the uncertainties surrounding the underlying cost estimates, and the level of precision necessary, given the greater uncertainty inherent on the benefit side with which these costs were compared.

19.4.6 Cost-Benefit Comparison

19.4.6.1 Westinghouse Evaluation

The applicant performed a cost-benefit comparison to determine whether any of the potential severe accident design features could be justified. The applicant assessed the benefits of each design alternative in terms of potential risk reduction, which was defined as the reduction in whole body person-rem per year received by the total population within a 80.5-km (50-mile) radius of the AP1000 plant site. The applicant used the cost-benefit methodology of NUREG/BR-0184 to calculate the maximum attainable benefit associated with completely eliminating all risk for the AP1000. This methodology includes consideration of replacement power costs. The applicant estimated the present worth of eliminating all risk to be $21,000. This value is an upper bound because in practice there is no design alternative which, if implemented, would reduce the plant CDF to zero. The applicant also provided additional sensitivity analyses exploring the impacts of the following:

- a 3-percent discount rate rather than the 7-percent discount rate assumed in the base case
- a factor of 10 increase in the population dose used in the base case
- a more realistic reduction in CDF (i.e., each SAMDA reduces CDF by 50 percent rather than 100 percent, as assumed in the base case)
- a factor of 2 increase in the base case CDF
- a factor of 10 increase in the maximum attainable benefit

DCD Tier 2, Table 1B-4, summarizes the results for these cases. With the exception of the last sensitivity case, the calculated maximum attainable benefit was about $43,000 or less. Even

when the AP1000 CDF and LRF were increased by a factor of 10, the maximum attainable benefit (associated with eliminating all risk for the AP1000) increased to only about $200,000.

The applicant found that none of the 14 design alternatives and neither of the two additional alternatives related to the PRA success criteria would be cost beneficial. Only one alternative has an implementation cost close to $21,000, namely, SAMDA 3, self-actuating CIVs, which has an estimated cost of $33,000. All of the remaining alternatives have estimated implementation costs at least a factor of 20 greater than the maximum attainable benefit of $21,000. On this basis, the applicant concluded that only SAMDA 3 warranted further evaluation.

SAMDA 3 consists of improved containment isolation provisions on all normally open containment penetrations. The design alternative would involve either adding a self-actuating valve or enhancing the existing inside CIV to provide for self-actuation in the event that containment conditions are indicative of a severe accident. The applicant noted that even if this SAMDA completely eliminated all releases associated with containment isolation failures (i.e., release category CI) and reduced CDF to zero, the benefit of the SAMDA would be on the order of $1000. More realistically, the CDF would not be impacted, and elimination of all containment isolation failures would only have a benefit on the order of $100. Thus, even the lowest cost SAMDA would not be cost beneficial.

On the basis of the cost-benefit comparison, the applicant concluded that no additional modifications to the AP1000 design are warranted.

19.4.6.2 Staff Evaluation

The applicant's estimates of risk do not account for uncertainties either in the CDF or in the offsite radiation exposures resulting from a core damage event. The uncertainties in both of these key elements are fairly large because key safety features of the AP1000 design are unique, and their reliability has been evaluated through analysis and testing programs rather than operating experience. In addition, the estimates of CDF and offsite exposures do not account for the added risk from earthquakes.

As part of the AP600 review, detailed analyses were performed to assess design alternative benefits, taking into account the uncertainties in estimated CDF, offsite releases of radioactive materials from a severe accident, and the effects of external events. Given the similarities between the AP1000 and AP600 design features and risk profiles and the set of SAMDAs relevant for each design, the staff considers this prior evaluation for the AP600, summarized below, to be applicable to the AP1000 as well.

Estimates were made of the maximum benefits that can be achieved with the AP600 design alternatives, assuming a design alternative can either completely eliminate all core damage events or completely eliminate offsite releases of radioactive materials in the event of a severe accident. The estimates of benefits were calculated using the NRC-developed FORECAST code (NUREG/CR-5595, Revision 1, "FORECAST: Regulatory Effects Cost Analysis Software Manual, Version 4.1," Science and Engineering Associates, Inc., July 1996). FORECAST allows the use of uncertainty ranges for all key parameters and provides a means for combining

uncertainties in these parameters. For the purposes of estimating the maximum potential benefit from the AP600 design alternatives, external events and accident sequences not yet accounted for in the PRA were assumed to increase the reference CDF by two orders of magnitude (i.e., a factor of 100).

The results of the analysis indicated that design alternatives which prevent accidents (i.e., reduce the accident frequency to zero) are much more cost effective than design alternatives which reduce or eliminate offsite releases, but which have no effect on accident frequency. This is because of the fairly large benefits associated with averted onsite cleanup and decontamination costs and avoided replacement energy costs. Neither of these costs are assumed to be impacted by design alternatives which do not reduce accident frequency. The design alternatives were divided between those that impact the CDF and those that impact containment performance, but not CDF. Benefits were estimated by taking the fractional reduction in risk for each design alternative (compared to the AP600 baseline risk as defined by the applicant) and applying that fraction to the mean benefits.

Design alternatives that were within a decade of meeting a benefit-cost criteria of $5000/person-rem were subjected to further probabilistic and deterministic considerations. None of the design alternatives had a cost-benefit ratio of less than $5000/person-rem. The only design alternatives which came within a decade of the $5000/person-rem criteria were SAMDA 10, diverse IRWST injection valves, and SAMDA 3, self-actuating CIVs. The staff concludes, on the basis of further probabilistic and deterministic evaluation, that these design alternatives are not cost beneficial and need not be further pursued.

Given the similarities between the AP1000 and the AP600 design features and risk profile and the set of SAMDAs relevant for each design, the staff considers the results of this prior evaluation for the AP600 to be applicable to the AP1000 as well. Accordingly, the staff further evaluated each of these two SAMDAs for the AP1000, as discussed below.

19.4.6.2.1 Self-Actuating Containment Isolation Valves

This design alternative would reduce the likelihood of containment isolation failure by adding self-actuating valves or enhancing the existing CIVs for automatic closure when containment conditions indicate a severe accident has occurred. Conceptually, the design would either be an independent valve or an appendage to an existing fail-closed valve that would respond to postaccident containment conditions within containment. For example, a fusible link would melt in response to elevated ambient temperatures resulting in venting the air operator of a fail-closed valve, thus providing the self-actuating function. This design alternative is estimated to impact releases from containment by less than 10 percent.

This improvement to the containment isolation capability would appear to be effective in reducing offsite releases for accidents involving external events, as well as internal events. The addition of this design alternative would impose minor operational disadvantages to the plant because the operations and maintenance staff would require some additional training. Additionally, these automatic features would require periodic testing to assure that they are functioning properly.

The most important question regarding this design alternative is whether or not it can be implemented for a cost of only $33,000. The cost estimate does not appear to include the first-time engineering and qualification testing that would be required to demonstrate that the valve would perform its intended function in a timely and reliable manner. The costs associated with periodic testing and maintenance do not appear to have been included. The staff believes that the actual costs of this design alternative would be substantially higher than the applicant's estimate (by a factor of 10 or more) when all related costs are realistically considered. On the basis of the unfavorable cost-benefit ratio and the expectation that actual costs would be even higher than estimated by the applicant, the staff concludes that this design alternative is not cost beneficial and need not be further evaluated.

19.4.6.2.2 Diverse IRWST Injection Valves

In the current AP1000 design, a squib valve in series with a CV isolates each of four IRWST injection paths. This design alternative would reduce the likelihood of CCFs of IRWST injection to the reactor by utilizing diverse valves in two of the four lines. The complete elimination of the CCFs of IRWST injection squib valves would lead to a moderate (up to 10 percent) reduction of the at-power internal events CDF. In the absence of a comprehensive external events PRA for the AP1000 plant, it is difficult to estimate the effectiveness of this design alternative in reducing the risk from events such as seismic events. However, it appears likely that failure to inject coolant to the reactor would remain a contributor to the CDF from external events, in which case diversity in the IRWST injection valves should help to reduce the risk from both external and internal events.

For the CVs, alternate vendors are available. However, it is questionable if CVs of different vendors would be sufficiently varied to be considered diverse unless the type of CV was changed from the current swing disk check to another type. The swing disk-type is preferred for this application and other types are considered less reliable.

Adding diversity to the injection line squib valves would require additional spares at the plant and some additional training for plant operations and maintenance staff, but would not appear to add significantly to the operational aspects of the AP1000. However, a greater issue concerns the availability and costs of acquiring diverse valves from a second vendor. Squib valves are specialized valve designs for which there are few vendors. The applicant claimed that a vendor may not be willing to design, qualify, and build a reasonable squib valve design for this application, considering that they would only supply two valves per plant. The cost estimate for this design alternative assumes that a second squib valve vendor exists and that the vendor only provides the two diverse IRWST squib valves. The cost impact does not include the additional first-time engineering and qualification testing that will be incurred by the second vendor. The applicant estimated that those costs could be more than $1 million dollars. As a result, the applicant concluded that this design alternative would not be practicable because of the uncertainty in the availability of a second squib valve design/vendor and the uncertainty in reliability of another type of CV. The staff considers the rationale set forth by the applicant regarding the potential reductions in reliability and high costs associated with obtaining diverse valves to be reasonable. On the bases of these arguments, the staff concludes that this design alternative need not be further pursued.

19.4.7 Conclusions

As discussed in Section 19.1 of this report, the applicant made extensive use of the results of the PRA to arrive at a final AP1000 design. As a result, the estimated CDF and risk calculated for the AP1000 plant are very low, both relative to operating plants and in absolute terms. The low CDF and risk for the AP1000 plant are a reflection of the applicant's efforts to systematically minimize the effect of initiators/sequences that have been important contributors to CDF in previous PWR PRAs. This minimization has been done largely through the incorporation of a number of hardware improvements in the AP1000 design. Section 19.1 of this report discusses these improvements and the additional AP1000 design features which contribute to low CDF and risk for the AP1000.

Because the AP1000 design already contains numerous plant features oriented toward reducing CDF and risk, the benefits and risk reduction potential of additional plant improvements is significantly reduced. This reduction is true for both internally and externally initiated events. Moreover, with the features already incorporated in the AP1000 design, the ability to estimate CDF and risk approaches the limitations of probabilistic techniques. Specifically, when CDFs of 1 in 100,000 or 1,000,000 years are estimated in a PRA, it is the area of the PRA where modeling is least complete, or supporting data are sparse or even nonexistent, that could actually be the more important contributors to risk. Areas not modeled or incompletely modeled include human reliability, sabotage, rare initiating events, construction or design errors, and systems interactions. Although improvements in the modeling of these areas may introduce additional contributors to CDF and risk, the staff does not expect that additional contributions would change anything in absolute terms.

In 10 CFR 50.34(f)(1)(i), the NRC requires an applicant to perform a plant-/site-specific PRA. The aim of this PRA is to seek such improvements in the reliability of core and containment heat removal systems that are significant and practical and do not impact excessively on the plant. The staff concludes that the AP1000 PRA and the applicant's use of the insights of this study to improve the design of the AP1000 meet this requirement. The staff concurs with the applicant's conclusion that none of the potential design modifications evaluated are justified on the basis of cost-benefit considerations. It further concluded that it is unlikely that any other design changes would be justified on the basis of person-rem exposure considerations because the estimated CDFs would remain very low on an absolute scale. Therefore, Open Item 19.4-1 is resolved.

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-7	1E-6 to 8E-5
— Large	4.5E-8	
— Spurious ADS Actuation	3.0E-8	
— Safety Injection Line Break	9.5E-8	
— Medium	1.6E-8	
— Small	1.8E-8	
— CMT Line Break	4.0E-9	
— RCS Leak	3.0E-9	
Steam Generator Tube Rupture	7.0E-9	9E-9 to 3E-5
Transients	8.0E-9	5E-7 to 3E-4
Loss of Offsite Power/Station Blackout	1.0E-9	1E-8 to 7E-5
Anticipated Transient Without Scram	5.0E-9	1E-8 to 4E-5
Interfacing System LOCA	5.0E-11	1E-9 to 8E-6
Vessel Rupture	1.0E-8	1E-7
Total	2.4E-7	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	2.2E-7	91.9	NA
Early Containment Failure	7.5E-9	3.1	38
Intermediate Containment Failure	1.9E-10	<0.1	1
Late Containment Failure	3.5E-13	<0.1	<0.1
Containment Isolation Failure	1.3E-9	0.6	7
Containment Bypass	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	2.2E-7	8.8E2	1.9E-4	1
Early Containment Failure	7.5E-9	9.4E5	7.0E-3	52
Intermediate Containment Failure	1.9E-10	8.9E5	1.7E-4	1
Late Containment Failure	3.5E-13	5.8E5	2.0E-7	--
Containment Isolation Failure	1.3E-9	2.1E6	2.9E-3	21
Containment Bypass	1.1E-8	3.1E5	3.3E-3	24
Total	2.4E-7		1.3E-2	100

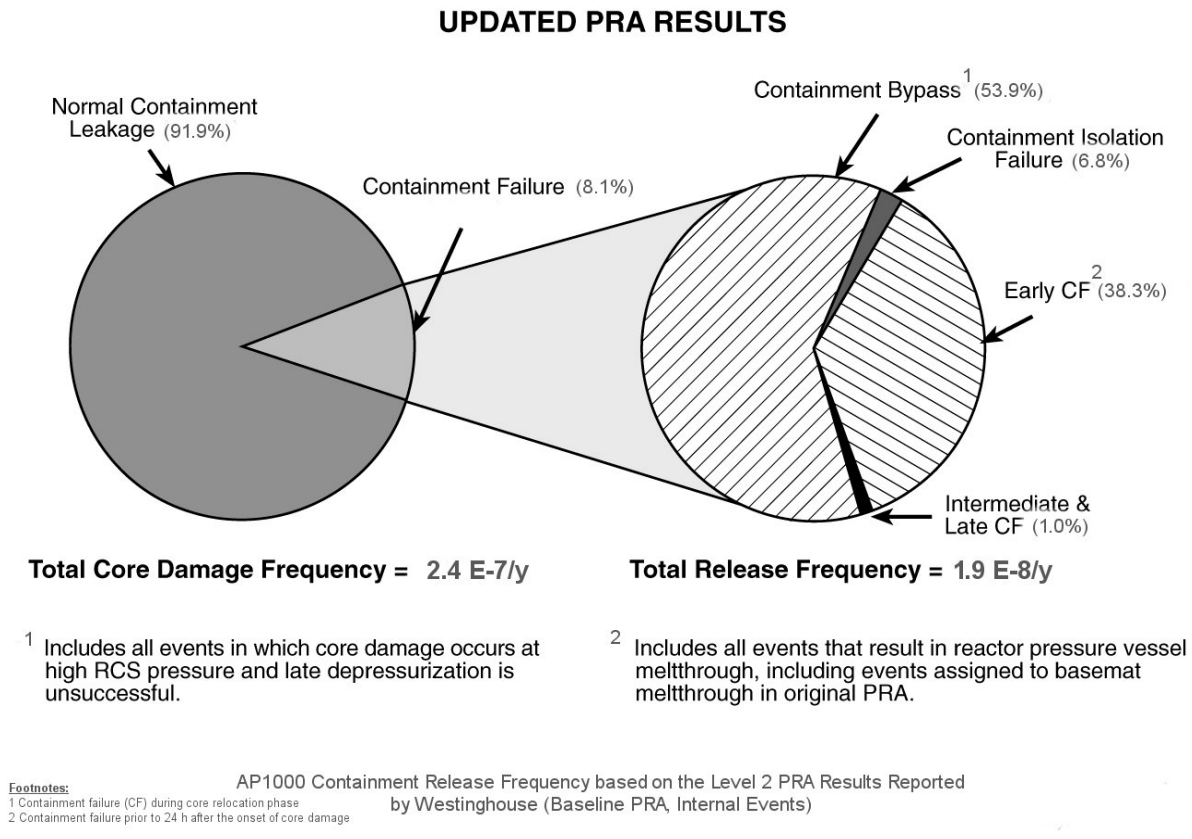

Figure 19.1-1 Breakdown of Containment Release Frequency Based on the Level 2 PRA Results Reported by Westinghouse (Baseline PRA, Internal Events)

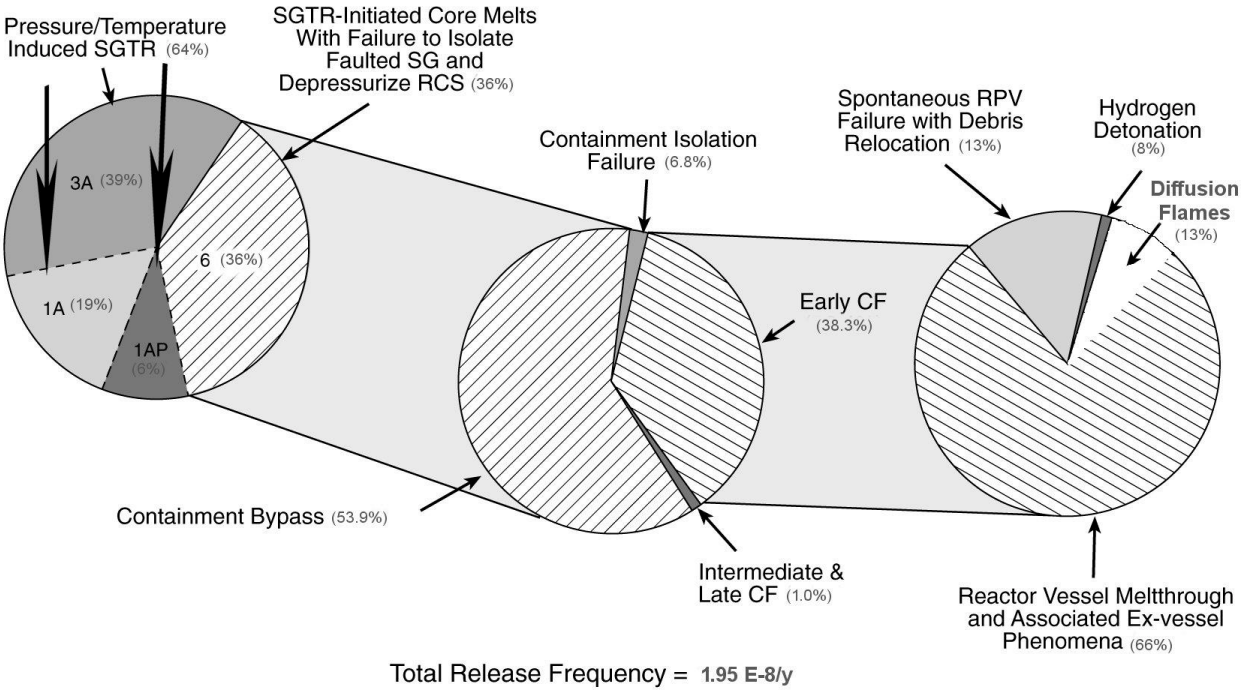

Figure 19.1-2 Breakdown of AP1000 Containment Release Modes by Contributor, as Reported by Westinghouse

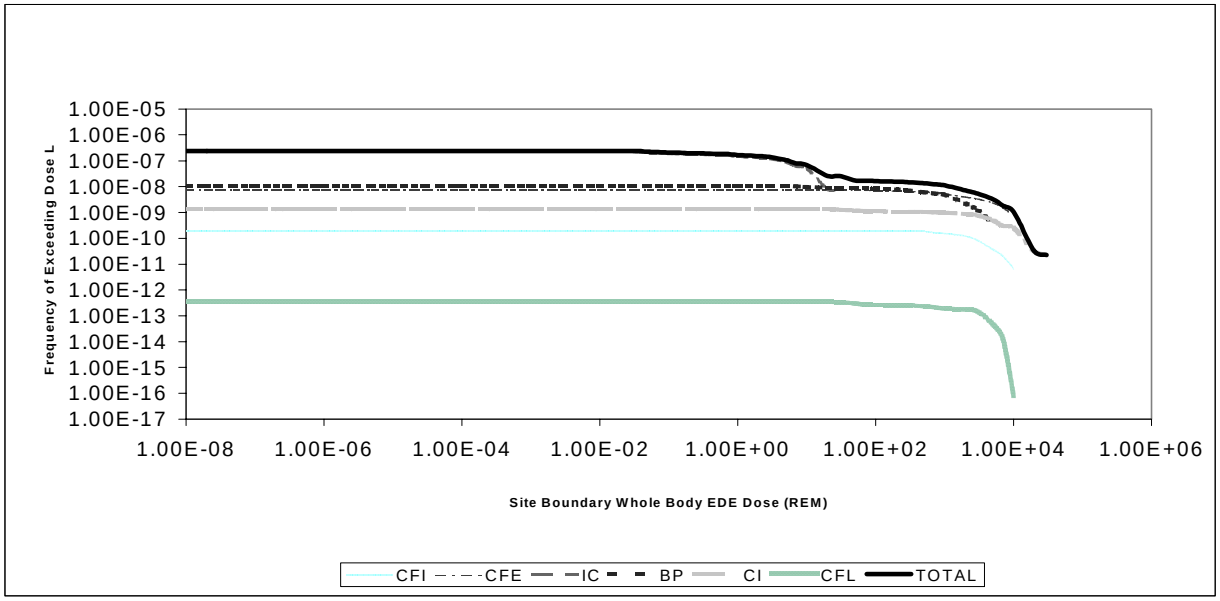

Figure 19.1-3 Overall Dose Risk
Site Boundary Whole Body EDE, 24-Hour Dose

19A. SEISMIC MARGIN ANALYSIS

Background

In DCD Tier 2, Chapter 19, with supporting details in Chapter 55 of the AP1000 PRA, "AP1000 Seismic Margins Evaluation," the applicant discussed the SMA. In this section, the staff evaluated the adequacy of the AP1000 SMA to estimate the High Confidence, Low Probability of Failures (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 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 guidance 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.

DCD Tier 2, Table 2-1, discusses the site parameters that constitute the seismic design basis for the AP1000. The seismic ground motion spectrum for a 0.5 g RLE is based on the AP1000 design response spectra anchored to a 0.5 g peak ground acceleration value. DCD Tier 2, Chapter 3, describes the seismic design criteria and methodology used in the design of SSCs. 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 that 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. The other part consists of evaluating the seismic capacity of components and structures that comprise those safe shutdown systems.

Seismic Margin Analysis

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 the following:

(1) A_m for median ground acceleration capacity
(2) logarithmic standard deviation (LSD) $ß_r$ for randomness in the capacity
(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 the following fragility model :

$$\text{HCLPF capacity} = A_m \exp(-1.65\,[ß_r + ß_u]) = A_m \exp(-2.326\, ß_c)$$

The mean peak ground acceleration capacity, A_m, is related to the stress and 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 did not explain how this factor was used in its probabilistic FA. This was Open Item 19A.2-1 in the DSER.

In a letter dated July 31, 2003, the applicant presented an example for calculating the deterministic strength factor. The staff reviewed the example and concluded that the applicant has adequately demonstrated how this factor is calculated. Therefore, Open Item 19A.2-1 is resolved.

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 did not explain how this factor was used in its probabilistic FA. This was Open Item 19A.2-2 in the DSER.

In a letter dated July 31, 2003, the applicant presented an example for calculating the variable strength factors. The staff reviewed the example and concluded that it adequately demonstrates how this factor is calculated. Therefore, Open Item 19A.2-2 is resolved.

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 did not explain how this factor was used in its probabilistic FA. This was Open Item 19A.2-3 in the DSER.

Seismic Margin Analysis

In a letter dated July 31, 2003, the applicant presented an example for calculating the material factor. The staff reviewed the example and concluded that it adequately demonstrates how this factor is calculated. Therefore, Open Item 19A.2-3 is resolved.

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 SSCs 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 included in the probabilistic FA, the applicant used conservative damping values in the range of 4 percent to 5 percent of critical damping. The staff finds the damping values used by the applicant to be lower than the values associated with failure level motion; consequently, the applicant's values 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 post-yield 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 FA 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 was requested to justify the use of such a high variability factor for the natural frequency calculations when using detailed finite element models. This was Open Item 19A.2-4 in the DSER.

In a letter dated July 31, 2003, the applicant confirmed the staff's conclusion that modal frequency values can vary by a factor of 1.8 when using a composite logarithmic standard deviation of 0.3. The applicant presented a reevaluation to estimate a more realistic standard deviation and concluded that a margin factor of 1.3 for steel structures, corresponding to a standard deviation of about 0.14, is appropriate. For concrete structures, the applicant concluded that a margin factor of 1.35 is appropriate. The staff reviewed the applicant's reevaluation and finds it acceptable. The applicant also committed to revise Section 55.2.2.3 of

the AP1000 PRA. The staff planned to review the implementation of the revised margin factors for modal frequencies to assess their effect on the calculated HCLPF capacities.

During the audit on October 6 through 9, 2003, the staff reviewed a draft revision to Table 55-1 of the AP1000 PRA, which lists the revised HCLPF capacities. The revised margin factors resulted in increases to the HCLPF capacities, as would be expected. The staff found the changes in the HCLPF capacities to be consistent with the revised margin factors.

During the audit conducted on December 15 and 16, 2003, the staff noted that the revised table of HCLPF capacities had not been included in the latest revisions to the DCD and the PRA report. The DCD and PRA were revised to implemented the changes related to this (Table 55-1 of the AP1000 PRA and DCD Tier 2, Chapter 19); therefore, this issue is resolved.

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), and is acceptable to the staff. Therefore, Open Item 19A.2-4 is resolved.

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 staff concluded that the discussion about the SSI-related variability in Chapter 55 of the PRA report for the AP1000 was inappropriate because the use of the variability factor $(\beta_c)_{SSI}$ was not justified. This was Open Item 19A.2-5 in the DSER.

In a letter dated July 31, 2003, the applicant committed to revise Section 55.2.2.3 of the AP1000 PRA, "Analysis of Structure Response," to remove all references to SSI. The staff finds this acceptable. During the audit on December 15 and 16, 2003, the staff verified that this change is incorporated in the AP1000 PRA. Therefore, Open Item 19A.2-5 is resolved.

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 for which 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 American Concrete Institute (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 an HCLPF value of 0.51 g (Table 55-1 of the AP1000 PRA, 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 was requested 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 (NI) basemat are predicted to lift up under the SSE loading. As noted in Section 3.7 of this report, the effect of uplift because of design-basis seismic excitation is an open area. Consequently, at 0.5 g RLE, the capacity of the tension ring could potentially be lower. Therefore, the validation of HCLPF values calculated by the CDFM approach was Open Item 19A.2-6 in the DSER.

In a letter dated July 31, 2003, the applicant addressed the shear modulus issue raised by the staff and the possible double-counting of energy dissipation. The resolution of potential effect of lift-off under seismic excitation was deferred to Open Item 19A.2-8.

The staff agreed to review CDFM calculations to verify the applicant's response to the open item issues related to an increase in concrete shear strength and the double-counting of energy dissipation, and to track the resolution of the lift-off issue under Open Item 19A.2-8.

During the audit conducted on October 6 through 9, 2003, the staff reviewed APP-PRA-GSR-002, Revision 0, "AP1000 Seismic Margins HCLPF Calculations," and APP-1277-S3C-009, Revision 0, "Shield Building Roof Seismic Margin Evaluation." The staff concluded that the applicant has appropriately implemented the CDFM method to estimate conservative HCLPF capacities, in accordance with standard industry practice. On this basis, Open Item 19A.2-6 is resolved.

Test Results

The 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 PRHR and CMT system valves automatically fail open on loss of instrument air whenever these losses are caused by seismically induced LOOP). In the AP1000 design, the applicant used solid-state switching devices and robust electromechanical 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 natural frequency of the equipment 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 did not identify any equipment for which such design specifications will be included. Although the applicant appeared to have used a conservative approach to obtain the equipment HCLPF value from test results, it was not clear how the use of known

natural frequency values for equipment within the standard design scope will be implemented. Because 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 was Open Item 19A.2-7 in the DSER.

During a teleconference on August 22, 2003, the staff requested to review representative design specifications for equipment with known fundamental natural frequency.

During the audit on October 6 through 9, 2003, the staff discussed this issue with the applicant and reviewed a typical design specification for equipment with known fundamental natural frequency. The staff noted that there is no discussion in the DCD about the COL applicant's responsibility to order equipment that maintains the validity of the HCLPF capacities reported in the SMA. The applicant agreed to incorporate such direction in DCD Tier 2, Chapter 19.

In a letter to NRC, dated October 10, 2003, the applicant submitted a second revision to its response to this open item. The applicant identified a revision to DCD Tier 2, Section 19.59.10.5, which defines the COL applicant's responsibilities to ensure that purchased equipment meets minimum seismic requirements consistent with those used to define the HCLPF values in DCD Tier 2, Table 19.55-1. This is acceptable to the staff. This is part of COL Action Item 19A.2-1.

During the audit conducted on December 15 and 16, 2003, the staff verified that the DCD was revised to incorporate the revision to DCD Tier 2, Section 19.59.10. Therefore, Open Item 19A.2-7 is resolved.

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 the polar crane, baffle plate supports, PRHR HX, CMT, 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 CMT has an 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 NI structure would necessitate a review of this HCLPF value. This was Open Item 19A.2-8 in the DSER.

In a letter dated August 1, 2003 , the applicant presented its technical justification for concluding that lift off of either the internal structure or the NI structure will not change the HCLPF values reported in the PRA report. The staff reviewed the information but could not reach the same conclusion. Reported quantitative information showed some significant effects of lift off on the seismic response spectra for the 0.5g RLE. The applicant presented qualitative arguments that the increased spectral accelerations do not affect the reported HCLPF capacities. An additional consideration was that the staff had not yet accepted the applicant's methodology for analyzing lift off.

During a teleconference on August 22, 2003, the staff identified its concerns. The resolution of the lift-off issue is crucial to staff acceptance of the AP1000 seismic design basis and also the

SMA. There were apparent conflicts between data presented and the conclusions reached about the effect of liftoff on the seismic response at the SSE (0.3g) and the RLE (0.5g) levels. In addition, the staff did not have a clear picture of the models used and the analyses conducted to address liftoff.

Floor response spectra for a 0.5g RLE, with and without basemat liftoff from the underlying rock, are presented in the open item response. The nonlinear lift-off results show significant increases in vertical-direction spectral acceleration for frequencies above 15 Hz, when compared to the linear results without liftoff. The applicant stated that there are no significant lift-off effects at the 0.3g SSE level. The results presented did not consider the simultaneous effect of containment shell/containment internal structures liftoff from the basemat.

The results of a separate nonlinear analysis of containment shell liftoff from the basemat are also reported. At the 0.3g SSE level, a maximum lift-off of about 0.25 cm (0.1 in.) is predicted. At the 0.5g RLE level, the predicted maximum lift-off is about 2.54 cm (1.0 in.). These predictions are based on static analysis. Therefore, in-structure response spectra, with and without lift-off effects, are not presented.

The applicant appeared to be addressing this issue in a piecemeal fashion, justifying the insignificance of liftoff at each step. The staff requested the applicant to perform an integrated evaluation of lift-off effects that justified its conclusions.

During the audit on October 6 through 9, 2003, the staff conducted a review of the applicant's latest analysis methods and results for the lift-off evaluation. The two separate potential liftoffs that can occur include basemat from underlying rock and containment shell/containment internal structure from the basemat. At the SSE level of 0.3g PGA, the staff concluded that the applicant's analyses and results adequately demonstrate that liftoff would be minimal and would not have a significant effect on seismic loads and in-structure response spectra. However, the nonlinear increase in liftoff reported at the seismic margins earthquake level of 0.5g PGA was still a concern to the staff. Also, the analysis methods employed to date did not consider coupling effects between the two liftoffs. On this basis, the staff concluded that the applicant's analysis methods were insufficient for the SMA and did not accept the conclusion that liftoff is not significant at the 0.5g PGA level.

During the audit, the applicant identified a number of options it was considering to resolve the lift-off issue, but stated that it had not chosen a specific course of action.

In a letter to the NRC, dated November 17, 2003, the applicant submitted a second revision to its response to this open item. To address the issue of liftoff during a seismic margins review level earthquake (0.5g PGA), the applicant submitted the results of new NI basemat lift-off analyses and identified a design change for the containment shell to provide positive anchoring to the NI basemat by the use of shear studs welded to the lower head of the containment shell. This design change is intended to preclude liftoff of the containment shell/containment internal structures from the NI basemat. Section 3.8.2 of this report includes the staff's evaluation of this design change. The new NI basemat lift-off analyses include several refinements to previous analyses, including (1) more accurate modeling of the basemat footprint and (2) increased structural damping, consistent with SMAs. Based on the ANSYS nonlinear time

history analysis performed by the applicant, the maximum predicted uplift (at the east edge of the basemat) is 0.30 cm (0.12 in.), compared to the previous prediction of 0.74 cm (0.29 in.). A comparison of the in-structure response spectra at 5 percent damping, between the new lift-off results and the original linear results (no liftoff), indicate that the effect of liftoff is insignificant in the horizontal direction and produces only small differences in the vertical direction, limited to the higher frequency region, for the shield building cylinder up to Elevation 265'. The applicant also studied the sensitivity of the results to different assumptions for soil mass participation and concluded that the in-structure response spectra are insensitive to this parameter.

The applicant evaluated the effect of NI basemat liftoff on the previously reported HCLPF values. For two electrical components, the estimated HCLPF values were reduced by a small amount, but are still significantly higher than 0.5g PGA.

The applicant identified a revision to DCD Tier 2, Section 3.8.2.1.2, "Containment Vessel Support," describing the shear studs, and a revision to Table 55-1 of the PRA report to reflect the reductions in HCLPF values for the two electrical components. The staff concluded that the information contained in the revised open item response provides a reasonable basis for resolving the issue of liftoff during a seismic margins RLE (0.5g PGA).

During the audit conducted on December 15 and 16, 2003, the staff verified that DCD Tier 2, Section 3.8.2.1.2, and the PRA Table 55-1 were revised. The staff reviewed the documents, "Effects of Basemat Lift-off on Seismic Response," APP-1000-S2C-064, Revision 2 and "Independent Verification of Containment Vessel Stability Analysis," APP-1100-S2C-101, Revision 1. These calculations include the details of the new analyses summarized in the second revision to the response to the open item. The staff concluded that the analyses conducted are technically adequate to support the revised evaluation of liftoff during a seismic margins RLE (0.5g PGA). Therefore, Open Item 19A.2-8 is resolved.

Generic Fragility Data

When HCLPF values could not be determined by using one of the methods described above, the applicant used generic fragility data. The cases in which this approach was used are the following:

- reactor internals and core assembly that includes fuel
- control rod drive mechanism (CRDM) and hydraulic drive units
- RCP
- accumulator tank
- piping
- cable trays
- valves
- MCR operation and switch stations
- ceramic insulators
- battery racks

The generic fragility data came from the URD which was reviewed by the NRC. Therefore, the use of the generic fragility data in the URD, which were developed by a joint industry group, 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 waterflow transmitter, located at Elevation 261' with a HCLPF value of 0.53 g, is likely to have an amplified seismic response. The applicant was requested 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 was Open Item 19A.2-9 in the DSER.

In a letter dated July 31, 2003, the applicant stated that no amplification factor was used to adjust generic fragility data for the AP1000 plant and presented qualitative arguments to support its approach. A quantitative basis was presented for valves, which are generally accepted as being seismically rugged. From PRA Table 55-1, Sheets 1 through 4, there are 3 primary components, 3 categories of mechanical equipment, 15 valves, and 3 categories of electrical equipment for which the HCLPF capacity is based on URD generic fragility data.

During a teleconference on August 22, 2003, the applicant agreed to revise the open item response to provide a quantitative basis for not applying amplification factors to the URD generic fragility data for primary components, mechanical equipment, and electrical equipment. The staff indicated that it would review calculations of HCLPF capacity based on URD generic fragility data.

During the audit conducted on October 6 through 9, 2003, the staff reviewed Revision 2 to the open item response, dated October 9, 2003. The revision addressed the staff's request that the applicant provide a quantitative basis for not applying amplification factors to URD generic fragility data for primary components, mechanical equipment, and electrical equipment. The staff found that the revised open item response shows that the generic HCLPF values obtained from the URD data are always higher than the seismic demand for the AP1000 application. This is an acceptable quantitative demonstration that the AP1000 demand is less than the capacity. In a letter to the NRC, dated October 10, 2003, the applicant officially transmitted and docketed its second revision to the response to this open item. Therefore, Open Item 19A.2-9 is resolved.

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 0.5 g, except for the ceramic insulators. Ceramic insulators are not safety-related, so their failure during an earthquake can disrupt the offsite ac power. However, the AP1000 plant design is such that it can safely accommodate the LOOP. The staff finds the seismic HCLPF value of 0.5 g is validated. The staff reviewed the revised DCD and PRA and concluded the item was resolved.

Verification of Equipment Fragility Data

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 NI 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 that 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 indicated that the steamline break events that could damage equipment in the upper elevations are not dominant contributors to the CDF. 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 the applicant 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 to the staff.

19A.3 Seismic Margin Model

Major SMA Model Assumptions

The applicant has used a PRA-based, SMA method similar to the AP600 plant. In conducting its SMA, the applicant made the following assumptions:

- Seismic events occur at full power.

- The RLE is 0.5 g.

- The LOOP occurs at the RLE. No credit is taken for non-safety-related diesel generators for onsite 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 the AP600 because the height of the containment and the overall mass of the AP1000 plant have increased. As indicated in the previous section

of this report, the staff determined that it would 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 was Open Item 19A.3-1 in the DSER.

In a letter dated July 31, 2003, the applicant provided a technical basis for concluding that the plant HCLPF is controlled by the minimum of the initiating event HCLPF values, independent of the HCLPF values for the mitigating systems modeled in the event trees. This is true for all but the transient event (EQ-IEV-LOSP). The applicant calculated the AP1000-specific HCLPF values for the initiating events and compared them to the AP600 values in PRA Tables 55-3 through 55-7. A comparison of basic event HCLPF values is presented in PRA Table 55-2. The staff found the response to be acceptable, except that the reported HCLPF values were subject to revision based on the resolution of open items related to the AP1000 seismic analysis methods.

Open Item 19A.2-8 tracked the resolution of seismic analysis methods and any consequential changes to HCLPF capacities. On the basis that Open Item 19A.3-1 addressed the systems-related methodology for determining the controlling HCLPF, and the staff has reviewed and accepted this methodology, therefore, Open Item 19A.3-1 is resolved.

Seismic Initiating Events

The applicant arranged the seismic event categories in the following hierarchical groups:

(1) EQ-STRUC—gross structural failure
(2) EQ-RVFA—failure of the reactor vessel occurs
(3) EQ-LLOCA—failure of RCS
(4) EQ-SLOCA—SGTR and large secondary line break
(5) EQ-ATWS—ATNS caused by an earthquake
(6) EQ-LOSP—LOOP caused by an earthquake

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 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 have been validated through the resolution of Open Item 19A.2-8 discussed in the previous section. The applicant 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 stated, “this assumption needs to be verified by a plant walkdown when an AP1000 plant is built.” However, there was no entry on the COL interface requirement

about the plant walkdown in DCD Tier 2, Table 1.8-2. There is an entry in DCD Tier 2, Table 1.8-2, item 19.59.10-1, "As-Built SSC HCLPF Comparison to Seismic Margin Evaluation." The applicant was asked 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 was Open Item 19A.3-2 in the DSER.

In its letter dated July 31, 2003, the applicant stated that the COL action items are described in DCD Tier 2, Section 19.59.10.5 and PRA Section 59.10.5 and identified in DCD Tier 2, Table 1.8-2. A verification walkdown will be included in DCD Chapter 19.59.10.5 and PRA Section 59.10.5. The applicant revised the DCD to include a COL action item for as-built verification of HCLPF values that have been incorporated into DCD Tier 2, Table 1.8-2 by referring to DCD Tier 2, Section 19.59.10.5 for verification walkdown. The staff finds the applicant's action satisfactory. This is COL Action Item 19A.2-2. Therefore, Item 19A.3-2 is resolved.

- 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 for which 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 the failure of the PRHR HX 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, SGTR, and large steamline breaks. SGTR event considers up to five simultaneous tube ruptures. The EQ-SLOCA grouping appears reasonable. However, it was not clear if the applicant considered degradation of SG tubes under the full service life of SG for developing the seismic fragility. The applicant was requested to explain how it considered service-related degradation of SG tubes in the development of the HCLPF value of this group. This was Open Item 19A.3-3 in the DSER.

In a letter dated July 31, 2003, the applicant submitted a revision to its response to this open item. This revision contains the technical basis for considering five simultaneous tube ruptures. In its original response to this open item, the applicant had addressed the tube degradation issue to the satisfaction of the staff.

During the August 22, 2003, teleconference followup, the applicant committed to revise the open item response to include its original discussion related to SGTR.

The applicant submitted a second revision to the open item response on September 23, 2003. The staff reviewed the final response to the open item during the audit and found that it adequately addressed the staff's concerns. Therefore, Open Item 19A.3-3 is resolved.

- EQ-LOSP: The applicant 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 group 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 of the AP1000 PRA. 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 Conclusions

SECY-93-087 advises 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 1 and 2/3 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 a PGA value of 0.5 g.

In order to satisfy this guidance, 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 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 PGA of 0.5 g. Thus, the AP1000 standard design meets the guidance indicated in SECY-93-087 and the corresponding SRM regarding the SMA methodology, and is, therefore, acceptable.